Národné centrum zdravotníckych informácií

INFORMÁCIA O VÝSLEDKU VYHODNOTENIA PONÚK A PORADIE UCHÁDZAČOV

podľa § 55 ods. 2 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“)

Názov predmetu zákazky:
DNS pre IKT vybavenie a súvisiace služby_ Revitalizácia existujúceho pracoviska kybernetickej bezpečnosti NCZI

Postup vo verejnom obstarávaní:
Zákazka zadávaná v rámci dynamického nákupného systému na predmet „DNS pre IKT vybavenie a súvisiace služby“

Vyhlásenie verejného obstarávania:
Oznámenie o vyhlásení verejného obstarávania uverejnené v Dodatku k Úradnému vestníku Európskej únie č. OJ S 226/2025 zo dňa 24.11.2025 pod zn. 779298-2025 a vo Vestníku verejného obstarávania č. 237/2025 zo dňa 25.11.2025 pod zn. 18626 - MUT na nadlimitnú zákazku postupom užšej súťaže za účelom zriadenia dynamického nákupného systému s názvom „DNS pre IKT vybavenie a súvisiace služby“ (ďalej len „DNS“). DNS bol zriadený dňa 16.02.2026.

PČ uchádzača	Uchádzač	Kritérium na vyhodnotenie ponúk: **Najnižšia celková cena v EUR s DPH**	Poradie uchádzača po vyhodnotení ponúk na základe kritérií na vyhodnotenie ponúk
		Návrh na plnenie kritérií	
1	**Corpus Solutions a.s.** Štětkova 1638/18, Nusle 140 00 Praha 4 IČO: 257 64 616	8 609 691,27	1.

Identifikácia úspešného uchádzača:
Corpus Solutions a.s.
Štětkova 1638/18, Nusle
140 00 Praha 4
IČO: 257 64 616 (ďalej len „úspešný uchádzač“)

Dôvod úspešnosti ponuky:
Ponuka predložená úspešným uchádzačom na vyššie uvedený predmet zákazky bola predložená v súlade so všetkými požiadavkami verejného obstarávateľa a splnila všetky požiadavky verejného obstarávateľa určené v oznámení o vyhlásení verejného obstarávania, v súťažných podkladoch, vo Výzve na predloženie ponuky na predmet zákazky „DNS pre IKT vybavenie a súvisiace služby_ Revitalizácia existujúceho pracoviska kybernetickej bezpečnosti NCZI“ a v iných dokumentoch potrebných na vypracovanie ponuky a v rámci vyhodnocovania ponúk na základe určeného kritéria na vyhodnotenie ponúk sa ponuka úspešného uchádzača umiestnila na prvom mieste v poradí. Úspešný uchádzač je zapísaný v zozname hospodárskych subjektov a spĺňa podmienky účasti osobného postavenia podľa zákona o verejnom obstarávaní a zároveň všetky doklady preukazujúce splnenie podmienok účasti v predmetnom dynamickom nákupnom systéme sú aktuálne. Verejný obstarávateľ skonštatoval, že ponuka úspešného uchádzača spĺňa požiadavky na predmet zákazky.

Vlastný návrh plnenia úspešného uchádzača:
Predmet zákazky pozostáva z dodania, rozšírenia a sprevádzkovania technologických komponentov pre revitalizáciu existujúceho pracoviska kybernetickej bezpečnosti NCZI vrátane pripojenia štyroch verejných nemocníc do monitorovaného a chráneného prostredia. Súčasťou plnenia sú najmä tieto časti:

1. **Enterprise bezpečnostná analytická platforma typu XDR/SIEM/SOAR**
   Dodanie centrálnej bezpečnostnej analytickej platformy na zber, spracovanie, koreláciu a vyhodnocovanie bezpečnostných udalostí, incidentov, alertov, endpointovej telemetrie, threat intelligence dát a reportingu, vrátane požadovaných licencií, modulov, úložísk, integračných možností, podpory a prevádzkového nastavenia. Platforma má pokrývať funkcionality SIEM, XDR, SOAR, incident management, threat intelligence management a identity threat detection and response.
2. **Rozšírenie existujúceho nástroja pre riadenie kybernetickej bezpečnosti**
   Rozšírenie existujúceho nástroja pre riadenie kybernetickej bezpečnosti o požadované moduly a funkcionality, najmä na podporu riadenia bezpečnostných procesov, rizík, súladu, workflowov a súvisiacich činností kybernetickej bezpečnosti.
3. **Centrálny firewall systém**
   Dodanie alebo rozšírenie centrálneho firewallového riešenia novej generácie s podporou vysokej dostupnosti, NGFW funkcionalít, IDS/IPS, aplikačnej kontroly, anti-malware ochrany, URL filtrovania, SD-WAN funkcionality, virtuálnych inštancií, centrálneho manažmentu, logovania a integrácie s dodávanou bezpečnostnou analytickou platformou.
4. **Firewall pre monitorovanú lokalitu**
   Dodanie firewallového zariadenia pre monitorovanú lokalitu s požadovanou priepustnosťou, podporou IPS, IPsec VPN, SD-WAN spoke funkcionality, ochranou pred hrozbami, aplikačnou kontrolou, botnet ochranou, URL/DNS filtrovaním, redundantným napájaním, dopravou, montážou, inštaláciou a nastavením.
5. **Privileged Access Management server**
   Dodanie komponentu pre potreby riešenia správy privilegovaných prístupov, vrátane hardvérových, bezpečnostných, manažmentových a servisných parametrov potrebných na jeho prevádzku.
6. **Serverová infraštruktúra – Server Typ 2**
   Dodanie serverových zariadení určených pre monitorované lokality s požadovaným výkonom, procesormi, pamäťou, diskovým subsystémom, sieťovými adaptérmi, bezpečnostnými prvkami, vzdialenou správou, servisnou podporou a integráciou do centrálnej správy serverovej infraštruktúry.
7. **Sieťové prepínače pre dátové centrum a LAN infraštruktúru**
   Dodanie DC prepínačov a LAN prepínačov jednotlivých typov s požadovanými portami, priepustnosťou, smerovacími a prepínacími funkciami, podporou VLAN, NetFlow, bezpečnostných mechanizmov, centrálnej správy, servisnej podpory a inštalácie.
8. **Prepojovacie káble a optické moduly**
   Dodanie metalických 10G a 100G káblov, 10G SFP modulov a 100G QSFP/QFP modulov v požadovaných počtoch, parametroch, dosahu, dĺžkach a kompatibilite s dodávanými prepínačmi, vrátane požadovanej záruky a podpory rýchlej výmeny.
9. **Rozšírenie existujúcej serverovej infraštruktúry – Chassis**
   Dodanie chassis pre rozšírenie existujúcej serverovej infraštruktúry, vrátane zdrojov, X-Fabric modulov, Fabric Interconnect modulov, licencií, servisnej podpory, dopravy, montáže, inštalácie a nastavenia.

10. **Rozšírenie licencií existujúcej virtualizačnej platformy**
    Dodanie predplatného na rozšírenie existujúcej virtualizačnej platformy o licencie VMware vSphere Foundation a Standard trvaním predplatného na 2 roky vrátane podpory, aktualizácií, bezpečnostných záplat, administrácie a asistencie pri aktivácii.
11. **Rozšírenie licencií existujúceho zálohovacieho riešenia**
    Dodanie licencií existujúceho zálohovacieho riešenia Veeam Data Platform Advanced v požadovanom počte 6 ks na obdobie 2 rokov, vrátane podpory hybridných prostredí, replikácie, rýchlej obnovy, inkrementálneho zálohovania, archivácie, 24/7 Production Support, aktualizácií a asistencie pri aktivácii.
12. **NDR senzory/collectory pre monitorovanú lokalitu**
    Dodanie 4 ks virtuálneho NDR riešenia pre monitorovanú lokalitu, určeného na pasívny zber, analýzu a spracovanie kópie sieťovej prevádzky, vrátane softvéru, licencií, aktualizácií, podpory, forenznej analýzy, vizualizácie komunikácie a detekcie bezpečnostných a prevádzkových anomálií.

Miesto dodania

Miesto dodania je sídlo verejného obstarávateľa (alebo jeho určené prevádzkové lokality).

Trvanie zákazky / lehota dodania

Predmet zákazky musí byť dodaný do 31.10.2026

Uchádzač pre každú položku tvoriacu predmet zákazky:

1. **Vyplní všetky údaje v stĺpci *„Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru“* hodnotu parametra alebo vlastnosť ponúkaného tovaru, z ktorej je zrejmý spôsob splnenia minimálnej požiadavky, tzn. vyplní všetky údaje v stĺpci *„Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru“* – uviesť parameter alebo vlastnosť ponúkaného tovaru v nižšie uvedených tabuľkách pri každom predmete zákazky slovne s objektívnym vyjadrením danej hodnoty (plnenie daného parametra uchádzačom), pričom presne špecifikuje jednoznačné označenie príslušného komponentu výrobcu s označením part number, resp. product code.**
2. **Pripojí detailnú technickú konfiguráciu s jednoznačným označením komponentov podľa výrobcu (part number, product code a pod...).**
3. **Pripojí priamy odkaz (weblink) na internetovú stránku výrobcu s daným produktom pre možnú verifikáciu (kontrolu) popisu ponúkaného produktu (riešenia) s požiadavkou verejného obstarávateľa.**
4. **Všetky komponenty uvedené v konfigurácii ponúkaného predmetu zákazky musia byť nové, nepoužité a certifikované výrobcom daného predmetu zákazky (originálne príslušenstvo).**
5. **Verejný obstarávateľ upozorňuje uchádzačov, aby uchádzači uviedli parameter/vlastnosť ponúkaného tovaru na každú požiadavku verejného obstarávateľa, resp. každú časť jednotlivých požiadaviek.**
6. **V prípade nesplnenia vyššie uvedených požiadaviek verejného obstarávateľa na predmet zákazky, bude ponuka uchádzača z verejnej súťaže vylúčená.**

1. Centrálna lokalita

1.1 Enterprise bezpečnostná analytická platforma typu XDR/SIEM/SOAR

Revitalizácia existujúceho pracoviska kybernetickej bezpečnosti NCZI			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Palo Alto Networks* ***Produkt**: Cortex XSIAM – jednotná bezpečnostná analytická platforma typu XDR/SIEM/SOAR* ***Edícia**: Cortex XSIAM Enterprise s Enterprise Multi-Tenant funkcionalitou* ***Verzia**: Aktuálna výrobcom podporovaná SaaS verzia; platforma je priebežne aktualizovaná výrobcom bez potreby lokálneho upgrade. Produktová dokumentácia je vedená pre Cortex XSIAM 3.x.* ***Model poskytovania**: Centrálne spravovaná cloudová služba/SaaS* ***Konfigurácia obsahuje**:* • ***PAN-XSIAM-ENT-MT** – 1 parent tenant Enterprise Multi-Tenant, ktorý zahŕňa 1 child tenant.* • ***PAN-XSIAM-ENT-MT-TEN** – 5 ďalších child tenantov; celkovo 1 parent tenant a 6 child tenantov.* • ***PAN-XSIAM-BASE-ENT** – Enterprise Employee Tier pre 5 000 zamestnancov v základnej fáze a ďalších 5 000 v rozširujúcej fáze; licencia zahŕňa endpointové oprávnenie pre každého licencovaného zamestnanca.* • ***PAN-XSIAM-BASE-GB** – denný ingest minimálne 580 GB/deň s následným kapacitným rozšírením podľa fázovanej konfigurácie.* • ***PAN-XSIAM-TIM** – modul Threat Intelligence Management.* • ***PAN-XSIAM-ITDR** – modul Identity Threat Detection and Response, dimenzovaný podľa počtu licencovaných používateľov.* • ***PAN-XSIAM-GB-FRWRD** – forwardovanie ingestovaných dát v rozsahu 580 GB/deň počas jedného roka.* • ***PAN-XSIAM-EP-FRWRD** – forwardovanie endpointových dát počas jedného roka v rozsahu uvedenom v licenčnej konfigurácii.* • ***PAN-XSIAM-INCDT-GB-RTN** a **PAN-XSIAM-INCDT-EP-RTN** – rozšírenie retencie alertov a incidentov o 6 mesiacov nad základnú retenciu.*	**SPLNIL**

		• ***PAN-XSIAM-GB-HOT-RTN*** *a* ***PAN-XSIAM-EP-HOT-RTN*** *– ďalších 11 mesiacov hot storage nad základnú 30-dňovú retenciu, teda celkovo 12 mesiacov hot storage pre ingestované a endpointové dáta.* • ***PAN-XSIAM-PREM-SUCCESS*** *– Cortex XSIAM Premium Success zahŕňajúci prémiovú podporu a služby Scale and Optimize.* *Overenie produktu:* *https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiam* *Overenie licenčného modelu: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Cortex-XSIAM-product-licenses* *Overenie multitenantného modelu: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Onboard-Cortex-multi-tenant* *Overenie retencie: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Data-retention* *Overenie Premium Success:* *https://www.paloaltonetworks.com/resources/datasheets/sd-cortex-xsiam-premium-success* *Technická špecifikácia:* • *1x PAN-XSIAM-ENT-MT* • *580x PAN-XSIAM-BASE-GB* • *5000x PAN-XSIAM-BASE-ENT* • *5x PAN-XSIAM-ENT-MT-TEN* • *1x PAN-XSIAM-TIM* • *580x PAN-XSIAM-GB-FRWRD* • *4999x PAN-XSIAM-EP-FRWRD* • *5000x PAN-XSIAM-ITDR* • *3480x PAN-XSIAM-INCDT-GB-RTN* • *30000x PAN-XSIAM-INCDT-EP-RTN* • *6380x PAN-XSIAM-GB-HOT-RTN* • *55000x PAN-XSIAM-EP-HOT-RTN* • *30000x PAN-XSIAM-INCDT-EP-RTN* • *3480x PAN-XSIAM-INCDT-GB-RTN*	

		• *5000x PAN-XSIAM-BASE-ENT* • *580x PAN-XSIAM-BASE-GB* • *55000x PAN-XSIAM-EP-HOT-RTN* • *6380x PAN-XSIAM-GB-HOT-RTN* • *1x PAN-XSIAM-ENT-MT* • *5000x PAN-XSIAM-EP-FRWRD* • *580x PAN-XSIAM-GB-FRWRD* • *1x PAN-XSIAM-TIM* • *5x PAN-XSIAM-ENT-MT-TEN* • *5000x PAN-XSIAM-ITDR* • *1x PAN-XSIAM-PREM-SUCCESS*	
Architektúra platformy	Riešenie musí byť poskytované ako centrálne spravovaná bezpečnostná analytická platforma s jednotnou administrátorskou konzolou a spoločným úložiskom bezpečnostných dát alebo ekvivalentným dátovým jazerom použiteľným pre SIEM, XDR, SOAR, endpoint telemetriu, incidenty, alerty, threat intelligence a reporting.	***Spĺňa.*** *Cortex XSIAM je centrálne spravovaná bezpečnostná analytická platforma s jednotnou administrátorskou konzolou a spoločným dátovým jazerom Cortex XDL. XDL centralizuje, normalizuje a obohacuje dáta používané pre SIEM, XDR, SOAR, endpointovú telemetriu, incidenty, alerty, threat intelligence a reporting. Ponúkaná Multi-Tenant konfigurácia zároveň umožňuje centrálnu správu child tenantov z parent tenantu.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://www.paloaltonetworks.com/cortex/cortex-xdl* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/child-tenant-management*	**SPLNIL**
	Riešenie musí pokrývať funkcionality SIEM, XDR, SOAR, incident management, endpoint telemetry analytics, threat intelligence management, identity threat detection and response a reporting v jednom ucelenom prevádzkovom modeli.	***Spĺňa.*** *Cortex XSIAM Enterprise poskytuje v jednej platforme a administrátorskej konzole funkcionality SIEM, XDR/EDR, SOAR, incident management, analýzu endpointovej telemetrie a reporting. Threat Intelligence Management a Identity Threat Detection and Response sú pokryté ponúkanými modulmi PAN-XSIAM-TIM a PAN-XSIAM-ITDR.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr	
	Riešenie musí byť postavené na škálovateľnej architektúre vhodnej pre cloudovú alebo SaaS prevádzku, prípadne ekvivalentný poskytovaný model služby, pričom musí umožňovať paralelné analytické a vyhľadávacie procesy bez obmedzenia požadovaných kapacitných parametrov.	***Spĺňa.*** *Cortex XSIAM je cloudová SaaS platforma postavená na horizontálne škálovateľnom dátovom jazere Cortex XDL s petabajtovou kapacitou. Distribuovaná architektúra umožňuje paralelný zber dát, kontinuálnu detekčnú a ML analytiku a súbežné XQL vyhľadávanie bez zníženia ponúkanej licencovanej ingestnej a retenčnej kapacity.* https://www.paloaltonetworks.com/cortex/cortex-xdl https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiam	**SPLNIL**
	Poskytovateľ alebo výrobca platformy musí preukázať primeranú úroveň bezpečnostného riadenia služby, napríklad certifikáciou alebo auditom typu ISO/IEC 27001, SOC 2 alebo ekvivalentným nezávisle overiteľným bezpečnostným štandardom.	***Spĺňa.*** *Výrobca Palo Alto Networks je certifikovaný podľa ISO/IEC 27001 a Cortex XSIAM je nezávisle auditovaný podľa SOC 2 Type II. Aktuálne certifikáty a audítorské správy sú dostupné prostredníctvom Trust Center výrobcu, pričom SOC 2+ report možno poskytnúť na vyžiadanie.* https://www.paloaltonetworks.com/legal-notices/trust-center/iso-27000-series https://www.paloaltonetworks.com/legal-notices/trust-center/soc https://www.paloaltonetworks.com/customers/cortex-xsiam-reshapes-secops-for-fortune-500-financial-giant	**SPLNIL**
	Riešenie musí podporovať šifrovanie dát pri prenose medzi komponentmi a šifrovanie uložených dát; požaduje sa podpora riadenia šifrovacích kľúčov zákazníkom alebo ekvivalentný mechanizmus kontroly nad ochranou dát.	***Spĺňa.*** *Cortex XSIAM šifruje uložené dáta aj komunikáciu medzi endpointovými agentmi, Broker VM a cloudovou platformou prostredníctvom HTTPS/TLS; komunikácia Broker VM so serverom podporuje TLS 1.3. Funkcia BYOK umožňuje zákazníkovi vytvárať, importovať, spravovať a rotovať vlastné šifrovacie kľúče pre dáta tenantu a aktivuje sa pri jeho vytvorení.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/activate-cortex-xsiam/bring-your-own-keys https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets/activate-local-agent-settings	**SPLNIL**

	Riešenie musí umožňovať nasadenie lokálneho sprostredkovateľského alebo zberového komponentu v prostredí obstarávateľa pre prípady, keď nie je vhodná alebo možná priama komunikácia dátových zdrojov a endpointov so službou platformy.	***Spĺňa.*** *Cortex XSIAM umožňuje v prostredí verejného obstarávateľa nasadiť lokálny komponent Broker VM. Ten zabezpečuje zber a sprostredkovanie dát z interných zdrojov a prostredníctvom funkcie Agent Proxy aj komunikáciu endpointov, ktoré nemajú alebo nemôžu používať priame pripojenie ku cloudovej platforme.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/broker-vm/set-up-and-configure-broker-vm* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets*	**SPLNIL**
	Riešenie musí umožňovať správu endpointov bez priamej konektivity do internetu prostredníctvom lokálneho sprostredkovateľského komponentu alebo ekvivalentného proxy mechanizmu, ktorý zabezpečí komunikáciu s centrálnou platformou a prenos telemetrie bezpečným spôsobom.	***Spĺňa.*** *Funkcia Agent Proxy na lokálnom Broker VM umožňuje správu endpointov bez priameho internetového pripojenia. Endpointové agenty komunikujú s Broker VM bezpečne prostredníctvom HTTPS na porte TCP/443; Broker VM následne sprostredkuje komunikáciu s centrálnou platformou Cortex XSIAM vrátane prenosu telemetrie, politík a aktualizácií.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets/activate-local-agent-settings*	**SPLNIL**
	Technická dokumentácia platformy, integračných mechanizmov, API a odporúčaných prevádzkových postupov musí byť dostupná minimálne v anglickom jazyku počas celej doby poskytovania služby.	***Spĺňa.*** *Palo Alto Networks poskytuje priebežne aktualizovanú technickú dokumentáciu Cortex XSIAM v anglickom jazyku, ktorá pokrýva správu platformy, integračné mechanizmy, dátové zdroje, REST API, nasadenie a odporúčané prevádzkové postupy. Dokumentácia bude dostupná v anglickom jazyku počas celej doby poskytovania služby.* *https://docs-cortex.paloaltonetworks.com/* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM-REST-API/Get-started-with-Cortex-XSIAM-APIs* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources*	**SPLNIL**
	Lokálny sprostredkovateľský komponent musí umožňovať bezpečný zber logov, telemetrie a	***Spĺňa.*** *Cortex XSIAM Broker VM zabezpečuje lokálny zber logov a telemetrie prostredníctvom zberových appletov a bezpečnú komunikáciu endpointových agentov cez Agent Proxy*	**SPLNIL**

	komunikáciu agentov alebo dátových zdrojov s platformou a musí byť dostupný ako virtuálne alebo softvérové nasadenie použiteľné v bežnom enterprise virtualizačnom prostredí.	*a HTTPS/TLS. Komponent je dostupný ako virtuálny softvérový appliance vo formátoch OVA, VHD a QCOW2 pre VMware ESXi, Microsoft Hyper-V, KVM a Nutanix AHV.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets* *https://docs-cortex.paloaltonetworks.com/r/Cortex-CLOUD/Cortex-Cloud-Runtime-Security-Documentation/Set-up-Broker-VM-on-VMware-ESXi-using-vSphere-Client* *https://cortex-docs.paloaltonetworks.com/cortex-xdr-5.x/configure-cortex-xdr/data-management/broker-vm/set-up-and-configure-broker-vm/broker-vm-image-installations/set-up-broker-vm-on-microsoft-hyper-v*	
Kapacitné požiadavky	Licencovanie minimálne pre 5 000 enterprise používateľov/zamestnancov alebo ekvivalentný enterprise tier, pričom riešenie musí umožňovať využitie bezpečnostnej analytiky pre celé prostredie obstarávateľa.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje 5 000 licencií PAN-XSIAM-BASE-ENT, pričom každá licencia Enterprise tier zahŕňa jedného zamestnanca a jeden chránený endpoint. Spolu s licencovanou dátovou ingestnou kapacitou umožňuje Cortex XSIAM využívať jednotnú bezpečnostnú analytiku nad endpointovými, sieťovými, cloudovými, identitnými a ďalšími dátami celého prostredia obstarávateľa.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://www.paloaltonetworks.com/cortex/cortex-xdl*	**SPLNIL**
	Podpora spracovania endpointovej telemetrie a bezpečnostných udalostí minimálne z 5 000 koncových zariadení.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje 5 000 licencií PAN-XSIAM-BASE-ENT, pričom každá licencia zahŕňa jeden endpoint. Cortex XSIAM tak zabezpečuje kontinuálny zber, spracovanie, koreláciu a analýzu endpointovej telemetrie a bezpečnostných udalostí minimálne z 5 000 koncových zariadení.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/manage-event-forwarding/endpoints-event-forwarding-included-excluded-fields-by-event-type*	**SPLNIL**
	Podpora denného ingestu bezpečnostných dát minimálne 580 GB/deň bez degradácie základných analytických, vyhľadávacích a retenčných funkcií.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje licenciu PAN-XSIAM-BASE-GB v rozsahu 580 GB denného ingestu. Retenčné licencie PAN-XSIAM-GB-HOT-RTN a PAN-XSIAM-INCDT-GB-RTN sú dimenzované na rovnaký objem dát. Škálovateľná dátová vrstva*	**SPLNIL**

		Cortex XDL zabezpečuje spracovanie tohto objemu bez degradácie analytických, XQL vyhľadávacích a retenčných funkcií. *https://www.paloaltonetworks.com/cortex/cortex-xdl* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Overview-of-data-ingestion-metrics*	
	Uchovávanie alertov a incidentov minimálne 180 dní nad základnú licencovanú retenciu alebo ekvivalentne minimálne 180 dní dostupnej incidentovej histórie.	***Spĺňa.*** *Základná licencia Cortex XSIAM zahŕňa 180-dňovú retenciu alertov a incidentov. Ponúkané licencie PAN-XSIAM-INCDT-GB-RTN a PAN-XSIAM-INCDT-EP-RTN pridávajú ďalších 6 × 30 dní pre dáta z endpointov aj ostatných zdrojov. Celková dostupná história alertov a incidentov je preto 360 dní.* *https://live.paloaltonetworks.com/t5/cortex-xdr-articles/data-retention-enforcement-faq/ta-p/512873*	**SPLNIL**
	Hot storage pre endpointové dáta minimálne 12 mesiacov s možnosťou rýchleho vyhľadávania a vyšetrovania bez manuálnej obnovy z archívu.	***Spĺňa.*** *Základná licencia Cortex XSIAM zahŕňa 30 dní hot storage pre endpointové dáta. Ponúkaná licencia PAN-XSIAM-EP-HOT-RTN pridáva ďalších 11 × 30 dní, čím zabezpečuje celkovo minimálne 12 mesiacov hot storage. Dáta zostávajú online a sú okamžite dostupné na XQL vyhľadávanie, threat hunting a vyšetrovanie bez manuálnej obnovy z archívu.* *https://live.paloaltonetworks.com/t5/cortex-xdr-articles/data-retention-enforcement-faq/ta-p/512873* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Edit-and-run-queries-in-Query-Center*	**SPLNIL**
	Hot storage pre ingestované dáta minimálne 12 mesiacov pri objeme minimálne 580 GB/deň s dostupnosťou pre koreláciu, query, reporting a threat hunting.	***Spĺňa.*** *Licencia PAN-XSIAM-BASE-GB pokrýva denný ingest 580 GB a základných 30 dní hot storage. Ponúkaná licencia PAN-XSIAM-GB-HOT-RTN v rozsahu 6 380 GB-mesiacov pridáva ďalších 11 × 30 dní, čím zabezpečuje minimálne 12 mesiacov hot storage pri objeme 580 GB/deň. Dáta zostávajú online dostupné pre koreláciu, XQL query, reporting a threat hunting bez obnovy z archívu.* *https://live.paloaltonetworks.com/t5/cortex-xdr-articles/data-retention-enforcement-faq/ta-p/512873* *https://www.paloaltonetworks.com/cortex/cortex-xdl*	**SPLNIL**

	Forwardovanie endpointových dát z minimálne 5 000 endpointov po dobu minimálne 1 roka.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje licenciu PAN-XSIAM-EP-FRWRD v množstve 5 000, pričom každá jednotka oprávňuje na forwardovanie dát z jedného Cortex XSIAM endpointu počas jedného roka. Riešenie tak zabezpečuje forwardovanie endpointovej telemetrie z minimálne 5 000 endpointov na požadované obdobie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/manage-event-forwarding/endpoints-event-forwarding-included-excluded-fields-by-event-type*	**SPLNIL**
	Forwardovanie ingestovaných dát v rozsahu minimálne 580 GB/deň po dobu minimálne 1 roka do externého bezpečnostného, dátového alebo archivačného systému.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje licenciu PAN-XSIAM-GB-FRWRD v množstve 580, pričom každá jednotka umožňuje forwardovanie 1 GB dát denne počas jedného roka. Celkový licencovaný rozsah preto predstavuje minimálne 580 GB/deň počas 12 mesiacov do externého bezpečnostného, dátového alebo archivačného systému.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services*	**SPLNIL**
	Podpora multitenantného modelu minimálne v rozsahu 1 parent tenant a 6 child tenantov.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje jeden PAN-XSIAM-ENT-MT parent tenant, ktorý zahŕňa jeden child tenant, a ďalších päť licencií PAN-XSIAM-ENT-MT-TEN. Celkový rozsah predstavuje 1 parent tenant a 6 child tenantov s centrálnou správou, monitoringom a vyšetrovaním z parent tenantu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/child-tenant-management*	**SPLNIL**
	Licenčný model musí byť transparentný a predvídateľný; licencia pre ochranu alebo spracovanie endpointovej telemetrie nesmie obmedzovať objem bezpečnostných dát zbieraných z jednotlivých	***Spĺňa.*** *Licenčný model Cortex XSIAM transparentne oddeľuje počet chránených endpointov od celkovej dátovej kapacity. Položka PAN-XSIAM-BASE-ENT pokrýva 5 000 používateľov a endpointov, zatiaľ čo PAN-XSIAM-BASE-GB samostatne určuje celkový denný ingest 580 GB. Na jednotlivý endpoint sa neuplatňuje dodatočný licenčný limit objemu telemetrie ani EPS limit nad rámec celkovej licencovanej kapacity tenantu.*	**SPLNIL**

	endpointov nad rámec samostatne licencovaného denného ingestu.	*https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Overview-of-data-ingestion-metrics*	
	Všetky licencie, moduly, konektory, úložné kapacity, forwarding práva a podporné služby potrebné na splnenie minimálnych požiadaviek tejto špecifikácie musia byť súčasťou dodávky bez skrytých alebo dodatočných povinných poplatkov.	***Spĺňa.*** *Dodávka zahŕňa všetky licencie a oprávnenia potrebné na splnenie špecifikácie: Cortex XSIAM Enterprise pre 5 000 endpointov, ingest 580 GB/deň, Multi-Tenant model 1 parent + 6 child tenantov, TIM, ITDR, požadované hot storage a incidentové retencie, endpointové a dátové forwarding práva a službu Premium Success. Súčasťou sú aj potrebné štandardné konektory, integrácie a obsahové balíky. Splnenie požiadaviek nevyžaduje žiadne ďalšie povinné licencie alebo skryté poplatky výrobcu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Cortex-Marketplace* *https://www.paloaltonetworks.com/resources/datasheets/sd-cortex-xsiam-premium-success*	**SPLNIL**
	Súčasťou dodávky musí byť modul threat intelligence management, modul identity threat detection and response a prémiová servisná podpora.	***Spĺňa.*** *Súčasťou ponúkanej konfigurácie sú:* • *PAN-XSIAM-TIM – Threat Intelligence Management,* • *PAN-XSIAM-ITDR – Identity Threat Detection and Response pre požadovaný počet používateľov,* • *PAN-XSIAM-PREM-SUCCESS – Premium Success servisná a podporná služba pre Cortex XSIAM.* *Všetky požadované moduly a prémiová podpora sú zahrnuté priamo v dodávke.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr*	**SPLNIL**

		https://www.paloaltonetworks.com/resources/datasheets/sd-cortex-xsiam-premium-success	
Základná funkcionalita	Jednotné používateľské rozhranie pre prácu s udalosťami, alertmi, incidentmi, vyšetrovaním, vyhľadávaním, pravidlami, automatizáciou, threat intelligence dátami, identitnými rizikami, dashboardmi a reportmi.	***Spĺňa.*** *Cortex XSIAM poskytuje jednotné webové používateľské rozhranie pre udalosti, alerty, incidenty, vyšetrovanie, XQL vyhľadávanie, detekčné a korelačné pravidlá, automatizované playbooky, threat intelligence, identitné riziká, dashboardy a reporty. Moduly TIM a ITDR sú integrované priamo do rovnakej konzoly bez potreby používania samostatných nástrojov.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr*	**SPLNIL**
	Centralizovaná správa dátových zdrojov, konektorov, parserov, detekčných pravidiel, incidentových workflowov, playbookov, integrácií, tenantov, používateľov, rolí a oprávnení.	***Spĺňa.*** *Cortex XSIAM zabezpečuje centralizovanú správu dátových zdrojov, konektorov, parserov a dátového modelovania, detekčných a korelačných pravidiel, incidentových workflowov, playbookov a integrácií. Ponúkaná Multi-Tenant konfigurácia zároveň umožňuje z parent tenantu spravovať child tenantov, používateľov, roly a oprávnenia prostredníctvom RBAC.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Cortex-Marketplace* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/child-tenant-management* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Role-Based-Access-Control*	**SPLNIL**
	Riešenie musí kombinovať funkcionalitu SIEM pre zber a koreláciu logov, XDR pre analýzu naprieč bezpečnostnými	***Spĺňa.*** *Cortex XSIAM v jednej platforme kombinuje SIEM na zber, normalizáciu a koreláciu logov, XDR na detekciu a analýzu hrozieb naprieč endpointovou, sieťovou,*	**SPLNIL**

	doménami a SOAR pre automatizáciu reakčných postupov.	*cloudovou a identitnou doménou a natívne SOAR funkcionality na automatizáciu vyšetrovania a reakčných postupov prostredníctvom playbookov.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://www.paloaltonetworks.com/resources/techbriefs/cortex-xsiam*	
	Podpora korelácie udalostí z endpointov, sietí, firewallov, identity providerov, adresárových služieb, cloudových služieb, SaaS aplikácií, e-mailovej bezpečnosti, DNS, DHCP, VPN a aplikačných logov.	***Spĺňa.*** *Cortex XSIAM prostredníctvom jednotného dátového modelu Cortex XDL normalizuje a koreluje udalosti z endpointov, sietí, firewallov, identity providerov, adresárových služieb, cloudových služieb, SaaS aplikácií, e-mailových bezpečnostných riešení, DNS, DHCP, VPN a aplikačných logov. Zdroje možno pripájať natívnymi integráciami, API, Syslogom alebo lokálnymi kolektormi Broker VM.* *https://www.paloaltonetworks.com/cortex/cortex-xdl* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets*	**SPLNIL**
	Riešenie musí poskytovať škálovateľnú architektúru vhodnú pre enterprise alebo MSSP/SOC prevádzku s vysokým objemom bezpečnostných dát.	***Spĺňa.*** *Cortex XSIAM je cloudová SaaS platforma postavená na petabajtovo škálovateľnom dátovom jazere Cortex XDL, určená na spracovanie vysokých objemov bezpečnostných dát v enterprise a SOC prostrediach. Ponúkaný Multi-Tenant model s parent a child tenantmi zároveň podporuje centralizovanú MSSP prevádzku, oddelenie zákazníckych prostredí a riadenie bezpečnostných operácií vo veľkom rozsahu.* *https://www.paloaltonetworks.com/cortex/cortex-xdl* *https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiam* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/child-tenant-management*	**SPLNIL**
	Riešenie musí umožniť prevádzkové oddelenie administrátorských, analytických, reportovacích,	***Spĺňa.*** *Cortex XSIAM podporuje oddelenie administrátorských, analytických, reportovacích*	**SPLNIL**

	integračných a tenantových činností.	*a integračných činností prostredníctvom granulárneho RBAC, používateľských skupín a oprávnení k jednotlivým funkciám a objektom. Multi-Tenant architektúra zároveň zabezpečuje logické a prevádzkové oddelenie parent a child tenantov vrátane ich dát a správy.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Role-Based-Access-Control* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Manage-access-to-objects* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/child-tenant-management*	
	Riešenie musí viesť auditovateľnú históriu používateľskej, systémovej, administrátorskej, integračnej a reakčnej aktivity.	***Spĺňa.*** *Cortex XSIAM vedie centralizované Management Audit Logs a Agent Audit Logs, ktoré zaznamenávajú autentifikáciu používateľov, administrátorské a vyšetrovacie operácie, systémové udalosti, zmeny dátových zdrojov a integrácií, spustenia pravidiel a automatizácií aj reakčné zásahy vykonané prostredníctvom Action Center. Záznamy obsahujú vykonávateľa, čas, typ operácie, cieľ a výsledný stav a možno ich vyhľadávať alebo forwardovať do externého systému.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Monitor-administrative-activity* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/data-and-log-notification-formats/management-audit-log-messages* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/manage-endpoint-protection/monitor-agent-activity*	**SPLNIL**
Administrátorská konzola	Administrátorská konzola musí umožňovať správu všetkých podstatných funkcií platformy prostredníctvom webového rozhrania bez potreby	***Spĺňa.*** *Cortex XSIAM poskytuje jednotnú webovú administrátorskú konzolu na správu dátových zdrojov, endpointov, detekčných pravidiel, incidentov, vyšetrovania, automatizácií, playbookov, TIM, ITDR, používateľov, tenantov, dashboardov a*	**SPLNIL**

	samostatných desktopových konzol pre jednotlivé bezpečnostné moduly.	*reportov. Jednotlivé bezpečnostné moduly sú integrované do rovnakého rozhrania a nevyžadujú samostatné desktopové konzoly.* *https://www.paloaltonetworks.com/cortex/cortex-xsiam* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam*	
	Webové rozhranie musí byť založené na štandardných webových technológiách a nesmie vyžadovať inštaláciu špeciálnych pluginov do prehliadača.	***Spĺňa.*** *Administrátorské rozhranie Cortex XSIAM je webová aplikácia založená na štandardných webových technológiách a je prístupné prostredníctvom podporovaných verzií prehliadačov Google Chrome, Mozilla Firefox, Safari a Microsoft Edge. Na používanie konzoly sa nevyžaduje inštalácia žiadnych špeciálnych pluginov ani rozšírení prehliadača.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/supported-web-browsers*	**SPLNIL**
	Riešenie musí umožniť obmedzenie prístupu do administrátorskej konzoly podľa definovaných verejných IP adries alebo ekvivalentných sieťových pravidiel.	***Spĺňa.*** *Cortex XSIAM umožňuje v nastavení Security Settings – Allowed Sessions definovať schválené verejné IP adresy alebo IP rozsahy, z ktorých je povolený prístup do webovej administrátorskej konzoly. Prístupy z ostatných IP adries sú odmietnuté.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Configure-security-settings*	**SPLNIL**
	Riešenie musí podporovať MFA/2FA pre administrátorov a operátorov a podrobnú správu používateľských oprávnení na báze RBAC; výhodou je aj obmedzenie oprávnení podľa rozsahu, napríklad hostiteľských skupín, tenantov alebo dátových domén.	***Spĺňa.*** *Cortex XSIAM podporuje MFA prostredníctvom podnikového poskytovateľa identity a SAML 2.0 SSO. Detailné oprávnenia sú riadené pomocou RBAC a doplnené o SBAC, ktorý umožňuje obmedziť prístup napríklad podľa endpointových skupín a tagov, zdrojov logov, dátových objektov alebo tenantov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/set-up-authentication/authenticate-users-using-sso* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/manage-user-roles-and-access-management/manage-user-scope*	**SPLNIL**
	Riešenie musí automaticky zoskupovať prepojené alerty do incidentov a priraďovať incidentom	***Spĺňa.***	**SPLNIL**

	číselné alebo ekvivalentné rizikové skóre na urýchlenie triáže a prioritizácie.	*Cortex XSIAM automaticky zoskupuje súvisiace alerty podľa kauzality, spoločných entít a priebehu útoku do incidentov/prípadov. Funkcia SmartScore priraďuje číselné skóre naliehavosti, ktoré umožňuje prioritizáciu a zrýchlenie triáže.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/case-concepts/case-grouping* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Case-scoring*	
	Riešenie musí podporovať tvorbu vlastných dashboardov z preddefinovaných widgetov a vlastných ovládacích prvkov založených na dotazoch nad zozbieranými dátami.	***Spĺňa.*** *Cortex XSIAM umožňuje vytvárať vlastné dashboardy z preddefinovaných widgetov dostupných vo Widget Library. Používateľ môže vytvárať aj vlastné widgety a vizualizácie založené na XQL dotazoch nad zozbieranými dátami vrátane filtrov a interaktívnych drill-down prvkov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/create-dashboards/create-a-dashboard* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/overview-of-dashboards-and-reports/widget-library*	**SPLNIL**
	Riešenie musí umožňovať generovanie reportov minimálne vo formáte PDF a export incidentových alebo analytických dát vo formátoch vhodných pre ďalšie analytické spracovanie, napríklad JSON, CSV, TSV alebo ekvivalent.	***Spĺňa.*** *Cortex XSIAM umožňuje generovať a distribuovať reporty vo formáte PDF, pričom analytické dáta widgetov môžu byť priložené vo formáte CSV. Incidentové dôkazy, udalosti a výsledky vyšetrovania je možné exportovať vo formáte CSV alebo TSV na ďalšie analytické spracovanie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/create-reports/create-a-report-template-from-scratch* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/evidence*	**SPLNIL**
	Riešenie musí poskytovať metriky a prehľady pre hodnotenie činnosti SOC, najmä počet incidentov, stav	***Spĺňa.*** *Cortex XSIAM poskytuje systémové SOC dashboardy zobrazujúce počet a stav incidentov, závažnosť, trendy alertov, otvorené incidenty, pracovné zaťaženie*	**SPLNIL**

	incidentov, MTTR alebo ekvivalentné metriky reakcie, trendy alertov a výkonnostné ukazovatele analytikov.	*analytikov a individuálne ukazovatele MTTR. Metriky je možné filtrovať a rozšíriť vlastnými XQL widgetmi a reportmi.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/dashboard-reference/system-dashboards* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/dashboard-reference/command-center-reference/xsiam-command-center/cases-overview*	
	Administrátorská konzola musí umožniť manuálnu zmenu závažnosti incidentu, manuálne zlúčenie súvisiacich incidentov, pridávanie komentárov a notifikovanie priradeného riešiteľa alebo skupiny riešiteľov.	***Spĺňa.*** *Administrátorská konzola Cortex XSIAM umožňuje manuálne meniť závažnosť incidentu, zlučovať súvisiace incidenty a priraďovať ich používateľovi alebo tímu riešiteľov. Podporuje komentáre, spoločné poznámky a notifikovanie riešiteľov prostredníctvom konfigurovateľných pravidiel, playbookov a integračných kanálov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/use-the-interface* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/resolve-the-case/collaborative-notes-and-comments* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services/configure-notification-forwarding*	**SPLNIL**
	Riešenie musí umožniť vizualizáciu výsledkov dotazov a prevádzkových metrík v tabuľkovej a grafickej forme a ich využitie pri tvorbe pravidelných reportov a SOC metrík.	***Spĺňa.*** *Cortex XSIAM umožňuje zobrazovať výsledky XQL dotazov v tabuľkovej forme aj prostredníctvom grafov a ďalších vizualizácií. Výsledky je možné uložiť ako XQL widgety a opakovane ich používať v SOC dashboardoch, pravidelných reportoch a prevádzkových metrikách.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/how-to-build-xql-queries/review-xql-query-results*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/advanced-configuration/create-custom-widgets/create-xql-widgets	
AI a analytická podpora	Riešenie môže obsahovať zabudovaného asistenta založeného na umelej inteligencii alebo ekvivalentný analytický mechanizmus, ktorý podporuje triáž incidentov, analýzu hrozieb, návrh reakčných krokov a prácu v prirodzenom jazyku pri rešpektovaní používateľských oprávnení.	***Spĺňa.*** *Cortex XSIAM obsahuje Cortex Agentic Assistant, ktorý v prirodzenom jazyku podporuje triáž incidentov, sumarizáciu a analýzu hrozieb, tvorbu dotazov a návrh vyšetrovacích alebo nápravných krokov. Prístup k agentom, akciám a dátam je riadený prostredníctvom RBAC a rozsahu oprávnení používateľa.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/overview-of-cases/resolving-cases-with-ai https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/configure-the-cortex-agentic-assistant-1/agentic-assistant-role-based-access-control	**SPLNIL**
	Ak riešenie využíva AI alebo strojové učenie, musí byť použiteľné na detekciu anomálií, prispôsobenie analytiky špecifikám prostredia obstarávateľa a identifikáciu nezvyčajných aktivít v aktuálnych aj historických dátach.	***Spĺňa.*** *Cortex XSIAM využíva ML a UEBA na vytváranie behaviorálnych profilov používateľov, endpointov a ďalších entít špecifických pre prostredie obstarávateľa. Aktuálnu aktivitu porovnáva s historickým správaním a podobnými entitami, čím identifikuje anomálie a neobvyklé aktivity; nad uloženými dátami je možné vykonávať aj vlastnú ML analýzu.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/analytics/analytics-overview/analytics-engine https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/notebooks	**SPLNIL**
	V prípade využitia AI funkcionalít musí byť zabezpečená dôvernosť zákazníckych dát, rešpektovanie RBAC a spracovanie v súlade so zmluvne dohodnutými pravidlami ochrany dát.	***Spĺňa.*** *AI funkcionality Cortex XSIAM rešpektujú RBAC a používateľovi sprístupňujú iba dáta a operácie v rozsahu jeho oprávnení. Zákaznícke dáta sú chránené bezpečnostnými opatreniami platformy a spracúvané podľa zmluvy, pokynov zákazníka, príslušných Privacy Datasheets a Customer Data Processing Addendum (DPA) vrátane záväzkov dôvernosti.*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/agentic-ai-in-cortex-xsiam/agentic-assistant-security	
Integrácie a dátové zdroje	Riešenie musí podporovať integráciu s minimálne 100 rôznymi typmi dátových zdrojov alebo bezpečnostných technológií prostredníctvom produkčne podporovaných konektorov, API, syslogu, agentového zberu, cloud konektorov alebo ekvivalentných mechanizmov.	***Spĺňa.*** *Cortex XSIAM podporuje viac než 1 000 pripravených integrácií, čím výrazne prekračuje požadovaných 100 technológií. Zber a integrácia sú realizované prostredníctvom natívnych a dodávateľských konektorov, REST API, Syslogu, agentov a kolektorov, Broker VM, cloudových konektorov a certifikovaných balíkov Cortex Marketplace.* *https://www.paloaltonetworks.com/company/press/2024/palo-alto-networks-unveils-enhanced-flexibility-and-customization-with-cortex-xsiam--the-precision-ai-powered-soc-platform* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/what-are-cortex-xsiam-data-sources*	**SPLNIL**
	Integračné definície, konektory alebo skripty musia byť spravované z hlavnej konzoly platformy, dokumentované a aktualizované dodávateľom alebo výrobcom počas trvania podpory.	***Spĺňa.*** *Integračné konektory, skripty a súvisiace playbooky sú v Cortex XSIAM distribuované ako Content Packs a centrálne spravované z konzoly v častiach Marketplace a Data Sources & Integrations. Balíky obsahujú dokumentáciu, autora, podporovanú verziu, závislosti a históriu verzií; konzola umožňuje ich aktualizáciu, kontrolovaný návrat na staršiu verziu a upozorňuje na dostupné opravy alebo nové vydania od Palo Alto Networks alebo príslušného podporujúceho výrobcu.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Manage-content-packs* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/integrations*	**SPLNIL**
	Riešenie musí podporovať agentový aj bezagentový zber logov vrátane syslogu a REST API a musí umožniť filtrovanie nežiaducich logov na úrovni zberu, spracovania alebo vizualizácie.	***Spĺňa.*** *Cortex XSIAM podporuje agentový zber prostredníctvom Cortex XDR Agent a XDR Collector aj bezagentový zber cez Broker VM, Syslog Collector, cloudové a REST API konektory. Nežiaduce záznamy je možné filtrovať už pred prenosom zo zberového komponentu, pri parsovaní pomocou podmienok drop, ako aj pri zobrazovaní pomocou XQL filtrov.*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/what-are-cortex-xsiam-data-sources https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/parsing-rules/parsing-rules-file-structure-and-syntax/collect	
	Riešenie musí podporovať spracovanie viacriadkových logov a spoločný dátový model alebo ekvivalentnú normalizačnú vrstvu pre koreláciu údajov zo všetkých relevantných zdrojov.	***Spĺňa.*** *Cortex XSIAM podporuje jedno- aj viacriadkové logy; pri surových logoch je možné začiatok viacriadkovej udalosti definovať regulárnym výrazom. Prijaté dáta sa pomocou parsovacích a modelovacích pravidiel automaticky normalizujú do spoločného Cortex Data Model (XDM), ktorý umožňuje jednotné vyhľadávanie, detekciu a koreláciu naprieč zdrojmi.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/xdr-collectors/xdr-collector-profiles/add-an-xdr-collector-profile-for-linux https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/standard-data-sources	**SPLNIL**
	Riešenie musí umožniť automatické obohacovanie telemetrie z pripojených zdrojov o kontext aktív, používateľov, identít, hrozieb, zraniteľností alebo reputácie.	***Spĺňa.*** *Cortex XSIAM automaticky koreluje telemetriu s jednotným kontextom aktív, endpointov, používateľov a identít. Indikátory sú automaticky extrahované a obohacované pomocou Unit 42 Threat Intelligence a pripojených zdrojov o reputáciu, informácie o hrozbách a ďalší kontext; automatizačné playbooky umožňujú doplniť aj zraniteľnosti a údaje z externých systémov.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/indicator-extraction https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/associated-assets-and-artifacts	**SPLNIL**
	Riešenie musí podporovať integráciu s adresárovými a identitnými službami vrátane lokálnych a cloudových identitných	***Spĺňa.*** *Cortex XSIAM s modulom ITDR podporuje integráciu s lokálnym Active Directory aj cloudovými a SaaS identitnými službami, napríklad Microsoft Entra ID a Okta. Získané informácie o používateľoch, skupinách, organizačných atribútoch a*	**SPLNIL**

	prostredí, minimálne na účely obohacovania údajov o používateľoch, endpointoch a organizačnej štruktúre.	*identitách sa korelujú s endpointovou telemetriou a využívajú na obohacovanie detekcií a vyšetrovania.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/asset-management/asset-classes/identity-assets* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr/active-directory-security-posture-management*	
	Riešenie musí podporovať integráciu s ticketing/ITSM systémami, systémami správy zraniteľností, reputačnými službami, sandboxom a ďalšími bezpečnostnými nástrojmi prostredníctvom natívnych konektorov, API alebo ekvivalentných integračných mechanizmov.	***Spĺňa.*** *Cortex XSIAM podporuje integrácie s ticketing/ITSM systémami, nástrojmi na správu zraniteľností, reputačnými a threat-intelligence službami, sandboxmi a ďalšími bezpečnostnými technológiami. Integrácie sa realizujú prostredníctvom podporovaných konektorov a obsahových balíkov Cortex Marketplace, REST API a automatizačných playbookov.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Integration-use-cases* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/marketplace/cortex-marketplace*	**SPLNIL**
	Riešenie musí podporovať spracovanie sieťovej telemetrie alebo tokových dát, napríklad NetFlow, IPFIX alebo ekvivalentných formátov, ak sú tieto dáta súčasťou prostredia obstarávateľa.	***Spĺňa.*** *Cortex XSIAM umožňuje prostredníctvom lokálneho komponentu Broker VM zbierať a spracovávať sieťové tokové dáta. NetFlow Collector podporuje formáty NetFlow v5, NetFlow v9 a IPFIX a odovzdáva ich do platformy na analýzu, vyhľadávanie a koreláciu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets/activate-netflow-collector*	**SPLNIL**
	Riešenie musí podporovať napojenie na zdroje identít minimálne typu adresárová služba, identity provider, autentizačná služba a RADIUS alebo ekvivalentný zdroj autentizačných údajov na	***Spĺňa.*** *Ponúkaný Cortex XSIAM s modulom ITDR podporuje napojenie na adresárové služby a identity providery, napríklad Microsoft AD/Entra ID, OpenLDAP, Okta, OneLogin a PingFederate. Autentizačné udalosti zo systémov RADIUS, NAC, VPN alebo ekvivalentných zdrojov možno prijímať prostredníctvom konektorov, API alebo Syslog Collectora; získané dáta sa používajú na obohatenie detekcií, incidentov a rizikových skóre identít.*	**SPLNIL**

	účely obohatenia detekcií a incidentov.	*https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/generic-on-premise-data-collectors/broker-vm-data-collector-applets/syslog-collector-applet/pingfederate/ingest-authentication-logs-from-pingfederate* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/asset-management/manage-asset-scores*	
	Riešenie musí umožniť obohatenie udalostí zo sieťových a perimetrových bezpečnostných prvkov o endpointový a používateľský kontext tak, aby bolo možné identifikovať dotknuté zariadenie, používateľa, proces a súvisiacu postupnosť udalostí.	***Spĺňa.*** *Cortex XSIAM koreluje a prepája udalosti z firewallov a ďalších sieťových zdrojov s endpointovou a používateľskou telemetriou. Network Causality View umožňuje v rámci incidentu identifikovať dotknutý endpoint, používateľa, proces vrátane PID, cesty a hash hodnoty a zobraziť súvisiacu príčinnú postupnosť udalostí.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view/network-causality-view* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view*	**SPLNIL**
Automatizácia a reakcie	Riešenie musí umožniť spúšťanie pokročilých viacstupňových automatizácií vo forme playbookov alebo workflowov ako reakciu na alerty, incidenty, IOC, identitné udalosti alebo definované korelačné pravidlá.	***Spĺňa.*** *Cortex XSIAM podporuje vizuálne viacstupňové playbooky s podmienkami, skriptmi, integračnými príkazmi, slučkami a vnorenými sub-playbookmi. Playbooky možno spúšťať automaticky podľa vlastností alertu alebo incidentu, vrátane alertov vytvorených korelačnými pravidlami, IOC analýzou alebo ITDR, prípadne manuálne počas vyšetrovania.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/playbooks-overview* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam-developer-guide/cortex-xsiam-development-guide/playbooks*	**SPLNIL**
	Riešenie musí byť dodané s predpripravenými playbookmi alebo automatizačnými postupmi	***Spĺňa.*** *Cortex XSIAM obsahuje predpripravené playbooky a automatizačné postupy pre bežné bezpečnostné scenáre a podporované integrácie, distribuované aj*	**SPLNIL**

	pre bežné bezpečnostné scenáre a integrované systémy, s možnosťou ich úpravy podľa prostredia obstarávateľa.	*prostredníctvom obsahových balíkov Cortex Marketplace. Playbooky možno kopírovať a upravovať podľa prostredia obstarávateľa, prípadne vytvárať vlastné workflowy.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook/choose-from-existing-playbooks-or-create-your-own* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/marketplace/cortex-marketplace*	
	Riešenie musí umožniť testovanie alebo overenie automatizačných scenárov pred ich produkčným nasadením alebo ekvivalentný mechanizmus znižujúci riziko neželanej reakcie.	***Spĺňa.*** *Cortex XSIAM obsahuje debugger playbookov, ktorý umožňuje automatizáciu spustiť s testovacím „mock“ alertom, používať breakpointy a kontrolovať vstupy, výstupy a kontext jednotlivých krokov. Pred aktivovaním produkčného spúšťača možno playbook overiť, ladiť a verzovať, čím sa znižuje riziko nežiaducej reakcie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam-developer-guide/cortex-xsiam-development-guide/integrations-and-scripts/create-a-sample-integration/test-the-integration*	**SPLNIL**
	Riešenie musí podporovať automatické oznamovanie kritických incidentov a automatické e-mailové alebo integračné notifikácie na základe definovaných pravidiel.	***Spĺňa.*** *Cortex XSIAM umožňuje vytvárať pravidlá automatických notifikácií podľa závažnosti a ďalších atribútov alertov alebo incidentov, vrátane okamžitého oznamovania kritických udalostí. Notifikácie možno odosielať e-mailom alebo prostredníctvom integrácií, napríklad webhooku, Slacku, syslogu či Splunku.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services/configure-notification-forwarding* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services/configure-external-applications-for-forwarding/forward-notifications-to-webhook*	**SPLNIL**
	Riešenie musí ako súčasť reakcie na endpointový incident	***Spĺňa.***	**SPLNIL**

	podporovať primerané reakčné úkony prostredníctvom natívnych schopností alebo integrácií, najmä izoláciu endpointu, ukončenie procesu, zber dodatočných dát, karanténu alebo odstránenie škodlivého artefaktu, vyhľadanie súboru na ďalších endpointoch a spustenie definovaného skriptu alebo príkazu s auditnou stopou.	*Cortex XSIAM prostredníctvom natívneho Cortex XDR agenta podporuje izoláciu endpointu, ukončenie procesu alebo procesného reťazca, získanie súborov a diagnostických dát, karanténu alebo odstránenie škodlivého súboru, jeho vyhľadanie a odstránenie na ďalších endpointoch a spustenie definovaných agentových skriptov. Úkony možno vykonať manuálne alebo playbookom; Action Center eviduje iniciátora, čas, priebeh a výsledok akcie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/isolate-an-endpoint* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/remediate-changes-from-malicious-activity* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/run-agent-scripts-on-an-endpoint* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/overview-of-the-action-center/action-center-reference-information*	
	Riešenie musí umožniť spustenie reakčných skriptov alebo príkazov na jednom alebo viacerých endpointoch naprieč podporovanými operačnými systémami, minimálne pre Windows a Linux/macOS prostredie, s centrálnym auditom spustenia a výsledku.	***Spĺňa.*** *Cortex XSIAM umožňuje z centrálnej Agent Scripts Library spúšťať definované skripty na jednom alebo viacerých endpointoch so systémami Windows, Linux a macOS. Action Center a história vykonania centrálne evidujú iniciátora, cieľové endpointy, čas, stav a výsledok spustenia; prístup je riadený prostredníctvom RBAC.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/run-agent-scripts-on-an-endpoint* *https://www.paloaltonetworks.com/blog/2020/04/cortex-network-visibility/* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/overview-of-the-action-center/action-center-reference-information*	**SPLNIL**

	Riešenie musí obsahovať alebo podporovať preddefinovanú sadu reakčných a zberových skriptov na rýchly zber dát, analýzu, servisné zásahy a blokovanie prebiehajúceho útoku na endpointoch.	***Spĺňa.*** *Cortex XSIAM obsahuje centrálne spravovanú Agent Scripts Library s preddefinovanými skriptmi výrobcu, napríklad na výpis procesov a ich využitia zdrojov, kontrolu existencie súboru, zoznam adresárov a odstránenie súboru. Sadu možno rozširovať vlastnými skriptmi a kombinovať s natívnymi reakčnými úkonmi, ako sú izolácia endpointu, ukončenie procesu, karanténa a zber dodatočných dát.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/run-agent-scripts-on-an-endpoint* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/overview-of-the-action-center*	**SPLNIL**
	Riešenie musí umožniť automatickú alebo manuálnu vzdialenú izoláciu jedného alebo viacerých endpointov tak, aby endpoint komunikoval iba s platformou alebo administrátorom definovanými cieľmi.	***Spĺňa.*** *Cortex XSIAM umožňuje manuálnu aj automatizovanú izoláciu jedného alebo viacerých endpointov prostredníctvom konzoly, playbooku alebo REST API. Izolovaný endpoint štandardne komunikuje iba s platformou Cortex XSIAM; pomocou Network Isolation Allow List možno povoliť administrátorom definované procesy, aplikácie, cieľové IP adresy a porty.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/isolate-an-endpoint* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM-REST-API/Isolate-Endpoints*	**SPLNIL**
Detekcia a ochranné mechanizmy	Riešenie musí podporovať detekciu hrozieb v reálnom čase aj retrospektívne nad historickými dátami, vrátane automatickej	***Spĺňa.*** *Cortex XSIAM podporuje detekciu v reálnom čase prostredníctvom behaviorálnej analytiky, ML a real-time korelačných pravidiel. Retenované historické dáta možno retrospektívne analyzovať pomocou XQL a plánovaných korelačných pravidiel.*	**SPLNIL**

	korelácie medzi rôznymi typmi zdrojových dát na identifikáciu skrytých alebo viacstupňových útokov.	*Platforma automaticky koreluje udalosti z viacerých zdrojov a zoskupuje súvisiace detekcie podľa útoku alebo entity, čím odhaľuje skryté a viacstupňové útoky.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule/create-a-correlation-rule* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/case-concepts/case-grouping*	
	Riešenie musí podporovať behaviorálnu detekciu podozrivého používania legitímnych operačných, administrátorských a skriptovacích nástrojov, vrátane analýzy reťazcov príčin a následkov a mapovania na taktiky, techniky a procedúry útočníkov.	***Spĺňa.*** *Cortex XSIAM využíva Behavioral Threat Protection, behaviorálnu analytiku a BIOC pravidlá na detekciu podozrivého zneužitia legitímnych nástrojov, napríklad PowerShell, rundll32 alebo MSBuild, podľa procesného správania, príkazových riadkov a neobvyklých väzieb procesov. Causality View zobrazuje celý reťazec príčin a následkov a priraďuje detekciám taktiky a techniky MITRE ATT&CK, čím poskytuje kontext použitých TTP.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/endpoint-protection/malware-protection* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view* *https://www.paloaltonetworks.com/blog/security-operations/stopping-powershell-without-powershell/*	**SPLNIL**
	Riešenie musí umožniť využitie sandboxovej analýzy alebo ekvivalentného mechanizmu na vyhodnotenie podozrivých súborov, URL alebo artefaktov súvisiacich s incidentom a musí umožniť zobrazenie alebo export výsledku analýzy, ak je funkcionalita	***Spĺňa.*** *Cortex XSIAM využíva WildFire na vyhodnotenie podozrivých súborov a podporuje integračné sandboxové scenáre na odoslanie súboru alebo URL na detonáciu, získanie reportu a vyhľadanie predchádzajúcej analýzy podľa hash hodnoty alebo URL. Verdikt a výsledky sú dostupné pri artefakte alebo incidente; WildFire report možno zobraziť a stiahnuť.*	**SPLNIL**

	súčasťou dodávky alebo dostupná integračne.	*https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/integrations/integration-use-cases* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-artifacts-and-assets/investigate-a-file-and-process-hash* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view*	
	Riešenie musí poskytovať inventár chránených endpointov s údajmi o zariadení, používateľovi, operačnom systéme a relevantných aplikáciách alebo bezpečnostných parametroch.	***Spĺňa.*** *Ponúkaná licencia Cortex XSIAM Enterprise zahŕňa Cortex XDR agentov s funkcionalitou Host Insights. Centrálne obrazovky All Endpoints a Host Inventory poskytujú údaje o zariadení a hardvéri, IP adresách, používateľoch a skupinách, operačnom systéme, nainštalovaných aplikáciách, službách, ovládačoch, verzii a stave agenta, priradenej politike a poslednej komunikácii.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/harden-endpoint-security/host-inventory* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/manage-endpoints* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses/license-allocation*	**SPLNIL**
	Riešenie musí podporovať detekciu na základe baseline správania používateľov, endpointov, procesov a sieťovej komunikácie a vyhodnocovať odchýlky pomocou behaviorálnej analytiky alebo strojového učenia.	***Spĺňa.*** *Cortex XSIAM Analytics Engine vytvára dynamický baseline správania z priebežne prijímanej endpointovej, používateľskej a sieťovej telemetrie vrátane aktivity procesov. Pomocou strojového učenia, UEBA a Analytics BIOC pravidiel vyhodnocuje odchýlky od obvyklého správania používateľov, endpointov a ďalších entít. Ponúkaný modul ITDR rozširuje baseline o identitnú analytiku.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/analytics/analytics-overview/analytics-engine*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/cortex-xsiam-analytics/enable-the-analytics-engine-and-identity-analytics*	
	Riešenie musí podporovať detekciu podozrivých scenárov minimálne v rozsahu DNS tunneling alebo neštandardné DNS správanie, skenovanie portov alebo okolitých staníc, brute-force útoky, zneužitie PowerShellu vrátane obfuskácie a podozrivých príkazov, pokusy o získanie prihlasovacích údajov a spúšťanie nových alebo neštandardných služieb.	***Spĺňa.*** *Cortex XSIAM pri dostupnosti príslušnej endpointovej, DNS, sieťovej a autentizačnej telemetrie poskytuje preddefinované Analytics Alerts, Analytics BIOC a Behavioral Threat Protection detekcie pre:* • *DNS Tunneling, Suspicious DNS Traffic a náhodne vyzerajúce domény,* • *Port Scan, Port Sweep a abnormálne skenovanie SMB/RPC staníc,* • *brute-force, password-spray a opakované zlyhania NTLM, SSO, VPN, SSH alebo lokálnych účtov,* • *podozrivé, kódované a obfuskované PowerShell príkazy,* • *credential dumping, DCSync, prístup k prihlasovacím údajom a súborom s tajomstvami,* • *spustenie novej alebo neobvyklej služby.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Analytics-Alert-Reference-by-Alert-name/Cortex-XSIAM-Analytics-Alert-Reference* *https://www.paloaltonetworks.com/blog/security-operations/stopping-powershell-without-powershell/*	**SPLNIL**
	Riešenie musí umožniť vytváranie používateľských IOC a behaviorálnych IOC minimálne podľa cesty k súboru, názvu súboru, domény, IP adresy, hashu, registračných zmien, spúšťania procesov alebo reťazca súvisiacich udalostí.	***Spĺňa.*** *Cortex XSIAM umožňuje manuálne vytváranie aj hromadný import vlastných IOC pravidiel pre hash, IP adresu a doménu. Podmienky podľa názvu a cesty súboru, registračných zmien, spúšťania a vzťahov procesov alebo sieťovej aktivity sa definujú ako BIOC pravidlá. Viacstupňové reťazce súvisiacich udalostí možno pokryť XQL korelačnými pravidlami.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-an-ioc/create-an-ioc-rule*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-bioc https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule	
Pokročilé vyhľadávanie a korelácia	Riešenie musí podporovať pokročilé vyhľadávanie telemetrie, alertov a incidentov minimálne pomocou sprievodcu, manuálne prostredníctvom dotazov v konzole a programovo cez API.	***Spĺňa.*** *Cortex XSIAM poskytuje:* • *sprievodcu Query Templates s predpripravenými vyhľadávaniami pre endpointové, sieťové, identitné, cloudové a voľne textové dáta,* • *manuálny editor XQL v konzole na pokročilé dotazy nad telemetriou, alertmi a incidentmi,* • *REST API na spustenie XQL dotazu, získanie výsledkov a programové vyhľadávanie alertov a incidentov.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/issue-investigation-actions/query-case-and-issue-data https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM-REST-API/Get-XQL-query-results	**SPLNIL**
	Vyhľadávanie musí podporovať viac argumentové dotazy, zástupné znaky, regulárne výrazy alebo ekvivalentné pokročilé query mechanizmy, filtrovanie podľa polí aj voľné textové vyhľadávanie bez povinnosti špecifikovať konkrétne pole.	***Spĺňa.*** *Cortex Query Language (XQL) podporuje viacpodmienkové dotazy s operátormi AND, OR a NOT, filtrovanie podľa konkrétnych polí, zástupný znak *, regulárne výrazy implementované pomocou RE2 a ďalšie mechanizmy, napríklad join, union a agregácie. Šablóna Free Text umožňuje vyhľadávať reťazce v dátach bez povinnosti určiť konkrétne pole.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/get-started-with-xql/supported-operators https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/get-started-with-xql/understanding-string-manipulation-in-xql	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/query-builder-templates/run-a-free-text-query	
	Riešenie musí umožniť ukladať dotazy do súkromnej používateľskej knižnice alebo zdieľanej knižnice dostupnej oprávneným používateľom platformy.	***Spĺňa.*** *Cortex XSIAM umožňuje ukladať XQL dotazy do osobnej používateľskej knižnice alebo ich zdieľať v centrálnej Query Library. Vlastník môže nastaviť prístup pre konkrétnych používateľov, skupiny používateľov alebo API kľúče; oprávnenia na zobrazenie a úpravu sú riadené pomocou RBAC a prístupu na úrovni objektu.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/manage-user-roles-and-access-management/manage-access-to-objects/manage-access-to-saved-queries https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/role-based-access-control/investigation-and-response-permissions/search-permissions/query-library-permissions	**SPLNIL**
	Riešenie musí umožniť plánované alebo jednorazové spúšťanie dotazov a využitie výsledkov dotazov na pravidelné reporty, korelačné pravidlá alebo generovanie alertov.	***Spĺňa.*** *XQL dotazy možno v Cortex XSIAM spúšťať jednorazovo z Query Buildera alebo nastaviť ich opakované vykonávanie podľa harmonogramu. Výsledky možno použiť v XQL widgetoch a pravidelných reportoch alebo dotaz transformovať na plánované či real-time korelačné pravidlo, ktoré pri splnení podmienok vytvorí alert.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/manage-scheduled-queries https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/advanced-configuration/create-custom-widgets/create-xql-widgets https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule/create-a-correlation-rule	**SPLNIL**
	Riešenie musí umožniť vytvárať korelačné pravidlá pracujúce v reálnom čase aj retrospektívne nad	***Spĺňa.*** *Cortex XSIAM umožňuje oprávneným používateľom vytvárať vlastné korelačné pravidlá pomocou XQL. Pravidlo môže pracovať v režime Real Time nad práve*	**SPLNIL**

	historickými dátami, vrátane pravidiel vytvorených obstarávateľom.	*ingestovanými dátami alebo ako Scheduled pravidlo s definovaným harmonogramom a časovým rozsahom nad historickými dátami; plánované pravidlo možno spustiť aj jednorazovo.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule/create-a-correlation-rule* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule/manage-correlation-rules*	
	Výsledky dotazov musia byť exportovateľné minimálne v textovom, tabuľkovom alebo strojovo spracovateľnom formáte a vizualizovateľné v tabuľkovej aj grafickej forme.	***Spĺňa.*** *Cortex XSIAM umožňuje zobrazovať výsledky XQL dotazov v tabuľkovej forme, exportovať ich na ďalšie spracovanie a získavať ich cez REST API v strojovo spracovateľnom formáte. Výsledky možno vizualizovať grafmi a použiť vo widgetoch, dashboardoch a reportoch.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/how-to-build-xql-queries/review-xql-query-results* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/how-to-build-xql-queries/graph-query-results* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM-REST-API/Get-XQL-query-results*	**SPLNIL**
Zber a ingest dát	Príjem a spracovanie bezpečnostných dát prostredníctvom štandardizovaných mechanizmov, najmä syslog, API, agentový zber, cloud konektory, event streaming,	***Spĺňa.*** *Cortex XSIAM podporuje príjem a spracovanie bezpečnostných dát prostredníctvom syslogu, HTTP/REST API, endpointových agentov, cloudových a API konektorov, webhookov a event streamingu cez Apache Kafka. Súborový a dávkový zber zabezpečujú CSV, Files and Folders, FTP a cloudové objektové konektory, napríklad Amazon S3.*	**SPLNIL**

	webhook, súborový alebo batch import.	*https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Cortex-XSIAM-Data-Sources* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/vendor-specific-data-sources-and-connectors/http-log-collector* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Activate-Apache-Kafka-Collector* *https://xsoar.pan.dev/docs/reference/integrations/generic-webhook*	
	Normalizácia ingestovaných dát do jednotného dátového modelu alebo ekvivalentnej štruktúry použiteľnej na koreláciu, vyhľadávanie, reporting, detekciu, automatizáciu a audit.	***Spĺňa.*** *Cortex XSIAM normalizuje ingestované dáta prostredníctvom Data Model Rules do jednotného Cortex Data Modelu (XDM). Normalizované polia sú následne použiteľné naprieč zdrojmi na koreláciu, XQL vyhľadávanie, detekčné pravidlá, reporting, automatizáciu a auditné procesy.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/data-model-rules* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Data-Model-Schema-Guide-for-Cortex-XSIAM-with-Cortex-Cloud/Introduction* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/how-to-build-xql-queries*	**SPLNIL**
	Podpora onboardingu vlastných alebo neštandardných logových zdrojov vrátane mapovania polí, úprav parserov alebo transformačných pravidiel, ak je to potrebné.	***Spĺňa.*** *Cortex XSIAM umožňuje onboarding vlastných a neštandardných logových zdrojov prostredníctvom generických zberových mechanizmov. Vlastné Parsing Rules založené na XQL umožňujú parsovanie a transformáciu dát; Data Model Rules zabezpečujú mapovanie polí do jednotného modelu XDM.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/parsing-rules/create-parsing-rules* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/data-model-rules*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/vendor-specific-data-sources-and-connectors/http-log-collector	
	Monitoring stavu dátových zdrojov, konektorov a ingest pipeline vrátane upozornení na výpadok, oneskorenie, chybovosť, pokles objemu dát alebo prekročenie kapacitných limitov.	***Spĺňa.*** *Cortex XSIAM centrálne monitoruje stav pripojenia a poslednú synchronizáciu dátových zdrojov a konektorov. Ingestion Monitoring sleduje objem, rýchlosť, oneskorenie a aktuálnosť dát, pričom identifikuje výpadok príjmu alebo významný pokles oproti baseline. Nad ingest metrikami možno vytvárať korelačné pravidlá a upozornenia na chyby, oneskorenie a prekročenie definovaných kapacitných prahov.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/about-health-issues/monitor-data-ingestion-health https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/overview-of-data-ingestion-metrics https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/overview-of-data-ingestion-metrics/creating-correlation-rules-to-monitor-data-ingestion-health	**SPLNIL**
	Možnosť filtrovania, transformácie, smerovania alebo obohatenia dát pred uložením, koreláciou, detekciou alebo forwardovaním.	***Spĺňa.*** *Cortex XSIAM umožňuje pomocou XQL Parsing Rules filtrovať alebo zahadzovať nepotrebné logy a transformovať ich polia už počas zberu a ingestu. Sekcie INGEST umožňujú smerovanie výsledkov do určených datasetov, zatiaľ čo Data Model Rules a lookup datasety zabezpečujú normalizáciu a obohatenie dát pred koreláciou, detekciou a ďalším spracovaním. Pri endpointovom forwardovaní je podporované riadenie zahrnutých a vylúčených polí podľa typu udalosti.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/parsing-rules/parsing-rules-file-structure-and-syntax/collect	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/parsing-rules/parsing-rules-file-structure-and-syntax/ingest *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/data-model-rules* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/manage-event-forwarding/endpoints-event-forwarding-included-excluded-fields-by-event-type*	
	Podpora spracovania pôvodného eventu aj normalizovanej reprezentácie tak, aby bolo možné auditné overenie zdrojovej udalosti.	***Spĺňa.*** *Cortex XSIAM uchováva pôvodné udalosti v raw datasetoch spravidla pomenovaných <vendor>_<product>_raw. Súčasne ich prostredníctvom Data Model Rules sprístupňuje v normalizovanej reprezentácii Cortex Data Model (XDM). Raw aj normalizované dáta sú vyhľadateľné pomocou XQL, čo umožňuje porovnanie a auditné overenie zdrojovej udalosti.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/dataset-management/what-are-datasets* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/parsing-rules/create-parsing-rules* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/data-model-rules*	**SPLNIL**
	Podpora dátových zdrojov minimálne v rozsahu endpoint, firewall, proxy, identity provider, adresárová služba, cloudová platforma, SaaS aplikácia, e-mail security, DNS, DHCP, VPN, EDR/XDR a aplikačné logy.	***Spĺňa.*** *Cortex XSIAM podporuje zber dát z endpointov, firewallov, proxy a VPN riešení, identity providerov a adresárových služieb, cloudových platforiem, SaaS aplikácií, e-mailovej bezpečnosti, DNS, DHCP, EDR/XDR nástrojov a aplikačných logov. Podpora je realizovaná prostredníctvom Cortex XDR agentov, natívnych konektorov, cloudových integrácií a štandardných mechanizmov, ako sú syslog, API, HTTP, Filebeat a Broker VM kolektory.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/what-are-cortex-xsiam-data-sources*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/vendor-specific-data-sources-and-connectors *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/standard-data-sources* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/cloud-service-provider-csp-onboarding*	
Endpoint telemetria	Zber a analýza endpointových udalostí minimálne v rozsahu procesy, súbory, sieťová komunikácia, používateľské aktivity, skripty, zmeny konfigurácie, bezpečnostné alerty a indikátory kompromitácie.	***Spĺňa.*** *Cortex XDR agent zbiera a analyzuje udalosti procesov, súborov, sieťových spojení, používateľov, príkazov a skriptov, ako aj zmeny registrov a konfigurácie. Súčasťou spracovania sú bezpečnostné alerty, IOC a behaviorálne udalosti.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/install-cortex-xdr-agents/endpoint-data-collection* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles*	**SPLNIL**
	Korelácia endpointovej telemetrie s dátami zo sieťových, cloudových, identitných, aplikačných a ďalších bezpečnostných zdrojov.	***Spĺňa.*** *Cortex XSIAM koreluje endpointovú telemetriu s udalosťami zo sieťových, cloudových, identitných, aplikačných a ďalších bezpečnostných zdrojov. Korelácia je vykonávaná analytickými mechanizmami platformy a XQL korelačnými pravidlami nad spoločnou dátovou vrstvou.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule*	**SPLNIL**
	Vyšetrovanie incidentov na úrovni endpointu vrátane časovej osi udalostí, dotknutých používateľov, procesov, súborov, IP adries, domén, hashov a ďalších entít.	***Spĺňa.*** *Causality View a Timeline poskytujú chronologické vyšetrovanie endpointových udalostí vrátane dotknutých používateľov, procesov, súborov, IP adries, domén, hashov a súvisiacich entít.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view/timeline	
	Identifikácia postihnutých endpointov, rozsahu incidentu a súvisiacich entít v rámci jedného incidentového alebo vyšetrovacieho pohľadu.	***Spĺňa.*** *Cortex XSIAM zobrazuje postihnuté endpointy, používateľov, súvisiace entity a reťazec príčin a následkov v jednotnom Case/Issue a Causality pohľade. Analytik tak môže určiť rozsah incidentu a vzťahy medzi jednotlivými udalosťami.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view	**SPLNIL**
	Endpointový agent musí podporovať minimálne operačné systémy MS Windows 11, aktuálne podporované verzie MS Windows Server, vybrané enterprise distribúcie Linuxu a macOS počas obdobia ich výrobcom podporovaného životného cyklu.	***Spĺňa.*** *Cortex XDR agent podporuje Windows 11, podporované vydania Windows Server, macOS a vybrané enterprise distribúcie Linuxu, napríklad Red Hat Enterprise Linux a Ubuntu. Podporované kombinácie operačného systému a verzie agenta sú priebežne aktualizované v Compatibility Matrix výrobcu.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix/Windows-11 https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix/Windows-Server https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix/Red-Hat-Enterprise-Linux https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix/Ubuntu	**SPLNIL**
	Riešenie musí umožňovať generovanie a distribúciu inštalačných balíkov agentov vo formátoch vhodných pre podporované operačné systémy, napríklad MSI, RPM, DEB, SH, PKG alebo ekvivalent.	***Spĺňa.*** *Cortex XSIAM umožňuje centrálne generovať a distribuovať inštalačné balíky Cortex XDR agenta vo formátoch MSI pre Windows, PKG distribuovanom v ZIP balíku pre macOS a RPM, DEB alebo shell inštalátore pre Linux.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/install-cortex-xdr-agents/create-an-agent-installation-package	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/install-cortex-xdr-agents/deploy-installation-packages	
	Inštalácia a aktivácia endpointového agenta nesmie za bežných okolností vyžadovať reštart operačného systému, ak to konkrétny operačný systém alebo bezpečnostný modul technicky nevyžaduje.	***Spĺňa.*** *Štandardná inštalácia a aktivácia Cortex XDR agenta nevyžaduje povinný reštart operačného systému. Reštart môže byť potrebný iba pri špecifických požiadavkách operačného systému alebo aktivácii vybraných ochranných modulov a pravidiel.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/9.0/Cortex-XDR-Agent-Administrator-Guide/Install-the-Cortex-XDR-agent-for-Windows https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/manage-endpoint-protection/upgrade-cortex-xdr-agents	**SPLNIL**
	Riešenie musí umožňovať manuálne aj automatické aktualizácie agentov pre vybrané skupiny endpointov vrátane plánovania aktualizácií, riadenia paralelizmu, oneskorenia nasadenia a výberu zdroja aktualizačných balíkov.	***Spĺňa.*** *Cortex XSIAM podporuje manuálny upgrade aj automatické aktualizácie agentov podľa profilov a skupín endpointov. Možno nastaviť plán aktualizácie, oneskorené nasadenie, počet paralelných aktualizácií a zdroj balíkov, napríklad P2P, Broker VM alebo Cortex server.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/manage-endpoint-protection/upgrade-cortex-xdr-agents https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/install-cortex-xdr-agents/configure-global-agent-settings https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles	**SPLNIL**

	Riešenie musí umožňovať rozdielne konfiguračné profily agentov a bezpečnostných modulov pre skupiny endpointov alebo jednotlivé endpointy podľa prevádzkových, tenantových alebo bezpečnostných potrieb.	***Spĺňa.*** *Cortex XSIAM umožňuje vytvárať rozdielne Agent Settings, Malware, Exploit a Restrictions profily. Politiky možno priradiť dynamickým alebo statickým skupinám, prípadne konkrétnym endpointom v rámci príslušného tenanta.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/apply-profiles-to-endpoints* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles*	**SPLNIL**
	Agent musí poskytovať ochranu proti neoprávnenej deaktivácii alebo odinštalovaniu vrátane auditovania takýchto pokusov a podpory ochranného hesla, tokenu alebo ekvivalentného mechanizmu riadeného z platformy.	***Spĺňa.*** *Agent obsahuje ochranu proti manipulácii s jeho registrami a politikami. Odinštalovanie možno chrániť centrálne definovaným šifrovaným heslom alebo tokenom agenta; udalosti, ako sú zmeny politiky, upgrade a odinštalovanie, sa zaznamenávajú v Agent Audit Logs.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/manage-endpoint-protection/monitor-agent-activity* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Manage-agent-tokens*	**SPLNIL**
	Agent musí kontinuálne prenášať relevantnú endpointovú telemetriu do platformy bez toho, aby bol zber obmedzený iba na výskyt špecifickej bezpečnostnej udalosti.	***Spĺňa.*** *Funkcia Monitor and Collect Enhanced Endpoint Data zabezpečuje priebežný zber aktívnej procesnej, súborovej, sieťovej a registrovej telemetrie. Zber preto nie je obmedzený iba na okamih vzniku bezpečnostného alertu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-*	**SPLNIL**

		protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles	
	Riešenie musí podporovať automatickú alebo manuálnu izoláciu chráneného endpointu pri identifikácii hrozby, pričom musí zostať zachovaná potrebná komunikácia s platformou na účely vyšetrovania a obnovy.	***Spĺňa.*** *Endpoint možno manuálne izolovať z konzoly alebo automatizovane prostredníctvom playbooku. Izolácia zablokuje sieťovú komunikáciu okrem spojenia s Cortex XSIAM a povolených IP adries alebo procesov, čím zostáva zachovaná komunikácia potrebná na vyšetrovanie a obnovu.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Isolate-an-endpoint* *https://xsoar.pan.dev/docs/reference/playbooks/containment-plan---isolate-device*	**SPLNIL**
	Endpointová funkcionalita musí zahŕňať ochranu proti známym aj neznámym škodlivým súborom, exploitom, ransomware správaniu a podozrivým makrám alebo ekvivalentné ochranné mechanizmy dostupné pre podporované operačné systémy.	***Spĺňa.*** *Cortex XDR agent poskytuje viacvrstvovú ochranu proti známym aj neznámym škodlivým súborom, exploitom, ransomware šifrovaniu, škodlivým makrám a skriptovým útokom. Využíva lokálnu analýzu, behaviorálnu ochranu, WildFire a špecializované preventívne moduly podľa podporovaného operačného systému.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/endpoint-protection/endpoint-protection-capabilities* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/endpoint-protection/file-analysis-and-protection-flow*	**SPLNIL**
	Podpora reakčných opatrení nad endpointmi prostredníctvom natívnych schopností alebo integrácií, najmä izolácia endpointu, obmedzenie komunikácie, zber dodatočných dát alebo spustenie vyšetrovania.	***Spĺňa.*** *Cortex XSIAM poskytuje natívne reakčné opatrenia zahŕňajúce izoláciu endpointu, obmedzenie komunikácie, malware scan, získanie súborov a podporných logov, spustenie skriptov a ďalšie vyšetrovacie alebo nápravné úkony. Priebeh a výsledky akcií sú centrálne evidované v Action Center.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/overview-of-the-action-center*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/manage-endpoints	
	Funkcie zberu endpointovej telemetrie, detekcie, ochrany a reakcie na endpointoch musia byť zabezpečené jedným endpointovým agentom alebo ekvivalentným jednotným komponentom bez potreby samostatných agentov pre základné požadované funkcie.	***Spĺňa.*** *Cortex XSIAM využíva jeden Cortex XDR agent na kontinuálny zber endpointovej telemetrie, prevenciu a detekciu hrozieb a vykonávanie reakčných opatrení. Pre základné požadované funkcie nie sú potrebné samostatné endpointové agenty.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses https://www.paloaltonetworks.com/cortex/endpoint-protection	**SPLNIL**
	Endpointový agent musí byť hromadne nasaditeľný štandardnými enterprise nástrojmi, najmä prostredníctvom centralizovanej správy softvéru pre Windows a ekvivalentných nástrojov pre Linux a macOS.	***Spĺňa.*** *Inštalačné balíky Cortex XDR agenta je možné centrálne vytvárať a hromadne distribuovať štandardnými enterprise nástrojmi. Podporované sú najmä Windows MSI balíky, macOS PKG/JAMF a Linux RPM, DEB alebo shell inštalátory.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/install-cortex-xdr-agents/deploy-installation-packages	**SPLNIL**
	Endpointová telemetria musí zahŕňať minimálne údaje o používateľovi, zariadení, IP a MAC adrese, operačnom systéme, inštalovanom softvéri, procesoch, súborových operáciách, sieťových spojeniach, systémových udalostiach, prihláseniach a odhláseniach a zmenách registrov alebo konfigurácie, ak to daný operačný systém podporuje.	***Spĺňa.*** *Agent zhromažďuje údaje o používateľoch, skupinách, zariadení, hardvéri, IP a MAC adresách, operačnom systéme, aplikáciách, procesoch, súborových operáciách, sieťových spojeniach, registroch, systémových udalostiach a používateľských reláciách v rozsahu podporovanom príslušným operačným systémom.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/harden-endpoint-security/host-inventory	**SPLNIL**
	Endpointový agent nesmie za bežných okolností zásadne ovplyvňovať výkon	***Spĺňa.***	**SPLNIL**

	endpointu a nesmie narúšať prevádzku bežných VPN riešení alebo ekvivalentných vzdialených prístupových mechanizmov používaných obstarávateľom.	*Cortex XDR používa jeden ľahký agent navrhnutý na minimalizovanie vplyvu na výkon endpointu a sieťovej komunikácie. V štandardnej konfigurácii nenarúša prevádzku VPN; kompatibilita konkrétneho VPN klienta sa overuje podľa matice kompatibility výrobcu a pri pilotnom nasadení.* *https://www.paloaltonetworks.com/cortex/endpoint-protection* *https://docs.paloaltonetworks.com/compatibility-matrix/reference/cortex-xdr*	
	Riešenie musí umožňovať obmedziť alebo blokovať spúšťanie súborov podľa hash hodnoty, umiestnenia, digitálneho podpisu, dôveryhodnosti vydavateľa, allowlistu alebo blocklistu.	***Spĺňa.*** *Platforma umožňuje riadiť spúšťanie súborov pomocou allowlistu a blocklistu hashov, pravidiel podľa umiestnenia súboru a pravidiel alebo výnimiek založených na digitálnom podpise a dôveryhodnom vydavateľovi.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-files/manage-file-execution* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-restrictions-prevention-profiles*	**SPLNIL**
	Riešenie musí podporovať kontrolu alebo overenie šifrovania disku endpointu minimálne pre Windows a macOS a správu lokálnych firewallových pravidiel endpointu, ak to daný operačný systém podporuje.	***Spĺňa.*** *Cortex XSIAM poskytuje kontrolu stavu šifrovania diskov prostredníctvom BitLocker pre Windows a FileVault pre macOS. Súčasne umožňuje centrálne definovať a aplikovať pravidlá lokálneho firewallu na podporovaných endpointoch.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/harden-endpoint-security* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/harden-endpoint-security/host-firewall*	**SPLNIL**
	Riešenie musí poskytovať inventár endpointov vrátane hardvérových údajov, operačného systému, aplikácií, lokálnych účtov, členstva v skupinách a informácií	***Spĺňa.*** *Host Inventory poskytuje inventár hardvéru, operačných systémov, nainštalovaných aplikácií, používateľov, lokálnych účtov a skupín. Členstvo*	**SPLNIL**

	využiteľných na identifikáciu lokálnych administrátorov.	*lokálnych účtov v administrátorských skupinách umožňuje identifikovať lokálnych administrátorov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/harden-endpoint-security/host-inventory* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles*	
	Riešenie musí umožňovať riadenie používania prenosných úložísk alebo iných periférnych zariadení, najmä USB zariadení, a ak je podporované, aj riadenie vybraných Bluetooth zariadení podľa typu, výrobcu alebo iných atribútov.	***Spĺňa.*** *Device Control umožňuje na podporovaných Windows a macOS endpointoch povoliť, zablokovať alebo nastaviť režim iba na čítanie pre USB a podporované Bluetooth zariadenia. Pravidlá a výnimky možno definovať podľa typu zariadenia, výrobcu, produktu, identifikátora alebo sériového čísla.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/harden-endpoint-security/device-control*	**SPLNIL**
	Riešenie musí umožňovať plánované aj ad hoc skenovanie endpointov na prítomnosť malvéru alebo podozrivých artefaktov a musí podporovať asset management vrátane identifikácie neznámych alebo cudzích zariadení v prostredí.	***Spĺňa.*** *Cortex XSIAM podporuje ad hoc aj pravidelne plánované úplné skenovanie endpointov. Host Insights a funkcie zisťovania aktív poskytujú inventár spravovaných aj nespravovaných zariadení; Host Insights je súčasťou ponúkanej licencie Cortex XSIAM Enterprise.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/scan-an-endpoint-for-malware* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses/license-allocation* *https://www.paloaltonetworks.com/cortex/endpoint-protection*	**SPLNIL**
	Endpointové dáta musia byť použiteľné pri spätnom hľadaní IOC, rekonštrukcii incidentu, vyhodnotení laterálneho pohybu a prioritizácii dopadu.	***Spĺňa.*** *Historická endpointová telemetria je dostupná pre spätné vyhľadávanie IOC a threat hunting pomocou XQL. Causality View, časová os a Network Causality*	**SPLNIL**

		View umožňujú rekonštruovať incident, sledovať laterálny pohyb a súvisiace entity; zoskupovanie a skórovanie prípadov podporuje prioritizáciu dopadu. *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/issue-investigation-actions/query-case-and-issue-data* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view/network-causality-view* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/customize-cases-and-issues/set-up-case-scoring*	
Retencia a hot storage	Dáta v hot storage musia byť dostupné pre rýchle vyhľadávanie, koreláciu, incidentové vyšetrovanie, dashboardy, reporty a threat hunting bez potreby manuálnej obnovy z offline archívu.	***Spĺňa.*** *Cortex XSIAM sprístupňuje dáta v hot storage priamo pre XQL vyhľadávanie, koreláciu, vyšetrovanie, threat hunting, dashboardy a reporty. Hot storage je predvoleným zdrojom dotazov a nevyžaduje import ani manuálnu obnovu dát z offline archívu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/how-to-build-xql-queries* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/advanced-configuration/create-custom-widgets/create-xql-widgets*	**SPLNIL**
	Hot storage pre endpointové dáta musí byť zabezpečený minimálne na 12 mesiacov a musí umožňovať spätné vyhľadávanie historického výskytu IOC a entít.	***Spĺňa.*** *Ponuka obsahuje hot storage pre 5 000 endpointov na 12 mesiacov. Základných 30 dní je rozšírených licenciou PAN-XSIAM-EP-HOT-RTN v množstve 55 000, čo predstavuje* *5 000 endpointov × 11 dodatočných mesiacov. Historické dáta sú dostupné na vyhľadávanie IOC, súborov, procesov, používateľov, zariadení a ďalších entít.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-an-ioc*	**SPLNIL**

	Hot storage pre ingestované dáta musí byť zabezpečený minimálne na 12 mesiacov pri dennom objeme minimálne 580 GB/deň.	***Spĺňa.*** *Ponuka obsahuje hot storage pre ingestované neendpointové dáta v objeme 580 GB/deň na 12 mesiacov. Základných 30 dní je rozšírených licenciou PAN-XSIAM-GB-HOT-RTN v množstve 6 380, čo predstavuje 580 GB/deň × 11 dodatočných mesiacov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/dataset-management*	**SPLNIL**
	Podpora indexovaného alebo ekvivalentne optimalizovaného vyhľadávania nad historickými dátami počas celej požadovanej retenčnej doby.	***Spĺňa.*** *Cortex XSIAM poskytuje ekvivalentne optimalizované vyhľadávanie prostredníctvom distribuovaného XQL analytického mechanizmu nad datasetmi v hot storage. Dotazy je možné vykonávať nad celým licencovaným retenčným obdobím bez obnovy dát z archívu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/how-to-build-xql-queries* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/xql-query-management*	**SPLNIL**
	Uchovávanie incidentovej histórie vrátane alertov, eskalačných krokov, komentárov, úloh, dôkazových artefaktov, vykonaných reakcií a auditnej stopy.	***Spĺňa.*** *Cortex XSIAM uchováva históriu prípadov a incidentov vrátane alertov, zmien stavu, komentárov, úloh, dôkazov, automatických a manuálnych reakcií. War Room a časová os predstavujú auditnú stopu vykonaných činností. Ponúkané licencie PAN-XSIAM-INCDT-EP-RTN a PAN-XSIAM-INCDT-GB-RTN rozširujú základnú 180-dňovú retenciu o ďalších šesť mesiacov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/use-the-war-room-in-an-investigation* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/evidence*	**SPLNIL**

	Možnosť definovať retenčné pravidlá podľa typu dát, dátových zdrojov, tenantov alebo legislatívnych a prevádzkových požiadaviek obstarávateľa.	***Spĺňa.*** *Dataset Management umožňuje priraďovať a upravovať retenčné plány pre jednotlivé datasety. Datasety je možné oddeliť podľa typu dát alebo dátového zdroja a v multitenantnom modeli spravovať v rámci príslušných tenantov, čím možno zohľadniť legislatívne a prevádzkové požiadavky verejného obstarávateľa.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/dataset-management* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses*	**SPLNIL**
	Surové udalosti, alerty, incidenty a relevantná telemetria z endpointových aj neendpointových zdrojov musia byť v požadovanom retenčnom období dostupné v režime hot storage s okamžitým alebo primerane rýchlym prístupom bez čakacej doby na obnovu z archívu.	***Spĺňa.*** *Ponúkaná kombinácia licencií pre endpointové a neendpointové hot storage spolu s rozšírenou retenciou alertov a incidentov zabezpečuje dostupnosť surových udalostí, telemetrie, alertov a incidentovej histórie počas požadovaného obdobia. Prístup k hot datasetom je priamy prostredníctvom XQL bez čakania na obnovu z archívu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/dataset-management* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/how-to-build-xql-queries*	**SPLNIL**
	Riešenie musí podporovať spätné vyhľadávanie novo pridaných alebo aktualizovaných IOC v historických dátach a vytvorenie incidentu alebo upozornenia pri zistení historického výskytu.	***Spĺňa.*** *Po pridaní alebo aktualizácii IOC Cortex XSIAM vyhľadáva zhodu v už zozbieraných historických dátach a následne vyhodnocuje aj nové prichádzajúce dáta. Zistená zhoda vytvorí alert, ktorý môže byť automaticky zaradený do nového alebo existujúceho prípadu podľa korelačných a zoskupovacích pravidiel.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-an-ioc* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-5.x-Documentation/What-s-an-IOC*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/case-concepts/case-grouping	
Detekcia hrozieb	Predpripravené detekčné pravidlá alebo analytické modely pre známe typy kybernetických útokov a možnosť ich aktualizácie počas podpory.	***Spĺňa.*** *Cortex XSIAM obsahuje výrobcom dodávané analytické modely, endpointové detekcie, korelačné pravidlá, playbooky a obsahové balíky pre známe typy útokov. Detekčná logika a ochranný obsah sú počas podpory pravidelne aktualizované výrobcom.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/analytics/analytics-overview/analytics-engine https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/install-cortex-xdr-agents/guidelines-for-keeping-cortex-xdr-agents-and-content-updated https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/marketplace/manage-content-packs	**SPLNIL**
	Detekcia a korelácia minimálne pre malware, ransomware, laterálny pohyb, privilege escalation, credential theft, command and control komunikáciu, exfiltráciu dát, perzistenciu, zneužitie administrátorských oprávnení, podozrivé cloudové aktivity a anomálne autentizačné udalosti.	***Spĺňa.*** *Cortex XSIAM kombinuje endpointovú ochranu, behaviorálnu analytiku, Identity Analytics, cloudovú analytiku a koreláciu viacerých dátových zdrojov. Pokrýva malware, ransomware, laterálny pohyb, privilege escalation, credential theft, C2 komunikáciu, exfiltráciu, perzistenciu, zneužitie administrátorských oprávnení, podozrivé cloudové operácie a anomálie autentizácie.* https://www.paloaltonetworks.com/cortex/detection-and-response https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/cortex-xsiam-analytics/enable-the-analytics-engine-and-identity-analytics https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Analytics-Alert-Reference-by-Alert-name/A-cloud-identity-performed-multiple-unusual-activities	**SPLNIL**
	Behaviorálna analýza používateľov, endpointov a systémov alebo ekvivalentné mechanizmy na identifikáciu anomálií.	***Spĺňa.*** *Analytics Engine a UEBA vytvárajú dynamické baseline správania používateľov, skupín, endpointov, hostiteľov a sieťovej komunikácie. Odchýlky od naučeného*	**SPLNIL**

		správania sa vyhodnocujú pomocou analytických a strojovo učených modelov a môžu vytvoriť alert alebo analytický incident. *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/analytics/analytics-overview/analytics-engine* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/cortex-xsiam-onboarding-checklist*	
	Mapovanie detekcií na MITRE ATT&CK alebo ekvivalentný rámec taktík, techník a procedúr.	***Spĺňa.*** *Detekčné a korelačné pravidlá Cortex XSIAM sú mapované na taktiky, techniky a podtechniky MITRE ATT&CK. Konzola poskytuje prehľad pokrytia MITRE ATT&CK a umožňuje zobraziť príslušné mapovanie pri hostiteľoch, používateľoch, alertoch a prípadoch.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/analytics/analytics-overview/review-mitre-att-and-ck-framework-coverage* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule/correlation-rule-details*	**SPLNIL**
	Možnosť vytvárať vlastné detekčné pravidlá, upravovať existujúce pravidlá, nastavovať výnimky, suppression pravidlá a logiku zníženia falošne pozitívnych alertov.	***Spĺňa.*** *Platforma umožňuje vytvárať a upravovať vlastné IOC, BIOC a XQL korelačné pravidlá vrátane ich závažnosti, časového režimu a suppression logiky. Výrobcom spravované detekcie sa ladia pomocou výnimiek, exclusions a suppression pravidiel bez narušenia ich ďalších aktualizácií.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-a-correlation-rule/manage-correlation-rules* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-*	**SPLNIL**

		protection/set-up-endpoint-profiles-and-exception-rules/set-up-exception-profiles-and-rules/add-an-ioc-or-bioc-rule-exception	
	Prioritizácia alertov a incidentov na základe závažnosti, dopadu, kontextu aktív, identity, threat intelligence, rozsahu zasiahnutia a tenantového kontextu.	***Spĺňa.*** *Cortex XSIAM automaticky zoskupuje súvisiace alerty a používa SmartScore na prioritizáciu prípadov podľa závažnosti a vypočítaného rizika. Vlastné scoring pravidlá môžu zohľadňovať polia incidentu, kritickosť aktív, používateľský a identitný kontext, škodlivé artefakty, threat intelligence, rozsah útoku, zdrojové alebo endpointové tagy a kontext príslušného child tenantu.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/overview-of-cases/resolving-cases-with-ai https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/customize-cases-and-issues/set-up-case-scoring https://www.paloaltonetworks.com/blog/security-operations/beating-alert-fatigue-with-cortex-xdr-smartscore-technology	**SPLNIL**
Forenzná analýza a threat hunting	Automatické zoskupovanie súvisiacich alertov do incidentov a vytváranie incidentového kontextu z viacerých dátových zdrojov.	***Spĺňa.*** *Cortex XSIAM automaticky spája súvisiace issues a alerty z endpointových, sieťových, identitných, cloudových a ďalších zdrojov do spoločného prípadu. Zoskupovanie využíva spoločný priebeh útoku a zhodné entity, čím vytvára jednotný incidentový kontext.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/case-concepts/case-grouping https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/grouping-graph	**SPLNIL**
	Podpora životného cyklu incidentu minimálne v stavoch nový, analyzovaný, eskalovaný, riešený, vyriešený a uzavretý alebo ekvivalentne konfigurovateľný workflow.	***Spĺňa.*** *Platforma podporuje riadený životný cyklus prípadu vrátane nového, analyzovaného, riešeného, vyriešeného a uzavretého stavu. Eskalačné a ďalšie prevádzkové stavy možno realizovať prostredníctvom vlastných stavov, dôvodov uzavretia, playbookov a automatizačných workflowov.*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/customize-cases-and-issues/create-custom-case-statuses-and-resolution-reasons *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/issue-investigation-actions/close-an-issue*	
	Možnosť priradiť incident analytikovi alebo skupine, evidovať úlohy, poznámky, komentáre, prílohy alebo odkazy a zaznamenávať vykonané úkony.	***Spĺňa.*** *Prípad možno priradiť vlastníkovi alebo case tímu s rolami assignee, contributor a watcher. Platforma eviduje manuálne a automatizované úlohy, poznámky, komentáre, prílohy, odkazy a vykonané úkony v časovej osi a auditnej stope prípadu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/overview-of-cases/overview-of-case-teams-and-roles* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/resolve-the-case/collaborative-notes-and-comments*	**SPLNIL**
	Zobrazenie časovej osi incidentu, súvisiacich udalostí, dotknutých aktív, používateľov, endpointov, IOC a odporúčaných reakčných krokov.	***Spĺňa.*** *Case Timeline zobrazuje chronologickú postupnosť udalostí, analytických a reakčných úkonov. Associated Assets and Artifacts a Evidence poskytujú pohľad na dotknutých používateľov, endpointy, procesy, súbory, IP adresy, domény, IOC a súvisiace odporúčania na nápravu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/case-timeline* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/associated-assets-and-artifacts*	**SPLNIL**
	Vyhľadávanie v incidentoch, alertoch a historických udalostiach podľa času, zdroja, závažnosti, entity, stavu, analytika a tenantového zaradenia.	***Spĺňa.*** *Konzola a XQL umožňujú vyhľadávať a filtrovať prípady, issues, alerty a historické udalosti podľa času, zdroja, závažnosti, stavu, vlastníka, entity a ďalších polí.*	**SPLNIL**

		Unified Case View umožňuje v multitenantnom prostredí filtrovať prípady podľa parent alebo child tenantu. *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/issue-investigation-actions/query-case-and-issue-data* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/additional-case-actions/unified-case-view*	
	Export incidentových dát pre auditné, forenzné, manažérske alebo reportovacie účely.	***Spĺňa.*** *Údaje o issues a prípadoch možno exportovať do strojovo spracovateľného súboru, prostredníctvom XQL alebo Cases API. Export zahŕňa incidentové polia, súvisiace artefakty, War Room záznamy a časovú os, čo umožňuje auditné, forenzné a manažérske spracovanie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/issue-investigation-actions/export-issue-details-to-a-file* *https://cortex-docs.paloaltonetworks.com/xsiam-api/cases-apis*	**SPLNIL**
	Riešenie musí poskytovať automatizovanú analýzu hlavnej príčiny incidentu alebo ekvivalentný mechanizmus identifikácie vzťahov medzi udalosťami, používateľmi, endpointmi, procesmi, súbormi, doménami a ďalšími entitami.	***Spĺňa.*** *Causality Analysis Engine automaticky vytvára kauzálne reťazce, identifikuje koreňovú príčinu alertu a zobrazuje vzťahy medzi udalosťami, používateľmi, endpointmi, procesmi, súbormi, doménami a sieťovou komunikáciou.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/case-concepts/what-is-causality* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/evidence*	**SPLNIL**
	Riešenie musí v rámci incidentu potláčať nerelevantný šum a zvýrazniť relevantné udalosti, pričom potlačené dáta musia zostať dohľadateľné pre detailnú analýzu alebo forenzné účely.	***Spĺňa.*** *Cortex XSIAM znižuje šum pomocou zoskupovania, deduplikácie, exclusions, suppression pravidiel a automatického uzatvárania nízkorizikových udalostí. Potlačenie sa vykonáva na úrovni issues a prípadov; pôvodná telemetria zostáva*	**SPLNIL**

		v licencovanom hot storage vyhľadateľná pomocou XQL a vylúčené issues možno kontrolovať samostatne. *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/customize-cases-and-issues/create-issue-exceptions/view-excepted-issues* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/build-xql-queries/how-to-build-xql-queries/create-xql-query*	
	Riešenie musí umožňovať riadené vyhľadávanie hrozieb na základe IOC naprieč spravovanými endpointmi a uloženými dátami vrátane overenia, či sa škodlivý súbor alebo artefakt nevyskytuje na ďalších endpointoch.	***Spĺňa.*** *XQL a Threat Intel Management umožňujú vyhľadávať IOC v uložených historických dátach. Funkcia File Search and Destroy vyhľadá súbor podľa hashu alebo cesty na spravovaných endpointoch, zobrazí jeho výskyt na ďalších zariadeniach a umožní následné odstránenie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/protect-your-endpoints/endpoint-security/install-and-manage-endpoints/set-up-endpoint-protection/set-up-endpoint-profiles-and-exception-rules/set-up-agent-settings-profiles* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Response-actions*	**SPLNIL**
	Riešenie musí umožniť automatizovaný alebo manuálny zber forenzných dát z endpointu minimálne v rozsahu procesy, sieťové spojenia, súbory, služby, prihlásenia, systémové artefakty a podľa technických možností aj obsah operačnej pamäte.	***Spĺňa.*** *Forenzný modul podporuje manuálny a automatizovaný zber procesov, súborov, sieťových spojení, služieb, perzistenčných mechanizmov, príkazovej histórie, prihlásení, registrov, systémových a používateľských artefaktov. Samostatná reakčná funkcia umožňuje získať obraz operačnej pamäte.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/data-collection/configure-collection* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/response-actions/collect-a-memory-image*	**SPLNIL**
	Zber forenzných dát musí byť možné spustiť vzdialene bez fyzického prístupu k	***Spĺňa.***	**SPLNIL**

	endpointu a musí byť auditovateľný vrátane času, používateľa, rozsahu operácie a výsledku.	*Online triage a forensic hunt možno spustiť vzdialene prostredníctvom existujúceho Cortex XDR agenta bez fyzického prístupu k endpointu. Stav, rozsah, cieľové endpointy, jednotlivé artefakty a výsledky zberu sú evidované v tabuľke Actions a v auditnej stope platformy.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/data-collection/triage/create-a-triage* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/data-collection/triage/triage-status*	
	Riešenie musí poskytovať preddefinované šablóny zberu dát podľa typu incidentu alebo podozrivého správania a centralizované zobrazenie výsledkov s možnosťou filtrovania, porovnania a časovej analýzy.	***Spĺňa.*** *Platforma umožňuje vytvoriť preddefinované a opakovane použiteľné triage konfigurácie výberom príslušných kategórií a artefaktov podľa incidentového scenára. Výsledky sú centralizované v Triage Results, Hunt Results a Host Timeline s filtrovaním a časovou analýzou.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/data-collection/configure-collection* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/data-collection/triage/triage-results*	**SPLNIL**
	Výsledky forenznej analýzy musia byť exportovateľné do štandardných formátov, napríklad JSON, CSV, PDF alebo ekvivalentných formátov použiteľných pre auditné a vyšetrovacie účely.	***Spĺňa.*** *Forenzné kolekcie, tabuľkové výsledky, dôkazové artefakty a výsledky XQL možno exportovať do strojovo spracovateľných alebo ekvivalentných vyšetrovacích formátov. Manažérsky alebo auditný výstup možno následne zahrnúť do reportu platformy.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/manage-an-investigation/create-a-new-investigation* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/analyze-case-details/evidence*	**SPLNIL**

	Forenzná funkcionalita musí byť integrovaná s incident managementom, threat intelligence a vyhľadávaním v platforme tak, aby bolo možné analyzovať artefakty v kontexte konkrétneho incidentu.	***Spĺňa.*** *Forenzné vyšetrovanie je súčasťou rovnakej Cortex XSIAM konzoly a využíva spoločné endpointové dáta, XQL, incidentový kontext, kauzálne reťazce a reakčné funkcie. Ponúkaný modul TIM zabezpečuje obohatenie forenzných artefaktov o threat intelligence a ich analýzu v kontexte konkrétneho prípadu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/forensics/manage-an-investigation* *https://www.paloaltonetworks.com/cortex/digital-forensics*	**SPLNIL**
Automatizácia a SOAR	Podpora automatizovaných playbookov alebo workflow mechanizmov pre obohacovanie, eskaláciu, notifikáciu, reakciu a uzatváranie incidentov.	***Spĺňa.*** *Cortex XSIAM obsahuje integrovanú SOAR funkcionalitu s automatizovanými playbookmi pre obohacovanie dát, eskaláciu, notifikovanie, vykonanie reakčných opatrení a aktualizáciu alebo uzatvorenie incidentov. Playbooky môžu byť automaticky priradené k definovanému typu alertu alebo incidentu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam-developer-guide/cortex-xsiam-development-guide/playbooks* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/issue-investigation-actions/close-an-issue*	**SPLNIL**
	Možnosť manuálneho, poloautomatického a plne automatizovaného spúšťania reakčných krokov podľa typu incidentu, závažnosti, zdroja alebo tenantového kontextu.	***Spĺňa.*** *Reakčné kroky a playbooky je možné spúšťať manuálne z incidentu, poloautomaticky s využitím manuálnych alebo schvaľovacích úloh a plne automaticky podľa typu alertu a podmienok vyhodnocujúcich polia incidentu, napríklad závažnosť alebo zdroj. V multitenantnom modeli sa zachováva príslušný tenantový kontext.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/use-the-interface* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook/add-objects-from-the-task-library/add-manual-tasks-and-blank-tasks*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/additional-case-actions/unified-case-view	
	Automatizované obohacovanie incidentov o interný a externý kontext, napríklad reputáciu IOC, informácie o aktíve, používateľovi, zraniteľnosti, hrozbe, kampani alebo TTP.	***Spĺňa.*** *Playbooky Cortex XSIAM automaticky obohacujú incidenty a indikátory prostredníctvom interných dát, Threat Intelligence Management a externých integrácií. Obohatenie môže zahŕňať reputáciu IOC, kontext aktíva, používateľa alebo identity, zraniteľnosti a informácie o hrozbách, kampaniach a TTP podľa dostupných dátových zdrojov.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/indicator-extraction https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/get-started-with-threat-intel-management/threat-intel-management-use-cases	**SPLNIL**
	Podpora reakcií minimálne: blokovanie IOC, izolácia alebo obmedzenie endpointu, vytvorenie alebo aktualizácia ticketu, odoslanie notifikácie, zmena závažnosti, eskalácia, spustenie dodatočného vyšetrovania a vyžiadanie schválenia analytikom.	***Spĺňa.*** *Cortex XSIAM podporuje natívnymi funkciami alebo playbookovými integráciami blokovanie IOC, izoláciu endpointu, vytvorenie a aktualizáciu ticketu, notifikácie, zmenu polí a závažnosti incidentu, eskaláciu, spustenie dodatočného vyšetrovania a schválenie reakcie analytikom.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-files/manage-file-execution https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/resolve-the-case/cortex-response-and-remediation-content-pack/investigate-an-issue-using-cortex-response-and-remediation-playbooks https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook/customize-your-playbook/update-issue-fields-with-playbook-tasks https://cortex.marketplace.pan.dev/marketplace/details/CommonPlaybooks/	**SPLNIL**

	Auditovateľné zaznamenávanie všetkých automatizovaných aj manuálne spustených reakčných úkonov vrátane času, používateľa, zdroja spustenia a výsledku.	***Spĺňa.*** *War Room uchováva auditnú stopu automatických aj manuálnych úkonov vykonaných v incidente. Endpointové reakcie sú zároveň evidované v Action Center vrátane typu a stavu akcie, času, používateľa, ktorý akciu inicioval, a výsledku vykonania.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/use-the-war-room-in-an-investigation* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-endpoints/overview-of-the-action-center/action-center-reference-information*	**SPLNIL**
	SOAR funkcionalita musí umožniť tvorbu a úpravu playbookov prostredníctvom grafického alebo ekvivalentne používateľsky zrozumiteľného editora s podporou vetvenia, podmienok, paralelizácie úloh a interakcie s externými systémami.	***Spĺňa.*** *Cortex XSIAM poskytuje grafický Playbook Editor na tvorbu a úpravu automatizačných workflowov bez potreby komplexného programovania. Editor podporuje štandardné, manuálne a podmienené úlohy, rozhodovacie vetvy, paralelné vykonávanie úloh, prácu s kontextovými dátami a volanie externých integračných príkazov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam-developer-guide/cortex-xsiam-development-guide/playbooks* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook/add-objects-from-the-task-library*	**SPLNIL**
	Riešenie musí obsahovať katalóg, marketplace alebo ekvivalentný mechanizmus dostupných integrácií, konektorov a reakčných akcií použiteľných v automatizácii bezpečnostných procesov.	***Spĺňa.*** *Cortex Marketplace poskytuje katalóg obsahových balíkov, ktoré môžu zahŕňať integrácie, konektory, playbooky, skripty, detekčné pravidlá a reakčné akcie. Obsahové balíky sa inštalujú, aktualizujú a spravujú priamo v platforme.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/marketplace/cortex-marketplace* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/cortex-marketplace/install-content-packs*	**SPLNIL**
	Riešenie musí umožňovať reportovanie výkonnosti automatizácie, incidentových	***Spĺňa.***	**SPLNIL**

	SLA alebo ekvivalentných prevádzkových metrík bezpečnostného tímu.	*Cortex XSIAM poskytuje dashboardy a dátové sady na sledovanie výkonu playbookov, chýb úloh, priemerného času vykonania a stavov manuálnych aj automatizovaných behov. Platforma zároveň podporuje definovanie a sledovanie SLA pre prípady a incidenty vrátane času riešenia a prekročenia stanovených limitov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook/test-your-playbook/troubleshoot-playbook-performance* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/customize-cases-and-issues/create-slas-for-issue-resolution*	
Threat intelligence management	Správa, import, obohacovanie, vyhľadávanie, hodnotenie a distribúcia indikátorov kompromitácie minimálne v rozsahu IP adresa, doména, URL, hash súboru, e-mailová adresa, CVE, ASN a CIDR rozsah.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje modul PAN-XSIAM-TIM. Cortex XSIAM podporuje správu, import, obohacovanie, vyhľadávanie, hodnotenie a distribúciu IOC typu IP adresa, doména, URL, hash, e-mailová adresa, CVE a CIDR. ASN je podporované ako intel atribút a prostredníctvom konfigurovateľného vlastného typu indikátora.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-management* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam-developer-guide/cortex-xsiam-development-guide/integrations-and-scripts/developing/reputation-and-dbot-score* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/customize-indicator-fields-and-types/create-an-indicator-type*	**SPLNIL**
	Podpora interných a externých threat intelligence zdrojov, feedov a vlastných kolekcií obstarávateľa.	***Spĺňa.*** *Cortex XSIAM TIM podporuje interné aj externé threat intelligence zdroje, komerčné a komunitné feedy, Unit 42 Intelligence, TAXII a vlastné kolekcie obstarávateľa. Vlastné zdroje je možné pripojiť prostredníctvom feed integrácie, API alebo vlastného integračného konektora.*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/configure-threat-intelligence-feed-integrations-1 *https://cortex-docs.paloaltonetworks.com/cortex-xsiam-developer-guide/cortex-xsiam-development-guide/readme/design/integration-design*	
	Podpora výmenných a integračných formátov minimálne STIX/TAXII alebo ekvivalent, CSV, JSON, API a formáty kompatibilné s bezpečnostnými nástrojmi obstarávateľa.	***Spĺňa.*** *Riešenie podporuje import a export indikátorov vo formáte STIX, integrácie TAXII 1.x, 2.0 a 2.1, export do CSV a spracovanie štruktúrovaných JSON dát prostredníctvom API, integračných príkazov a playbookov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/export-indicators* *https://cortex.marketplace.pan.dev/marketplace/details/FeedTAXII/* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/indicator-classification-and-mapping*	**SPLNIL**
	Obohacovanie alertov a incidentov o threat intelligence kontext vrátane zdroja, reputácie, confidence score, severity, súvisiaceho aktéra, malvéru, kampane, TTP, CVE a odporúčaných opatrení, ak sú dostupné.	***Spĺňa.*** *Cortex XSIAM automaticky obohacuje IOC, alerty a incidenty o dostupný kontext zdroja, reputácie, confidence/reliability skóre, závažnosti, aktéra, malvéru, kampane, TTP, CVE a vzťahov medzi entitami. Prostredníctvom playbookov môže doplniť aj odporúčané alebo automatizované reakčné opatrenia.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-investigation/extract-and-enrich-an-indicator* *https://xsoar.pan.dev/docs/reference/scripts/indicator-enrichment* *https://cortex.marketplace.pan.dev/marketplace/details/MITRECoA/*	**SPLNIL**
	Životný cyklus IOC vrátane pridania, schvaľovania, tagovania, allowlist/blocklist, expirácie, aktualizácie, deaktivácie a distribúcie do integračných cieľov.	***Spĺňa.*** *TIM zabezpečuje životný cyklus IOC vrátane vytvorenia, úpravy, tagovania, hodnotenia, expirácie, vyradenia a distribúcie. Schvaľovanie pred aktiváciou alebo distribúciou je možné realizovať manuálnou schvaľovacou úlohou v*	**SPLNIL**

		playbooku. Allowlist/blocklist je podporovaný prostredníctvom tagov, exclusion pravidiel a distribúcie do EDL alebo integračných cieľov. *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/get-started-with-threat-intel-management/indicator-lifecycle* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/automations/playbooks/build-your-playbook/add-objects-from-the-task-library/add-manual-tasks-and-blank-tasks* *https://cortex.marketplace.pan.dev/marketplace/details/EDL/*	
	Možnosť spätného vyhľadania historického výskytu IOC v uložených dátach a ich využitie v detekčných pravidlách alebo automatizačných workflowoch.	***Spĺňa.*** *Pri vytvorení alebo aktualizácii IOC pravidla Cortex XSIAM vykonáva spätné vyhľadávanie zhôd v uložených dátach. IOC je možné používať v detekčných pravidlách, threat hunting dotazoch a automatizovaných playbookoch na identifikáciu historického aj aktuálneho výskytu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules/whats-an-ioc/ioc-rule-details* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/generate-issues-from-indicators-using-indicator-rules-for-prevention-and-detection*	**SPLNIL**
	Podpora riadenia distribúcie IOC podľa typu, zdroja, tagu, confidence score, severity, kategórie hrozby alebo tenantového zaradenia.	***Spĺňa.*** *Distribúciu IOC je možné riadiť pomocou dotazov a filtrov nad poľami indikátora, najmä podľa typu, zdroja, tagu, skóre, verdictu, severity a kategórie. V multitenantnom modeli sa distribučné integrácie a pravidlá konfigurujú v kontexte príslušného parent alebo child tenantu.* *https://cortex.marketplace.pan.dev/marketplace/details/EDL/* *https://xsoar.pan.dev/docs/reference/playbooks/modify-edl* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/get-started-with-threat-intel-management/threat-intel-management-use-cases*	**SPLNIL**

	Súčasťou threat intelligence funkcionality musí byť schopnosť deduplikácie, normalizácie, prioritizácie a automatizovaného skórovania IOC podľa dôveryhodnosti zdroja, kontextu hrozby, závažnosti a relevancie voči prostrediu obstarávateľa.	***Spĺňa.*** *Cortex XSIAM konsoliduje rovnaký indikátor získaný z viacerých feedov, normalizuje jeho hodnotu pomocou formátovacích pravidiel a určuje verdict podľa zdroja s najvyššou dôveryhodnosťou. Reputačné a enhancement skripty umožňujú automatizované skórovanie a prioritizáciu podľa kontextu, závažnosti a relevancie IOC pre prostredie obstarávateľa.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/configure-threat-intelligence-feed-integrations-1* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/customize-indicator-fields-and-types/create-an-indicator-type/formatting-scripts* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-investigation/indicator-verdict*	**SPLNIL**
	Riešenie musí podporovať mapovanie IOC a súvisiacich hrozieb na MITRE ATT&CK, Cyber Kill Chain alebo ekvivalentné rámce a ich koreláciu s reálnymi udalosťami uloženými v platforme.	***Spĺňa.*** *Riešenie podporuje MITRE ATT&CK obsahové balíky a mapovanie threat intelligence na taktiky, techniky a podtechniky. IOC a súvisiace TTP je možné korelovať s reálnymi udalosťami uloženými v Cortex XSIAM a použiť v detekčných alebo reakčných playbookoch.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-configuration/configure-threat-intelligence-feed-integrations-1* *https://cortex.marketplace.pan.dev/marketplace/details/MITRECoA/* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/detection-rules/what-are-detection-rules*	**SPLNIL**
	Riešenie musí umožniť vizualizáciu vzťahov medzi hrozbami, IOC, entitami,	***Spĺňa.***	**SPLNIL**

	kampaňami, zraniteľnosťami a incidentmi formou grafovej analýzy, entity linking alebo ekvivalentného mechanizmu.	*Cortex XSIAM umožňuje vytvárať, zobrazovať a analyzovať vzťahy medzi indikátormi a súvisiacimi entitami. Relationships a Graph Search poskytujú entity-linking a grafový pohľad použiteľný na analýzu väzieb medzi IOC, incidentmi, hrozbami, aktívami, kampaňami a ďalšími dostupnými intel objektmi.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/threat-management/threat-intel-management/indicator-investigation/manage-indicator-relationships* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/graph-search/create-detection-rules-based-on-graph-search*	
	Riešenie musí podporovať tvorbu vlastných intel feedov a ich distribúciu do ostatných bezpečnostných nástrojov, napríklad SIEM, EDR/XDR, firewall alebo SOAR, podľa nastavených pravidiel.	***Spĺňa.*** *Generic Export Indicators Service umožňuje vytvoriť vlastný priebežne aktualizovaný intel feed podľa definovaného dotazu a sprístupniť ho ostatným bezpečnostným nástrojom. IOC je možné distribuovať prostredníctvom EDL, integračných konektorov, API a playbookov do firewallov, SIEM, EDR/XDR, SOAR alebo iných podporovaných systémov.* *https://cortex.marketplace.pan.dev/marketplace/details/EDL/* *https://xsoar.pan.dev/docs/reference/integrations/edl* *https://cortex.marketplace.pan.dev/marketplace/details/CortexXDR/*	**SPLNIL**
Identity threat detection and response	Spracovanie a korelácia udalostí z identitných systémov, identity providerov, adresárových služieb a autentizačných zdrojov.	***Spĺňa.*** *Ponúkaná konfigurácia obsahuje modul PAN-XSIAM-ITDR pre 5 000 identít. Cortex XSIAM spracúva a koreluje udalosti z Active Directory prostredníctvom Cloud Identity Engine, Microsoft Entra ID/Azure AD, Okta, SSO, VPN a ďalších adresárových, identitných a autentizačných zdrojov pripojených konektormi alebo API.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr/get-started-with-itdr* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/cloud-posture-and-runtime-security-data-sources/ingest-logs-and-data-from-okta*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr/conditional-access-policy	
	Detekcia anomálií v autentizácii a autorizácii používateľov vrátane podozrivého prihlasovania, nemožného cestovania, geograficky neštandardného prihlásenia, brute-force a password spraying aktivít.	***Spĺňa.*** *Identity Analytics vytvára behaviorálny profil používateľov a deteguje podozrivé autentizačné aktivity vrátane impossible travel, prihlásenia z neštandardnej krajiny alebo ASN, neobvyklého času prihlásenia, brute-force a password spraying útokov v SSO, VPN a adresárových prostrediach.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/Impossible-traveler-SSO https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/User-attempted-to-connect-from-a-suspicious-country https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/External-Login-Password-Spray https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/SSO-Brute-Force	**SPLNIL**
	Identifikácia rizikových používateľov, privilegovaných účtov, servisných účtov, kompromitovaných identít a neštandardných zmien oprávnení alebo členstva v skupinách.	***Spĺňa.*** *ITDR poskytuje User Risk View a Risk Management dashboard s rizikovým skóre identít. Podporuje označovanie citlivých a administrátorských rolí, identifikáciu kompromitovaných účtov a insider hrozieb a detekciu neštandardného používania servisných účtov, zmien oprávnení a členstva v privilegovaných skupinách.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr/investigate-user-risk https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr/asset-roles https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-Alert-name/A-user-was-added-to-a-Windows-security-group	**SPLNIL**

		https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/SSO-authentication-by-a-service-account	
	Detekcia laterálneho pohybu s využitím identity, zneužitia privilegovaných účtov, credential theft a anomálneho používania servisných účtov.	***Spĺňa.*** *Cortex XSIAM deteguje identitne podporovaný laterálny pohyb a zneužitie privilegovaných alebo servisných účtov. Detekčné modely pokrývajú napríklad neštandardné administrátorské správanie, RDP pohyb medzi zariadeniami, DCSync a ďalšie techniky získavania prihlasovacích údajov a neštandardné prihlasovanie servisných účtov.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/New-Administrative-Behavior https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-Alert-name/Abnormal-RDP-connections-to-multiple-hosts https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-data-source/Potential-DCSync-by-an-unusual-user https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Analytics-Alert-Reference-by-Alert-name/VPN-login-by-a-service-account	**SPLNIL**
	Korelácia identitných udalostí s endpointovými, sieťovými, cloudovými a aplikačnými dátami.	***Spĺňa.*** *Cortex XSIAM koreluje identitné udalosti s endpointovou, sieťovou, cloudovou, SaaS a aplikačnou telemetriou v spoločnom dátovom modeli. User Risk View, incidentový pohľad a causality view umožňujú vyšetrovať aktivitu identity spolu s použitými zariadeniami, IP adresami, procesmi, aplikáciami, sieťovými spojeniami a súvisiacimi alertmi.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/identity-threat-module-itdr/investigate-user-risk https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/investigate-issues/causality-view/saas-causality-view https://xsoar.pan.dev/docs/reference/playbooks/user-investigation---generic	**SPLNIL**

	Podpora reakčných postupov na identitné hrozby prostredníctvom natívnych funkcií alebo integrácií, napríklad eskalácia, notifikácia, blokovanie indikátora, integrácia s identity providerom alebo ticketing systémom.	***Spĺňa.*** *Identitné incidenty je možné riešiť automatizovanými alebo manuálnymi playbookmi. Podporované reakcie zahŕňajú eskaláciu a notifikáciu, blokovanie škodlivých indikátorov, zrušenie používateľských relácií, reset hesla, reakcie prostredníctvom Okta alebo Microsoft Entra ID a vytvorenie či aktualizáciu ticketu v ITSM systéme.* *https://xsoar.pan.dev/docs/reference/playbooks/cortex-xdr---identity-analytics* *https://xsoar.pan.dev/docs/reference/articles/XSIAM-Playbooks* *https://cortex.marketplace.pan.dev/marketplace/details/ServiceNow/*	**SPLNIL**
Multitenantný model	Logické oddelenie dát, incidentov, alertov, dashboardov, reportov, používateľov, rolí, pravidiel a nastavení medzi jednotlivými tenantmi.	***Spĺňa.*** *Cortex XSIAM Enterprise Multi-Tenant zabezpečuje logické oddelenie bezpečnostných dát a konfiguračných objektov jednotlivých child tenantov vrátane incidentov, alertov, dashboardov, reportov, používateľov, rolí, pravidiel a nastavení. Ponúkaná konfigurácia obsahuje 1 parent tenant a celkovo 6 child tenantov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/what-is-cortex-xsiam-multi-tenant*	**SPLNIL**
	Parent tenant musí umožňovať centrálny dohľad, administráciu, reporting a správu nad child tenantmi pri zachovaní oddelenia dát a oprávnení.	***Spĺňa.*** *Parent tenant poskytuje centrálnu viditeľnosť hrozieb a správu child tenantov. Funkcia Unified Case View umožňuje zobraziť a filtrovať prípady parent aj child tenantov, pričom prístup k jednotlivým tenantom je riadený pridelenými rolami a oprávneniami.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/what-is-cortex-xsiam-multi-tenant/enterprise-multi-tenant* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/additional-case-actions/unified-case-view*	**SPLNIL**
	Možnosť delegovanej správy child tenantov a nastavenia odlišných oprávnení, integrácií,	***Spĺňa.*** *Pre child tenantov možno definovať samostatné access configurations a RBAC oprávnenia a delegovať ich správu určeným administrátorom. Každý child*	**SPLNIL**

	detekcií, retenčných pravidiel a reportov pre jednotlivé tenanty.	*tenant môže mať vlastné integrácie, detekčný obsah, retenčné nastavenia v rozsahu pridelených licencií, dashboardy a reporty.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/onboard-cortex-multi-tenant/onboarding-checklist-for-multi-tenant-customer-owned-license-deployments/step-2.-define-access-configuations-and-role-permissions* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/child-tenant-management*	
	Zabránenie neoprávnenému prístupu medzi tenantmi a auditovanie administrátorských aktivít naprieč tenantovým modelom.	***Spĺňa.*** *Izolácia tenantových dát spolu s RBAC a samostatnými prístupovými konfiguráciami zabraňuje neoprávnenému prístupu medzi tenantmi. Administrátorské a vyšetrovacie operácie sú zaznamenávané v Management Audit Logs vrátane používateľa, času, vykonanej operácie a jej výsledku.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/what-is-cortex-xsiam-multi-tenant* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Monitor-administrative-activity*	**SPLNIL**
	Centralizovaný reporting a prehľad stavu incidentov, ingestu, konektorov, retencie a prevádzkových metrík naprieč tenantmi.	***Spĺňa.*** *Parent tenant poskytuje konsolidovaný pohľad na prípady parent a child tenantov s filtrovaním podľa tenantu. Stav ingestu, konektorov, datasetov, retencie a ďalšie prevádzkové metriky sú dostupné prostredníctvom dashboardov, Data Ingestion Health a Dataset Management, s možnosťou centrálneho dohľadu nad child tenantmi.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/analyze-and-resolve-cases/additional-case-actions/unified-case-view* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/about-health-issues/monitor-data-ingestion-health* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/dataset-management*	**SPLNIL**

Forwardovanie dát	Export alebo forwardovanie vybraných endpointových, bezpečnostných a ingestovaných dát do externých systémov prostredníctvom API, syslog, event streamingu, webhooku, feed exportu alebo ekvivalentného mechanizmu.	***Spĺňa.*** *Cortex XSIAM podporuje export endpointovej telemetrie, parsovaných ingestovaných dát, alertov, auditných záznamov, prípadov a reportov do externých SIEM, dátových alebo archivačných systémov. Podporované sú Event Forwarding, API, syslog, webhook a cloudové mechanizmy, napríklad Amazon SQS alebo S3. Ponuka obsahuje forwarding práva pre 5 000 endpointov a 580 GB/deň.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/learn-about-cortex-xsiam/cortex-xsiam-product-licenses* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Forward-notifications-to-webhook*	**SPLNIL**
	Možnosť filtrovania a smerovania forwardovaných dát podľa typu udalosti, zdroja, závažnosti, entity, tenantu, pravidla alebo iných atribútov.	***Spĺňa.*** *Forwarding konfigurácie umožňujú vybrať typ prenášaných záznamov a definovať filtre podľa ich polí, napríklad podľa závažnosti, zdroja alertu alebo typu udalosti. Ďalšie smerovanie podľa entity, pravidla a iných atribútov možno realizovať pomocou XQL, automatizačných pravidiel, playbookov a integračných webhookov. Konfigurácia sa vykonáva samostatne pre príslušný tenant.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Configure-notification-forwarding* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/data-management/manage-event-forwarding/endpoints-event-forwarding-included-excluded-fields-by-event-type*	**SPLNIL**
	Monitoring stavu forwardovania vrátane upozornení na výpadky, oneskorenia, chybovosť alebo prekročenie kapacitných limitov.	***Spĺňa.*** *Platforma umožňuje testovanie spojenia a sledovanie stavu nakonfigurovaných syslog a webhook cieľov. Výpadky alebo chyby integračných komponentov a dátových tokov možno monitorovať prostredníctvom health checks, Data Ingestion Health, integračných stavov a notifikácií; licenčné a objemové využitie je dostupné v správe licencií a dát.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services/configure-external-applications-for-forwarding/integrate-a-syslog-receiver*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/cortex-xsiam-data-sources/administration-and-troubleshooting/about-health-issues/monitor-data-ingestion-health	
	Zabezpečená autentifikácia, autorizácia a šifrovaný prenos pri forwardovaní dát do externých systémov.	***Spĺňa.*** *Prístup ku konfigurácii forwardovania je riadený prostredníctvom RBAC oprávnení. Syslog forwarding podporuje TCP so SSL/TLS a overovanie certifikátu cieľového systému; API, webhook a cloudové konektory používajú príslušné autentifikačné údaje, tokeny alebo cloudové IAM oprávnenia a šifrovanú HTTPS komunikáciu.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services/configure-external-applications-for-forwarding/integrate-a-syslog-receiver https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/role-based-access-control/configuration-permissions/data-management-permissions	**SPLNIL**
	Auditovateľnosť integračných a forwarding aktivít vrátane zmien konfigurácie a záznamu o odosielaní dát.	***Spĺňa.*** *Zmeny konfigurácie integrácií a forwardovania sú evidované v Management Audit Logs. Auditné záznamy obsahujú používateľa, čas, vykonanú akciu, dotknutý objekt a stav operácie; samotné auditné logy možno ďalej forwardovať do externého systému cez syslog alebo iný podporovaný mechanizmus.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Monitor-administrative-activity https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/data-and-log-notification-formats/management-audit-log-notification-format	**SPLNIL**
Integrácie	Podpora integrácie so SIEM, SOAR, XDR, EDR, NDR, firewall, e-mail security, sandbox, vulnerability management, identity provider, cloud platformami a ticketing/ITSM systémami.	***Spĺňa.*** *Cortex XSIAM podporuje integráciu so systémami kategórie SIEM, SOAR, XDR/EDR, NDR, firewall, e-mail security, sandbox, vulnerability management, identity provider, cloudové platformy a ticketing/ITSM. Integrácie sú realizované prostredníctvom natívnych dátových konektorov, Marketplace content packov, REST API, syslogu, webhookov a automatizačných playbookov.*	**SPLNIL**

		https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Vendor-specific-data-sources https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Cortex-Marketplace	
	Dostupné REST API alebo ekvivalentné programové rozhranie pre prácu s incidentmi, alertmi, IOC, vyhľadávaním, integráciami, reportmi a automatizáciou.	***Spĺňa.*** *Cortex XSIAM poskytuje dokumentované REST Public API a ekvivalentné automatizačné rozhrania na programovú prácu s incidentmi/prípadmi, alertmi, IOC, endpointmi, XQL vyhľadávaním a reakčnými operáciami. Integrácie, automatizácie a reportovacie procesy možno ovládať prostredníctvom API, integračných príkazov, playbookov a plánovaných úloh.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-API https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/API-endpoints	**SPLNIL**
	Správa API tokenov alebo integračných účtov vrátane vytvárania, deaktivácie, rotácie a obmedzenia oprávnení podľa rolí alebo integračného účelu.	***Spĺňa.*** *Administrátorská konzola umožňuje vytvárať a deaktivovať API kľúče, nastaviť ich typ a priradiť im preddefinovanú alebo vlastnú rolu. Rotácia sa realizuje vygenerovaním nového kľúča a zrušením pôvodného. Rozsah prístupu API kľúča je obmedzený pridelenou rolou, RBAC oprávneniami a oprávneniami k datasetom podľa integračného účelu.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Manage-API-keys https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Manage-user-roles-and-access-management	**SPLNIL**
	Dokumentovaná konfigurácia integračných mechanizmov a dostupná technická dokumentácia API/konektorov.	***Spĺňa.*** *Výrobca poskytuje technickú dokumentáciu konfigurácie dátových zdrojov, konektorov, API, autentifikácie, integračných content packov a automatizačných príkazov minimálne v anglickom jazyku. Dokumentácia je dostupná na portáloch Cortex Documentation a Cortex Developer Docs.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/What-are-Cortex-XSIAM-data-sources https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-API	**SPLNIL**

		https://xsoar.pan.dev/docs/reference/index	
	Podpora zabezpečenej integrácie s existujúcim bezpečnostným prostredím obstarávateľa bez požiadavky na zverejnenie alebo zdieľanie interných datasetov s tretími stranami bez súhlasu obstarávateľa.	***Spĺňa.*** *Integrácie Cortex XSIAM sa aktivujú a konfigurujú výhradne oprávneným zákazníkom a využívajú šifrovanú komunikáciu, autentifikované API, integračné účty a oprávnenia podľa princípu minimálnych privilégií. Integrácia nevyžaduje verejné sprístupnenie interných datasetov. Spracovanie alebo prenos zákazníckych dát výrobcom a jeho zmluvnými subdodávateľmi sa riadi dohodnutým účelom, zmluvnými podmienkami, DPA a dokumentovanými pravidlami ochrany súkromia.* https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiam-privacy https://www.paloaltonetworks.com/legal-notices/privacy https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Security-model-and-authentication	**SPLNIL**
Vyhľadávanie a analytika	Pokročilé vyhľadávanie nad normalizovanými aj pôvodnými dátami prostredníctvom query jazyka alebo ekvivalentného mechanizmu.	***Spĺňa.*** *Cortex XSIAM poskytuje plnohodnotný dotazovací jazyk Cortex Query Language (XQL). Pomocou XQL možno analyzovať pôvodné udalosti v raw datasetoch aj normalizované údaje mapované do jednotného Cortex Data Model (XDM).* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/how-to-build-xql-queries/create-xql-query	**SPLNIL**
	Filtrovanie podľa času, zdroja, tenantu, používateľa, endpointu, IP adresy, domény, URL, hashu, procesu, typu udalosti, závažnosti, incidentu, IOC a ďalších relevantných atribútov.	***Spĺňa.*** *XQL umožňuje filtrovať podľa času a ľubovoľných dostupných polí datasetu, vrátane zdroja, tenantu, používateľa, endpointu, IP adresy, domény, URL, hashu, procesu, typu udalosti, závažnosti, incidentu alebo IOC. Podporované sú logické operátory, porovnávanie, zoznamy hodnôt, regulárne výrazy, zástupné znaky, fulltextové vyhľadávanie a kombinovanie viacerých datasetov.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/XQL-language-features	**SPLNIL**

		https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM-REST-API/Get-XQL-query-results	
	Možnosť uložiť vyhľadávacie filtre, vytvárať vlastné dotazy, exportovať výsledky a použiť historické dáta na spätné hľadanie IOC a threat hunting.	***Spĺňa.*** *Používateľ môže vytvárať a ukladať vlastné XQL dotazy v osobnej alebo zdieľanej Query Library, následne ich upravovať a opakovane spúšťať. Výsledky možno exportovať do TSV alebo ekvivalentného strojovo spracovateľného formátu. Historické dáta v licencovanej retencii sú dostupné na spätné vyhľadávanie IOC a threat hunting.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Manage-access-to-saved-queries https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/how-to-build-xql-queries/review-xql-query-results https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/investigation-and-response/research-a-known-threat	**SPLNIL**
	Podpora vyšetrovania udalostí v časovej osi a prepájania súvisiacich entít, vrátane používateľov, endpointov, IP adries, domén, súborov, hashov, procesov a identít.	***Spĺňa.*** *Cortex XSIAM zobrazuje chronologickú časovú os udalostí a reakčných aktivít súvisiacich s incidentom. Causality View, Graph Search a incidentový kontext prepájajú používateľov, identity, endpointy, IP adresy, domény, súbory, hashe, procesy a ich vzájomné príčinné vzťahy.* https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Timeline https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/What-is-Causality https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/graph-search/create-graph-search-query	**SPLNIL**
	Vyhľadávací mechanizmus musí umožniť vyhľadať relevantné informácie vo všetkých uložených dátach pomocou plnohodnotného dotazovacieho jazyka alebo ekvivalentného query mechanizmu a zároveň poskytovať používateľsky prívetivé grafické vyhľadávanie.	***Spĺňa.*** *XQL umožňuje vyhľadávať vo všetkých oprávnenému používateľovi dostupných datasetoch vrátane endpointových, sieťových, cloudových, identitných a aplikačných dát. Súčasťou konzoly je používateľsky prívetivý Query Builder s preddefinovanými šablónami, formulárovými parametrami a free-text*	**SPLNIL**

		vyhľadávaním; pokročilí používatelia môžu zapisovať úplné XQL dotazy manuálne. *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/about-the-query-builder* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/how-to-build-xql-queries/create-xql-query*	
	Riešenie musí umožniť ukladať dotazy, opakovane ich spúšťať podľa harmonogramu a využiť ich výsledky na reportovanie, korelačné pravidlá alebo alertovanie.	***Spĺňa.*** *XQL dotazy možno uložiť, spustiť jednorazovo alebo opakovane podľa nastaveného harmonogramu a spravovať v Query Center. Rovnaká XQL logika môže byť použitá v dashboardoch a reportoch alebo ako základ vlastného korelačného pravidla, ktoré pri splnení definovaných podmienok vytvorí alert.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/cortex-agentix-xql/build-xql-queries/manage-scheduled-queries* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Correlation-rule-details* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Build-custom-dashboards-and-reports*	**SPLNIL**
Informačné panely a reporty	Predpripravené informačné panely pre SOC prevádzku, incidenty, alerty, ingest, konektory, tenanty, hrozby, identity, endpointy, úložisko a prevádzkové metriky.	***Spĺňa.*** *Cortex XSIAM obsahuje systémové a Command Center dashboardy pre bezpečnostnú a SOC prevádzku, prípady a alerty, stav a objem ingestu, dátové zdroje, endpointy, identity, hrozby, cloudové prostredie, úložisko a spotrebu kapacít. Ďalšie predpripravené dashboardy poskytujú moduly TIM, ITDR a nainštalované Marketplace content packy. Multitenantná konfigurácia umožňuje centrálne a tenantovo filtrované zobrazenie.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/dashboard-reference/system-dashboards* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/dashboard-reference/command-center-reference/cortex-command-center*	**SPLNIL**

	Možnosť vytvárať vlastné dashboardy a reporty, filtrovať ich podľa času, tenantu, kategórie, tagu, zdroja alebo iného atribútu a plánovať ich pravidelné generovanie.	***Spĺňa.*** *Používatelia môžu vytvárať vlastné dashboardy a reportové šablóny z preddefinovaných alebo vlastných XQL widgetov. Dashboardy a widgety podporujú časové a používateľské filtre podľa dostupných dátových polí, napríklad tenant, kategória, tag alebo zdroj. Reporty možno generovať jednorazovo alebo opakovane podľa nastaveného harmonogramu.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/create-dashboards/create-a-dashboard* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/create-reports/create-a-report-template-from-scratch* *https://cortex-docs.paloaltonetworks.com/cortex-xdr-3.x/cortex-xdr-3.x-documentation/investigate-and-respond-to-incidents/dashboards/reports/run-or-schedule-reports*	**SPLNIL**
	Reporty minimálne v oblastiach: počet a stav incidentov, závažnosť, čas do detekcie, čas do reakcie, najčastejšie hrozby, rizikoví používatelia a endpointy, stav ingestu, stav tenantov, využitie úložiska a aktivity analytikov.	***Spĺňa.*** *Systémové a vlastné reporty môžu obsahovať počet, stav a závažnosť prípadov a alertov, MTTD, MTTR, trendy a najčastejšie hrozby, rizikové identity a endpointy, stav a objem ingestu, tenantový kontext, využitie úložiska a činnosť analytikov. Požadované metriky možno zostaviť nad príslušnými datasetmi pomocou XQL widgetov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/dashboard-reference/system-dashboards* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/advanced-configuration/create-custom-widgets/create-xql-widgets*	**SPLNIL**
	Možnosť exportu reportov a dashboardov vo formátoch vhodných pre interný audit, manažérske vyhodnotenie a bezpečnostnú prevádzku.	***Spĺňa.*** *Obsah dashboardov možno použiť v reportových šablónach a exportovať ako PDF vhodné pre auditné a manažérske účely. Údaje použité v dashboardoch a reportoch možno zároveň exportovať z tabuliek alebo výsledkov XQL dotazov vo formátoch CSV, TSV alebo ekvivalentnom strojovo spracovateľnom formáte.*	**SPLNIL**

		https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/create-reports/create-a-report-template-from-scratch https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/role-based-access-control/investigation-and-response-permissions/search-permissions/query-center-permissions	
	Riešenie musí umožniť tvorbu dynamických dashboardov nad ľubovoľne definovanými používateľskými pohľadmi do dát a sledovanie SOC metrík v reálnom čase.	***Spĺňa.*** *Cortex XSIAM umožňuje vytvárať dynamické dashboardy nad ľubovoľnými používateľsky definovanými XQL pohľadmi a datasetmi. Vlastné widgety podporujú grafy, tabuľky, parametre, filtre a drill-down do zdrojových dát. Priebežným obnovovaním widgetov možno sledovať aktuálne incidentové, bezpečnostné a SOC metriky.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/advanced-configuration/create-custom-widgets/create-xql-widgets https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/advanced-configuration/create-custom-widgets/add-parameters-to-a-custom-xql-widget	**SPLNIL**
	Riešenie musí podporovať reporty pre bezpečnostný audit, compliance, výkonnosť SOC a vyhodnotenie incidentov vrátane exportu vo formátoch vhodných pre ďalšie spracovanie.	***Spĺňa.*** *Platforma podporuje systémové aj vlastné reporty pre bezpečnostný audit, compliance, výkonnosť SOC a vyhodnotenie prípadov. Reporty možno plánovať, uchovávať v histórii a exportovať do PDF; compliance výstupy podporujú aj CSV a analytické dáta možno exportovať do ďalších strojovo spracovateľných formátov.* https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/role-based-access-control/cloud-security-and-posture-management-permissions/compliance-cloud-permissions https://cortex-docs.paloaltonetworks.com/cortex-xsiam/detect-investigate-and-respond-to-threats/monitor-dashboards-and-reports/create-reports/create-a-report-template-from-scratch	**SPLNIL**
	Správa používateľov a rolí prostredníctvom RBAC vrátane oddelenia administrátorských,	***Spĺňa.*** *Cortex XSIAM podporuje správu používateľov, skupín, API kľúčov a*	**SPLNIL**

Bezpečnosť a riadenie prístupov	analytických, reportovacích a tenantových oprávnení.	*preddefinovaných alebo vlastných rolí prostredníctvom RBAC. Oprávnenia možno samostatne definovať pre administráciu, vyšetrovanie a reakciu, endpointy, vyhľadávanie, integrácie, automatizáciu, dashboardy, reporty, správu dát a tenantov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/manage-user-roles-and-access-management/manage-user-roles* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/reference-and-developer-docs/role-based-access-control/role-permissions-by-component*	
	Podpora viacfaktorovej autentifikácie alebo federovaného prihlásenia cez enterprise identity provider.	***Spĺňa.*** *Cortex XSIAM podporuje federované prihlásenie prostredníctvom SAML 2.0 s enterprise identity providermi, napríklad Microsoft Entra ID, Okta alebo PingOne. MFA a pravidlá podmieneného prístupu sa vynucujú na identity provideri pred povolením prístupu do platformy.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/set-up-authentication* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/set-up-authentication/authenticate-users-using-sso*	**SPLNIL**
	Komunikácia výhradne prostredníctvom zabezpečených protokolov, minimálne HTTPS/TLS alebo ekvivalentne šifrovaný prenos.	***Spĺňa.*** *Komunikácia administrátorskej konzoly, API, endpointových agentov, Broker VM a ďalších komponentov s Cortex XSIAM je realizovaná šifrovaným HTTPS/TLS spojením, štandardne prostredníctvom TCP portu 443. Ponúkané riešenie bude nakonfigurované tak, aby aj syslog a externé integračné prenosy používali TCP so SSL/TLS alebo HTTPS.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/activate-cortex-xsiam/enable-access-to-required-panw-resources* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/forward-logs-and-data-from-cortex-xsiam-to-external-services/configure-external-applications-for-forwarding/integrate-a-syslog-receiver*	**SPLNIL**

	Ochrana uložených dát primeranými kryptografickými a organizačnými mechanizmami, vrátane oddelenia zákazníckych/tenantových dát.	***Spĺňa.*** *Dáta uložené v Cortex XSIAM sú šifrované a chránené kryptografickými, prístupovými a organizačnými opatreniami výrobcu. Platforma podporuje výrobcom spravované šifrovanie aj BYOK, pri ktorom zákazník riadi vlastné šifrovacie kľúče. Multitenantná architektúra zabezpečuje logické oddelenie dát jednotlivých zákazníkov a child tenantov.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/activate-cortex-xsiam/bring-your-own-keys* *https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiam-privacy* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/what-is-cortex-xsiam-multi-tenant*	**SPLNIL**
	Vedenie auditných záznamov o používateľskej, systémovej, administrátorskej, integračnej a reakčnej aktivite.	***Spĺňa.*** *Cortex XSIAM vedie Management Audit Logs, Agent Audit Logs, incidentovú časovú os a záznamy vykonania automatizácií a reakčných opatrení. Evidovaný je používateľ alebo systémový proces, čas, typ operácie, dotknutý objekt, integračná alebo reakčná aktivita a výsledok vykonania.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Monitor-administrative-activity* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/data-and-log-forwarding/data-and-log-notification-formats/management-audit-log-notification-format*	**SPLNIL**
	Riešenie musí podporovať federované prihlásenie prostredníctvom SAML alebo ekvivalentného štandardu a MFA pre všetky administrátorské a operátorské prístupy.	***Spĺňa.*** *Platforma podporuje SAML 2.0 SSO a mapovanie skupín enterprise identity providera na používateľské skupiny a roly Cortex XSIAM. Pre administrátorov a operátorov možno vynútiť výhradné SSO prihlásenie a povinné MFA alebo podmienený prístup prostredníctvom IdP; odstránením priameho prístupu cez Cortex Gateway sa zabráni obídeniu tejto politiky.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/deployment-steps/set-up-authentication/authenticate-users-using-sso*	**SPLNIL**
	Riešenie musí umožniť segregáciu rolí podľa funkcionality, skupín endpointov, tenantov,	***Spĺňa.***	**SPLNIL**

	dátových domén alebo rozsahu oprávnení tak, aby používateľ pristupoval iba k dátam a funkciám, na ktoré má oprávnenie.	*Cortex XSIAM kombinuje RBAC, Scope-Based Access Control a oprávnenia k datasetom. RBAC oddeľuje funkčné oprávnenia, SBAC obmedzuje správu a reakčné operácie podľa skupín alebo tagov endpointov a datasetové oprávnenia obmedzujú prístup k dátovým doménam. Enterprise Multi-Tenant zároveň riadi prístup k jednotlivým parent a child tenantom pomocou samostatných rolí a prístupových konfigurácií.* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/manage-user-roles-and-access-management/manage-user-scope* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/onboard-cortex-xsiam/post-deployment/manage-user-roles-and-access-management/manage-user-roles* *https://cortex-docs.paloaltonetworks.com/cortex-xsiam/configure-cortex-xsiam/multi-tenant/what-is-cortex-xsiam-multi-tenant/enterprise-multi-tenant*	
Bezpečnosť a dôvernosť dát	Dáta verejného obstarávateľa, vyhľadávania, nahrané datasety, vlastné IOC, interné tagy a používateľská aktivita nesmú byť bez súhlasu obstarávateľa zdieľané s tretími stranami.	***Spĺňa.*** *Cortex XSIAM spracúva dáta obstarávateľa vrátane vyhľadávaní, datasetov, vlastných IOC, tagov a používateľskej aktivity iba podľa zmluvy, DPA a zdokumentovaných pokynov obstarávateľa. Dáta nie sú poskytované nesúvisiacim tretím stranám bez súhlasu; zapojenie subdodávateľov alebo externých obohacovacích služieb podlieha zmluvným pravidlám, informovaniu zákazníka a príslušným oprávneniam.* *https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiam-privacy* *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo_alto_networks_customer_data_processing_addendum.pdf*	**SPLNIL**
	Zmluvne garantované pravidlá uchovávania, dostupnosti, zálohovania, spracúvania a mazania dát počas trvania služby a po jej ukončení.	***Spĺňa.*** *Retencia dát je riadená licencovanými retenčnými kapacitami Cortex XSIAM. Dostupnosť služby je upravená SLA, pričom bezpečnostné opatrenia výrobcu zahŕňajú kontinuitu prevádzky, obnovu dát a disaster recovery. DPA upravuje spracovanie, vrátenie a bezpečné vymazanie dát po skončení zmluvy, ak ich ďalšie uchovávanie nevyžaduje zákon.*	**SPLNIL**

		https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Data-retention *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/data sheets/support/cortex-service-level-agreement.pdf* *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf*	
	Platforma musí poskytovať mechanizmy na oddelenie zákazníckych alebo tenantových dát a na obmedzenie neoprávneného prístupu.	***Spĺňa.*** *Cortex XSIAM zabezpečuje logické oddelenie dát jednotlivých zákazníkov a tenantov. Prístup je riadený prostredníctvom tenantového modelu, RBAC, používateľských rolí a rozsahu oprávnení, čím sa zabraňuje neoprávnenému prístupu medzi tenantmi.* *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Step-2.-Define-access-configurations-and-role-permissions*	**SPLNIL**
	Riešenie musí zabezpečiť ochranu dát pri prenose aj pri uložení a musí umožniť audit spracovania a prístupu k dátam.	***Spĺňa.*** *Dáta Cortex XSIAM sú šifrované pri uložení štandardom AES-256 a pri prenose prostredníctvom TLS. Platforma podporuje aj BYOK. Prístupy, administrátorské operácie a reakčné činnosti sú zaznamenávané v auditných logoch.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Activate-Cortex-XSIAM* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Monitor-administrative-activity* *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf*	**SPLNIL**
	Všetky dáta obstarávateľa vrátane telemetrie, alertov, incidentov a forenzných dát musia byť uchovávané v dátových centrách fyzicky umiestnených v EÚ/EHP alebo v inom zmluvne schválenom režime spĺňajúcom požiadavky GDPR; prípadný	***Spĺňa.*** *Ponúkaný tenant Cortex XSIAM bude aktivovaný v zmluvne určenom podporovanom regióne EÚ/EHP. Dokumentácia výrobcu uvádza, že všetky Cortex XSIAM logy a ingestované dáta zostávajú uložené v hraniciach zvoleného regiónu. Prípadné cezhraničné spracovanie subdodávateľom podlieha DPA,*	**SPLNIL**

	prenos anonymizovaných metadát mimo EÚ/EHP je prípustný len za splnenia podmienok GDPR.	*GDPR a platnému prenosovému mechanizmu, napríklad SCC alebo rozhodnutiu o primeranosti.* *https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-3.x-Documentation/Cortex-XSIAM-supported-regions* *https://www.paloaltonetworks.com/legal-notices/trust-center/privacy* *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo_alto_networks_customer_data_processing_addendum.pdf*	
	Údaje musia byť uchovávané v dátových centrách certifikovaných minimálne na SOC 2 Type II alebo ekvivalentne nezávisle overiteľnú bezpečnostnú certifikáciu.	***Spĺňa.*** *Cortex XSIAM podlieha nezávislému auditu SOC 2 Type II/SOC 2+. Hostingová infraštruktúra a dátové centrá sú prevádzkované podľa nezávisle overovaných štandardov, ako sú ISO/IEC 27001, SSAE 18 alebo ISAE 3000. Aktuálny SOC 2 report je zákazníkovi dostupný na vyžiadanie prostredníctvom Trust Center výrobcu.* *https://www.paloaltonetworks.com/legal-notices/trust-center/soc* *https://www.paloaltonetworks.com/customers/cortex-xsiam-reshapes-secops-for-fortune-500-financial-giant* *https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf*	**SPLNIL**
	Výrobca dodávaného systému musí mať platnú certifikáciu ISO 27001 alebo ekvivalentnú certifikáciu riadenia informačnej bezpečnosti.	***Spĺňa.*** *Výrobca Palo Alto Networks má systém riadenia informačnej bezpečnosti certifikovaný podľa ISO/IEC 27001. Rozsah certifikácie zahŕňa platformu Cortex vrátane Cortex XSIAM.* *https://www.paloaltonetworks.com/legal-notices/trust-center/iso-27000-series*	**SPLNIL**
Inštalácia	• súčasťou ponuky musí byť implementačná služba zahŕňajúca aktiváciu, konfiguráciu tenantového modelu, forwardovania, základných detekcií, dashboardov a reportov pre preukázanie funkčnosti a prevádzkyschopnosti dodanej	• *Súčasťou ponuky je implementačná služba zahŕňajúca aktiváciu, konfiguráciu tenantového modelu, forwardovania, základných detekcií, dashboardov a reportov pre preukázanie funkčnosti a prevádzkyschopnosti dodanej Enterprise bezpečnostnej analytickej platformy typu XDR/SIEM/SOAR.*	**SPLNIL**

	Enterprise bezpečnostnej analytickej platformy typu XDR/SIEM/SOAR. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať inštaláciu a nastavenie dodanej Enterprise bezpečnostnej analytickej platformy typu XDR/SIEM/SOAR. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodanú Enterprise bezpečnostnú analytickú platformu typu XDR/SIEM/SOAR.	• *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať inštaláciu a nastavenie dodanej Enterprise bezpečnostnej analytickej platformy typu XDR/SIEM/SOAR - Cortex XSIAM.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Palo Alto Networks Certified XSIAM Engineer vydaným výrobcom Palo Alto Networks pre dodanú Enterprise bezpečnostnú analytickú platformu typu XDR/SIEM/SOAR - Cortex XSIAM.*	
Servisná podpora	Súčasťou dodávky musí byť prémiová servisná podpora počas celého licenčného obdobia minimálne na 3 roky vrátane prístupu k aktualizáciám, opravám, znalostnej báze, eskalácii problémov a technickej podpore.	***Spĺňa.*** *Súčasťou dodávky je služba Cortex XSIAM Premium Success (PAN-XSIAM-PREM-SUCCESS) na celé licenčné obdobie minimálne 36 mesiacov. Zahŕňa Premium Support, prístup k aktualizáciám a opravám, znalostnej báze, zákaznickemu portálu, správu servisných prípadov, eskaláciu problémov a technickú podporu.* *https://www.paloaltonetworks.com/resources/datasheets/sd-cortex-xsiam-premium-success* *https://www.paloaltonetworks.com/services/support/customer-support-plan*	**SPLNIL**
	Dostupnosť podpory minimálne v režime 24x7 pre kritické incidenty alebo ekvivalentný prémiový režim podpory s reakčnými časmi primeranými kritickosti bezpečnostnej platformy.	***Spĺňa.*** *Cortex XSIAM Premium Success zahŕňa prémiovú technickú podporu dostupnú online a telefonicky v režime 24 × 7 × 365. Pre incident úrovne Severity 1 – Critical je stanovený počiatočný reakčný čas kratší ako 1 hodina; kritické prípady možno eskalovať pridelenému technikovi alebo Duty Managerovi.* *https://www.paloaltonetworks.com/services/support/customer-support-plan*	**SPLNIL**

		https://www.paloaltonetworks.com/services/solution-assurance/premium-support	

1.2 Rozšírenie nástroja pre riadenie kybernetickej bezpečnosti

Rozšírenie existujúceho nástroja pre riadenie kybernetickej bezpečnosti			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek. Verejný obstarávateľ požaduje rozšírenie existujúceho nástroja pre riadenie kybernetickej bezpečnosti - Archer Platform SKU: RSA-0012000	*Uchádzač ponúka rozšírenie existujúceho riešenia nasledovne:* ***Výrobca:*** *Archer Technologies LLC* ***Produkt:*** *Archer Platform* ***Edícia/verzia:*** *výrobcom podporovaná verzia kompatibilná s existujúcou inštaláciou Archer Platform, SKU RSA-0012000* ***Licenčný model:*** *časovo obmedzené predplatné na 24 mesiacov podľa licenčnej metriky jednotlivých SKU* ***Relevantné komponenty:*** • *2× GRC-CYBINBR-S-T2 – Archer Cyber Incident & Breach Response, Tier 2* • *2× GRC-AIGOV-S-T2 – Archer AI Governance, Tier 2* *Komponenty predstavujú natívne rozšírenia existujúcej Archer Platform; nenahrádzajú základnú platformovú licenciu SKU: RSA-0012000.* *Overenie produktu:* https://www.archerirm.com/solutions https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response https://www.archerirm.com/ai-governance	**SPLNIL**
Modul riadenia umelej inteligencie		***Archer AI Governance (SKU GRC-AIGOV-S-T2)***	**SPLNIL**
Základná funkcionalita	Musí umožňovať centralizovanú evidenciu AI modelov, datasetov a AI služieb.	***Spĺňa****. Archer AI Governance (SKU GRC-AIGOV-S-T2) poskytuje centralizovaný inventár AI aktív. Umožňuje evidovať AI systémy, modely a služby vrátane súvisiacich datasetov a dátových zdrojov prostredníctvom konfigurovateľných záznamov a vzájomných väzieb.*	**SPLNIL**

		https://community.archerirm.com/hc/en-us/articles/52147275269267-Archer-AI-Governance https://www.archerirm.com/post/the-ai-inventory-is-becoming-a-board-level-record	
	Musí umožňovať evidenciu vlastníkov AI modelov a organizačných zodpovedností.	***Spĺňa**. Archer AI Governance umožňuje ku každému AI systému alebo modelu priradiť obchodného a technického vlastníka, organizačnú jednotku, schvaľovateľov, používateľov a ďalšie zodpovedné osoby alebo skupiny.* https://www.archerirm.com/post/the-ai-inventory-is-becoming-a-board-level-record	**SPLNIL**
	Musí podporovať klasifikáciu AI systémov podľa úrovne rizika a kritickosti.	***Spĺňa**. Archer AI Governance umožňuje kategorizovať AI aktíva podľa úrovne rizika, kritickosti, oblasti použitia a ďalších konfigurovateľných klasifikačných kritérií. Klasifikácia môže zohľadňovať aj rizikové kategórie podľa EU AI Act.* https://community.archerirm.com/hc/en-us/articles/52147275269267-Archer-AI-Governance	**SPLNIL**
	Musí umožňovať správu životného cyklu AI modelov od návrhu po vyradenie.	***Spĺňa**. Archer AI Governance v spojení s workflow Archer Platform umožňuje riadiť životný cyklus AI modelu od registrácie a návrhu cez posúdenie, schválenie, nasadenie a pravidelné prehodnocovanie až po vyradenie a archiváciu.* https://www.archerirm.com/post/use-the-eu-ai-act-to-build-a-global-ai-governance-model https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/advancedworkflow/adv_wrkflw_basics.htm	**SPLNIL**
	Musí umožňovať mapovanie AI modelov na procesy, aktíva a regulačné požiadavky.	***Spĺňa**. Relačný dátový model Archer Platform umožňuje prepojiť AI modely a prípady použitia s organizačnými procesmi, IT a dátovými aktívami, dodávateľmi, rizikami, kontrolnými opatreniami a regulačnými povinnosťami.* https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/fields/fld_xref_adding.htm https://www.archerirm.com/post/use-the-eu-ai-act-to-build-a-global-ai-governance-model	**SPLNIL**
	Musí podporovať hodnotenie rizík AI systémov vrátane etických a bezpečnostných rizík.	***Spĺňa**. Archer AI Governance poskytuje predpripravené a konfigurovateľné hodnotenia AI rizík vrátane etických, bezpečnostných, regulačných a privacy*	**SPLNIL**

		rizík. Výsledky hodnotení možno prepojiť s kontrolami, zisteniami a nápravnými opatreniami. *https://www.archerirm.com/ai-governance* *https://community.archerirm.com/hc/en-us/articles/52147275269267-Archer-AI-Governance*	
	Musí zabezpečovať auditovateľnosť zmien a logovanie činností používateľov.	***Spĺňa**. Archer Platform zaznamenáva históriu zmien údajov vrátane používateľa, času a zmenenej hodnoty. Administratívne auditné logy evidujú zmeny konfigurácie aplikácií, polí a ďalších platformových objektov.* *https://help.archerirm.cloud/platform_2024_11/en-us/content/platform/fields/fld_histlog_adding.htm* *https://help.archerirm.cloud/platform_202508/en-us/content/platform/installation/message_logging.htm*	**SPLNIL**
	Musí podporovať riadenie prístupov na základe rol.	***Spĺňa**. Archer Platform podporuje riadenie prístupu na základe používateľov, skupín a rolí. Oprávnenia možno nastaviť na úrovni systému, aplikácie, záznamu a jednotlivých polí vrátane práv na vytvorenie, čítanie, úpravu a odstránenie údajov.* *https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/accesscontrol/ac_accroles_assigning.htm*	**SPLNIL**
	Musí umožňovať integráciu s AI/ML platformami.	***Spĺňa**. Archer Platform umožňuje integráciu s externými AI/ML platformami prostredníctvom REST API, dátových feedov a importných mechanizmov. Integrované údaje možno využiť na aktualizáciu inventára AI modelov, metrík, rizikových ukazovateľov a stavu kontrol.* *https://help.archerirm.cloud/api_2025_04/content/api/webapi/api_access_configuration.htm* *https://help.archerirm.cloud/api_2025_04/content/api/restfulapi/segmentsresources/data_feed.htm*	**SPLNIL**
	Musí poskytovať dashboardy pre monitoring výkonnosti a rizík AI modelov.	***Spĺňa**. Archer Platform poskytuje konfigurovateľné dashboardy s reportmi, tabuľkami a grafmi na zobrazovanie rizík, výsledkov hodnotení, KPI, KRI a výkonnostných ukazovateľov AI modelov. Technické metriky možno automatizovane prenášať z AI/ML platformy prostredníctvom integračných rozhraní.*	**SPLNIL**

		https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/ui/ui_landing_dashboard.htm	
	Musí podporovať automatizované notifikácie pri prekročení definovaných limitov.	***Spĺňa**. Archer Platform umožňuje definovať podmienky a limity nad evidovanými hodnotami. Po ich splnení môže workflow automaticky odoslať notifikáciu, vytvoriť úlohu, aktualizovať stav záznamu alebo spustiť eskalačný proces.* https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/advancedworkflow/adv_wrkflw_basics.htm https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/notifications/note_basics.htm	**SPLNIL**
	Musí umožňovať monitoring súladu s požiadavkami AI regulácie.	***Spĺňa**. Archer AI Governance je navrhnutý v súlade s požiadavkami EU AI Act a podporuje evidenciu regulačných povinností, klasifikáciu AI systémov, mapovanie kontrol, vykonávanie hodnotení, zhromažďovanie dôkazov a reporting stavu súladu. Riešenie možno prispôsobiť aj ďalším AI regulačným rámcom.* https://www.archerirm.com/ai-governance https://community.archerirm.com/hc/en-us/articles/52147275269267-Archer-AI-Governance	**SPLNIL**
Modul riadenia kybernetických incidentov a narušení bezpečnosti		***Archer Cyber Incident & Breach Response (SKU GRC-CYBINBR-S-T2)***	**SPLNIL**
Základná funkcionalita	Musí umožňovať centralizovanú evidenciu bezpečnostných incidentov.	***Spĺňa**. Archer Cyber Incident & Breach Response (SKU GRC-CYBINBR-S-T2) poskytuje centrálny register bezpečnostných udalostí a incidentov s jednotnou taxonómiou, klasifikáciou, prioritou, stavom, vlastníkom a súvisiacimi aktívami.* https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response	**SPLNIL**
	Musí podporovať životný cyklus incidentov vrátane eskalácie a uzatvorenia.	***Spĺňa**. Archer Cyber Incident & Breach Response podporuje riadený životný cyklus incidentu zahŕňajúci registráciu, triáž, klasifikáciu, pridelenie, eskaláciu, vyšetrovanie, reakciu, vyriešenie a uzatvorenie. Proces je riadený konfigurovateľným workflow.* https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response	**SPLNIL**

		https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/advancedworkflow/adv_wrkflw_basics.htm	
	Musí umožňovať správu nápravných opatrení a úloh.	***Spĺňa**. Archer Cyber Incident & Breach Response umožňuje evidovať nápravné opatrenia, priraďovať zodpovedné osoby, termíny a stav realizácie. Advanced Workflow podporuje automatické vytváranie úloh, aktualizáciu záznamov a odosielanie upozornení.* https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/advancedworkflow/adv_wrkflw_basics.htm	**SPLNIL**
	Musí podporovať integráciu so SIEM, EDR a log management riešeniami.	***Spĺňa**. Archer Cyber Incident & Breach Response podporuje integráciu so SIEM, log management, packet capture a endpoint security/EDR technológiami. Bezpečnostné udalosti a súvisiace údaje možno prenášať prostredníctvom dátových feedov alebo integračných API.* https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/integration/int_dfm_basics.htm	**SPLNIL**
	Musí umožňovať evidenciu forenzných aktivít a dôkazov.	***Spĺňa**. Archer Cyber Incident & Breach Response podporuje vedenie incidentného denníka, evidenciu forenzných analýz, vykonaných vyšetrovacích činností a súvisiacich dôkazov. Informácie a elektronické dôkazy sú uchovávané vo väzbe na konkrétny incident.* https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response https://community.archerirm.com/hc/en-us/articles/52147821708051-Next-Generation-Security-Operations-Telescopes-for-the-Lookouts	**SPLNIL**
	Musí podporovať hodnotenie dopadov incidentov na organizáciu.	***Spĺňa**. Archer Cyber Incident & Breach Response prepája incidenty s organizačnými a IT aktívami a využíva ich obchodný kontext na posúdenie dopadu, rizika a priority incidentu. Súčasťou funkcionality je aj hodnotenie rizika narušenia bezpečnosti.*	**SPLNIL**

		https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response	
	Musí zabezpečovať auditovateľnosť všetkých vykonaných činností.	***Spĺňa**. Archer Platform zaznamenáva históriu zmien incidentných záznamov vrátane používateľa, času a zmenených hodnôt. Auditovateľné sú tiež prechody workflow, aktualizácie úloh a administratívne zmeny konfigurácie.* https://help.archerirm.cloud/platform_2024_11/en-us/content/platform/fields/fld_histlog_adding.htm https://help.archerirm.cloud/platform_202508/en-us/content/platform/installation/message_logging.htm	**SPLNIL**
	Musí podporovať automatizovanú koreláciu incidentov.	***Spĺňa**. Archer Platform umožňuje automatizovane identifikovať a prepájať súvisiace incidenty a bezpečnostné udalosti podľa konfigurovateľných korelačných atribútov, napríklad identifikátora, zdroja, aktíva, kategórie alebo iného spoločného kľúča. Korelácia sa realizuje pomocou kľúčov dátových feedov, dynamických filtrov a vypočítaných väzieb medzi záznamami.* https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/integration/int_dfm_basics.htm https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/fields/fld_x-ref_dynamic_filters.htm	**SPLNIL**
	Musí umožňovať integráciu so SOAR platformami.	***Spĺňa**. Archer Cyber Incident & Breach Response umožňuje integráciu so SOAR platformami prostredníctvom REST API a dátových feedov. Integrácia umožňuje výmenu incidentov, stavov, priorít, úloh a výsledkov vykonaných SOAR playbookov.* https://help.archerirm.cloud/api_2025_04/content/api/webapi/api_access_configuration.htm https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/integration/int_dfm_basics.htm	**SPLNIL**
	Musí poskytovať SOC dashboardy a reporting.	***Spĺňa**. Archer Cyber Incident & Breach Response poskytuje konsolidované analýzy a reporting incidentov. Konfigurovateľné dashboardy umožňujú SOC tímu sledovať počet, závažnosť, stav, trend, čas riešenia, eskalácie a ďalšie ukazovatele incidentov prostredníctvom tabuliek a grafov.*	**SPLNIL**

		https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response *https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/ui/ui_landing_dashboard.htm*	
	Musí umožňovať automatizované eskalácie incidentov.	***Spĺňa**. Archer Cyber Incident & Breach Response podporuje automatizované eskalácie podľa závažnosti, priority, stavu, času alebo iných definovaných podmienok. Advanced Workflow môže incident presmerovať, zmeniť jeho stav, vytvoriť úlohu a odoslať notifikáciu príslušným osobám.* *https://community.archerirm.com/hc/en-us/articles/52147447048851-Archer-Cyber-Incident-Breach-Response* *https://help.archerirm.cloud/platform_2025_04/en-us/content/platform/advancedworkflow/adv_wrkflw_basics.htm*	**SPLNIL**
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca inštaláciu a nastavenie pre preukázanie funkčnosti a prevádzkyschopnosti dodaného rozšírenia existujúceho nástroja pre riadenie kybernetickej bezpečnosti. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať inštaláciu a nastavenie dodávaného rozšírenia existujúceho nástroja pre riadenie kybernetickej bezpečnosti. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané rozšírenie existujúceho nástroja pre riadenie kybernetickej bezpečnosti.	• *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie pre preukázanie funkčnosti a prevádzkyschopnosti dodaného rozšírenia existujúceho nástroja pre riadenie kybernetickej bezpečnosti.* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať inštaláciu a nastavenie dodávaného rozšírenia existujúceho nástroja pre riadenie kybernetickej bezpečnosti.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Archer Certified Administrator – Expert vydaný výrobcom Archer ACADEMY, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané rozšírenie existujúceho nástroja pre riadenie kybernetickej bezpečnosti.*	**SPLNIL**

Servisná podpora	Servisná podpora na obdobie 2 rokov v mieste inštalácie v režime 8x5 NBD	***Spĺňa**. Uchádzač zabezpečí servisnú podporu dodaného rozšírenia Archer Platform počas 24 mesiacov v režime 8×5 NBD. Podpora bude poskytovaná v pracovných dňoch osem hodín denne. Ak incident nebude možné odstrániť vzdialene, servisný zásah v mieste inštalácie sa začne najneskôr nasledujúci pracovný deň. Súčasťou služby je diagnostika, riešenie incidentov, odstraňovanie chýb a eskalácia produktových problémov na technickú podporu výrobcu.*	**SPLNIL**
	Servisná podpora musí byť realizovaná priamo vendorom, alebo jeho lokálnym autorizovaným servisným partnerom (zastúpením).	***Spĺňa**. Servisnú podporu bude poskytovať priamo vendor.*	**SPLNIL**
	Jednotný kontakt pre nahlasovanie servisných incidentov	***Spĺňa**. Verejnému obstarávateľovi bude počas celej doby podpory poskytnutý jednotný kontaktný pre nahlasovanie servisných incidentov.*	**SPLNIL**
	V rámci služby musí záujemca pre verejného obstarávateľa zabezpečiť: • prístup k továrenskej expertíze vendora za účelom riešenia komplexných problémov, • zrýchlené riešenie eskalácií na úrovni engineeringu, • prístup do elektronickej databázy riešení problémov, • prístup k vzdialeným elektronickým diagnostickým nástrojom.	***Spĺňa**. V rámci servisnej podpory uchádzač zabezpečí:* • *prístup k technickým expertom Archer Technical Support na riešenie komplexných produktových problémov,* • *riadenú a zrýchlenú eskaláciu potvrdených produktových chýb na príslušný produktový a engineeringový tím výrobcu,* • *prístup do Archer Community, ktorá obsahuje znalostnú databázu, technickú dokumentáciu, známe problémy, opravné verzie a odporúčané postupy riešenia,* • *vzdialenú diagnostiku prostredia vrátane bezpečnej vzdialenej relácie a analýzy diagnostických údajov, konfiguračných informácií, chybových hlásení, logov a trace súborov.* *Uchádzač bude voči verejnému obstarávateľovi zodpovedný za koordináciu riešenia až do uzatvorenia servisného incidentu.*	**SPLNIL**

1.3 Centrálny firewall systém

Centrálny firewall systém			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Check Point Software Technologies Ltd. – Check Point Quantum Maestro Hyperscale Security v edícii Maestro/MHS HyperScale, pozostávajúci z 2× Maestro Hyperscale Orchestrator MHO-140 (CPAP-MHO-140) a 4× Quantum Force 9100 Plus MHS so SandBlast balíkom (CPAP-SG9100-PLUS-MHS-SNBT).* ***Licenčný model je založený na fyzických appliance a časovo obmedzených subscription licenciách****: SNBT na 1 rok pre každú appliance, NGTP na ďalší 1 rok pre 4 appliance a SD-WAN na 2 roky pre 2 appliance.* *Technická špecifikácia:* • *4x CPAC-TR-100SR4-DM* • *4x CPAP-SG9100-PLUS-MHS-SNBT* • *2x CPSB-SDWAN-9100-PLUS-2Y* • *4x CPSB-NGTP-9100-PLUS-1Y* • *20 CPAC-TR-10SR-D* • *2x CPAP-MHO-140* • *20x CPAC-TR-1SX-D* • *4x CPAC-RAM32GB-9100/9400-INSTALL*	**SPLNIL**
Predmet dodania:	Centrálny firewall systém predstavuje ucelený hyperškálovací systém alebo cluster, ktorý je tvorený dostatočným počtom zariadení pre spracovanie definovaného objemu prevádzky, fyzické oddelenie firewall hardvéru pre jednotlivé inštancie a s požadovanými bezpečnostnými funkciami.	***Spĺňa****.* *Centrálny firewall tvorí hyperškálovací systém Check Point Maestro pozostávajúci z redundantnej dvojice 2× Maestro Hyperscale Orchestrator MHO-140 a 4× fyzických appliance Check Point Quantum Force 9100 Plus MHS. Každá požadovaná firewallová inštancia je realizovaná ako samostatná Maestro Security Group. Prvej Security Group sú výlučne pridelené dve appliance 9100 Plus MHS a druhej Security Group zostávajúce dve appliance 9100 Plus MHS. Žiadna fyzická appliance ani jej výkonové prostriedky nie sú súčasne pridelené alebo zdieľané medzi Security Groups. Každá Security Group má zároveň pridelené vlastné sieťové porty orchestrátorov, vlastnú*	**SPLNIL**

		bezpečnostnú politiku a samostatný prevádzkový kontext. Dvojica fyzických appliance v každej Security Group pracuje v režime Active/Active s distribúciou prevádzky a redundanciou. Požadované bezpečnostné funkcie Threat Prevention a sandboxing zabezpečuje balík SandBlast SNBT a nadväzujúce licencie NGTP. Fyzické oddelenie je preto zabezpečené vyhradenými firewallovými uzlami, nie iba logickým oddelením virtuálnych systémov na spoločnom dátovom hardvéri. *https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/Introduction.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Configuring-Security-Groups-Workflow.htm* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf* *https://www.checkpoint.com/quantum/advanced-network-threat-prevention/*	
Počet:	1 ks – ucelený hyperškálovací systém alebo cluster, počet jednotlivých typov zariadení dostatočný na splnenie podmienok	***Spĺňa***. *Ponúkaný 1 ks uceleného hyperškálovacieho systému Check Point Maestro pozostáva z 1× orchestrátora MHO-140 a 4× fyzických firewallov Check Point Force 9100 Plus MHS. Zariadenia pracujú ako jednotný škálovateľný Active/Active systém s automatickou distribúciou prevádzky; ich počet a výkon sú dimenzované na splnenie požadovaných podmienok.* *https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Maestro_AdminGuide/Content/Topics-Maestro-AG/Introduction.htm* *https://www.checkpoint.com/quantum/force/9100/*	**SPLNIL**
Požiadavky:	• systém alebo klaster musí umožňovať spracovanie prevádzky z pripojených monitorovaných lokalít. V úvodnej konfigurácii musí podporovať najmenej 4 monitorované lokality a musí byť výrobcom podporovaným spôsobom škálovateľný na najmenej 25	***Spĺňa***. • *Riešenie bude nakonfigurované ako dve samostatné Maestro Security Groups, každá s 2× Quantum Force 9100 Plus MHS. Prvá skupina s licenciami Quantum SD-WAN zabezpečí ingest prevádzky minimálne zo 4 monitorovaných lokalít prostredníctvom SD-WAN Overlay/Site-to-Site VPN; druhá skupina zabezpečí interné bezpečnostné spracovanie v dátovom centre. Rozšírenie na minimálne 25 lokalít sa realizuje pridávaním ďalších podporovaných SD-WAN/VPN peerov bez zmeny*	**SPLNIL**

	monitorovaných lokalít. Prevádzka bude spracovávaná na dvoch úrovniach – ingest prostredníctvom SD-WAN a interné spracovanie v rámci dátového centra.
	• systém alebo klaster musí umožňovať postupné rozširovanie výkonu pridávaním výrobcom podporovaných výkonných členov alebo komponentov podľa reálnych požiadaviek prostredia NCZI SOC.
	• v úvodnej konfigurácii v režime N musí riešenie dosahovať:
	  ○ najmenej 30 Gbps pre NGFW,
	  ○ najmenej 10 Gbps pre SD-WAN.
	• v cieľovej rozšírenej konfigurácii v režime N+1 musí riešenie dosahovať:
	  ○ viac ako 200 Gbps pre NGFW,
	  ○ najmenej 50 Gbps pre SD-WAN.
	• v režime N+1 musia byť uvedené výkonnostné parametre zachované aj po výpadku jedného výkonného člena. Riešenie musí zároveň umožňovať ďalšie budúce rozširovanie výkonu nad uvedené hodnoty výrobcom podporovaným spôsobom.
	• parametre NGFW a SD-WAN sa posudzujú samostatne podľa príslušných výkonnostných metrík, pričom ich musí podporovať rovnaká ponúkaná architektúra riešenia.
		architektúry centrálnej Maestro platformy. Nasadená bude verzia R82.10 alebo vyššia.
		Check Point uvádza podporu SD-WAN na Maestro Security Groups a škálovanie až na 1 500 gatewayov v jednej management doméne:
		https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/SD-WAN-with-Maestro.htm
		https://sc1.checkpoint.com/documents/SmartConsole/WhatsNew.html
		https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/SD-WAN-Connection-Types.htm
		https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/Quick-Start-MHO-140-Single-Site-2-Orchestrators.htm
		• *Check Point Quantum Maestro predstavuje scale-out architektúru, ktorá umožňuje postupne zvyšovať výkon pridaním ďalších výrobcom podporovaných členov Quantum Force 9100 Plus MHS do príslušnej Security Group. Maestro automaticky rozloží prevádzku medzi aktívne členy a nový člen prevezme softvér, konfiguráciu a bezpečnostné politiky zo SMO člena. Rozšírenie nevyžaduje výmenu existujúcich zariadení; v R82 je podporovaných až 28 Security Appliances v jednej Maestro Security Group.*
		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Working-with-Maestro.htm
		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Introduction.htm
		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Maximum-Supported-Items.htm
		• *Požiadavka je splnená v úvodnej fáze N a v cieľovej fáze N+1 nasledujúcou výrobcom podporovanou konfiguráciou. Dva*	

	• ak výrobca nepublikuje samostatný parameter „SD-WAN Throughput“, kapacita riešenia pre SD-WAN sa bude posudzovať podľa výrobcom deklarovaného parametra „IPsec VPN Throughput“, pokiaľ ponúkané riešenie realizuje SD-WAN prevádzku prostredníctvom IPsec VPN tunelov. • za dostatočné preukázanie parametra „IPsec VPN Throughput“ sa považuje uvedenie funkčného priameho odkazu na verejne dostupnú oficiálnu technickú dokumentáciu alebo produktovú stránku výrobcu, v ktorej je pre ponúkaný model deklarovaná príslušná hodnota. Samostatné potvrdenie výrobcu sa nevyžaduje. • pri klastrovom alebo škálovateľnom riešení sa výsledná kapacita SD-WAN určí podľa výrobcom dokumentovaného spôsobu výpočtu a pravidiel škálovania výkonu pre ponúkanú architektúru. Jednoduché sčítanie výkonov jednotlivých členov možno použiť iba vtedy, ak takýto spôsob výpočtu podporuje výrobca. • uchádzač v ponuke uvedie model a počet členov v úvodnej aj cieľovej konfigurácii a predloží výpočet podľa metodiky výrobcu spolu s funkčným priamym odkazom na príslušnú oficiálnu dokumentáciu výrobcu.	*redundantne zapojené orchestrátory Check Point Maestro MHO-140 budú prevádzkovať dve samostatné Active/Active Security Groups:* ○ *SG-NGFW – interné spracovanie prevádzky v dátovom centre,* ○ *SG-SD-WAN – spracovanie SD-WAN Overlay prevádzky; všetky jej členy budú vybavené licenciou Check Point SD-WAN.* *Check Point Force 9100 má výrobcom deklarovaný výkon 18,6 Gbps NGFW a 22,1 Gbps VPN AES-GCM pri veľkosti paketu 1452 B. Keďže Check Point SD-WAN Overlay vytvára šifrované Site-to-Site IPsec VPN tunely, parameter VPN AES-GCM predstavuje vstupný výkonnostný parameter použitý v sizingu SD-WAN časti riešenia.* *Výkonnostné hodnoty sú doložené priloženým sizingovým výpočtom potvrdeným výrobcom Check Point. Výpočet zohľadňuje režijnú záťaž Maestro vo výške 1 % za každý člen Security Group; pri výpočte výkonu po výpadku sa konzervatívne zachováva koeficient podľa pôvodného počtu nainštalovaných členov.* **Konfigurácia** | **Počet členov** | **Aktívne členy vo výpočte** | **Výpočet** | **Výsledok** **Úvodná N – NGFW** | 2× Force 9100 Plus MHS | 2 | 2 × 18,6 × 0,98 | **36,46 Gbps** **Úvodná N – SD-WAN** | 2× Force 9100 Plus MHS s licenciou SD-WAN | 2 | 2 × 22,1 × 0,98 | **43,32 Gbps** **Cieľová N+1 – NGFW po výpadku** | 14 nainštalovaných (N = 13 + 1) | 13 | 13 × 18,6 × 0,86 | **207,95 Gbps** **Cieľová N+1 – SD-WAN po výpadku** | 4 nainštalované (N = 3 + 1) | 3 | 3 × 22,1 × 0,96 | **63,65 Gbps** *V cieľovej konfigurácii pracujú všetky členy Active/Active. Pri výpadku jedného fyzického člena ho Maestro vyradí zo spracovania a prevádzku distribuuje medzi zostávajúce aktívne členy. Po výpadku zostáva k dispozícii 207,95 Gbps NGFW, resp. 63,65 Gbps SD-WAN Overlay, takže požadované hodnoty minimálne 200 Gbps NGFW a 50 Gbps SD-WAN zostávajú zachované.* *Cieľová konfigurácia vznikne rozšírením pôvodných Security Groups prevádzkovaných na rovnakej redundantnej dvojici MHO-140. Pôvodne dodané zariadenia zostanú členmi svojich Security Groups a nebudú nahradené ani presunuté do samostatného clustra.*	

	Do výpočtu možno zahrnúť iba aktívne členy s požadovanou SD-WAN licenciou. • pri režime N+1 musí výpočet podľa metodiky výrobcu zohľadňovať výpadok jedného výkonného člena, pričom zostávajúca kapacita musí dosahovať najmenej 50 Gbps pre SD-WAN. • parametre Firewall Throughput, NGFW Throughput, IPS Throughput ani Threat Protection Throughput nemožno použiť ako náhradu parametra SD-WAN Throughput alebo IPsec VPN Throughput. • musí umožniť vytvárať virtuálne inštancie firewallov a dynamický presun HW zdrojov medzi nimi, • musí umožňovať jednoduché zaradenie nového zariadenia do systému / clustera pomocou automatickej konfigurácie systémom / clusterom, • podpora rôznych modelov zariadení v rámci systému / clustera tak, aby bolo možné v budúcnosti integrovať nové modely výrobcu bez výmeny pôvodných zariadení.	*Pôvodná SG-NGFW s 2× Force 9100 Plus MHS sa rozšíri pridaním ďalších 12 podporovaných uzlov na celkových 14 členov. Finálny výkon nad 200 Gbps NGFW bude teda dosiahnutý výhradne pridaním uzlov do tej istej spoločnej Active/Active Security Group obsahujúcej pôvodne dodané zariadenia. Po výpadku jedného člena zostane aktívnych 13 uzlov s výkonom 207,95 Gbps NGFW.* *Pôvodná SG-SD-WAN s 2× Force 9100 Plus MHS sa rozšíri pridaním ďalších 2 uzlov na celkových 4 členov. Po výpadku jedného člena zostanú aktívne 3 uzly s výkonom 63,65 Gbps SD-WAN Overlay.* *Cieľová konfigurácia bude obsahovať celkovo 18× Force 9100 Plus MHS. Oproti úvodnej konfigurácii sa doplní 14 zariadení: 12 do existujúcej SG-NGFW a 2 do existujúcej SG-SD-WAN, vrátane príslušných licencií, rozšírenia RAM na 64 GB a potrebných prepojovacích komponentov. Pre SG-SD-WAN sa zároveň doplnia dve licencie Check Point SD-WAN.* *Na dosiahnutie požadovaného výkonu sa nevytvára nový HA cluster, nepoužíva sa externé rozdeľovanie NGFW prevádzky medzi clustre a pôvodne dodané zariadenia sa nenahrádzajú. Check Point R82 podporuje maximálne 28 Security Appliances v jednej Maestro Security Group, preto možno existujúcu SG-NGFW ďalej rozširovať pri dodržaní kompatibility zariadení, kapacity orchestrátorov, portovej konfigurácie a licenčných podmienok.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf* *https://support.checkpoint.com/results/sk/sk147853* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Maximum-Supported-Items.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Common/Working-with-Distribution-Mode.htm*	

		https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/SD-WAN-Connection-Types-Overlay.htm
		https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/Connecting-Two-Maestro-Hyperscale-Orchestrators-for-Redundancy.htm
		• *Splnené v cieľovej konfigurácii N+1. Riešenie bude obsahovať dve Security Groups v rovnakej Maestro/MHS architektúre:*
		  ○ *SG-NGFW: 14× Force 9100 Plus MHS; po výpadku zostáva 13 členov:*
		  13×18,6×0,86=207,95 Gbps
		  ○ *SG-SD-WAN: 4× aktívny a licencovaný Force 9100 Plus MHS; po výpadku zostávajú 3 členy:*
		  3×22,1×0,96=63,65 Gbps
		Aj po výpadku jedného člena zostáva zachovaný výkon vyšší ako 200 Gbps NGFW a minimálne 50 Gbps SD-WAN. Maestro automaticky prerozdelí prevádzku medzi zostávajúce aktívne členy.
		Ďalšie rozširovanie je podporované pridávaním rovnakých licencovaných členov Force 9100 Plus MHS. Check Point R82.10 podporuje až 28 členov v jednej Maestro Security Group; dostupná je aj funkcia Maestro Auto-Scaling.
		https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf
		https://support.checkpoint.com/results/sk/sk147853
		https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_RN/Content/Topics-RN/Maximum-Supported-Items.htm
		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Auto-Scaling.htm
		• *Rovnaká architektúra Check Point Maestro/MHS s 2× MHO-140 a členmi Force 9100 Plus MHS podporuje NGFW aj Quantum SD-WAN.*	

		Parametre sa vyhodnocujú samostatne: 18,6 Gbps NGFW a 22,1 Gbps VPN AES-GCM na jeden člen. SD-WAN a NGFW môžu byť prevádzkované v samostatných Security Groups tej istej Maestro platformy. *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf* *https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/SD-WAN-with-Maestro.htm* • *Výrobca pre Force 9100 neuvádza samostatnú metriku „SD-WAN Throughput“, preto sa používa hodnota VPN AES-GCM 1452B – 22,1 Gbps. Check Point Quantum SD-WAN Overlay realizuje komunikáciu medzi pobočkou a centrálnou lokalitou prostredníctvom šifrovaných Site-to-Site VPN tunelov.* *https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/SD-WAN-Connection-Types-Overlay.htm* • *Oficiálny verejne dostupný produktový list výrobcu deklaruje pre ponúkaný model Check Point Force 9100 parameter VPN AES-GCM 1452B: 22,1 Gbps. Samostatné potvrdenie výrobcu preto nie je potrebné.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf* • *Kapacita nie je určená jednoduchým sčítaním výkonov. Používa sa metodika Check Point Maestro so znížením výslednej kapacity o 1 % za každý člen Security Group. Výrobca uvádza napríklad výkon dvoch členov ako 196 % výkonu jedného člena.* *Použitý výpočet:* $P(n)=n\times P1\times(1-0{,}01n)$ *https://support.checkpoint.com/results/sk/sk147853*	

		https://community.checkpoint.com/t5/Hyperscale-Firewall-Maestro/Maestro-Masters-Round-Table-Selected-Questions-Part-1/td-p/151464 • *Úvodná konfigurácia: 4× CPAP-SG9100-PLUS-MHS-SNBT, rozdelené na 2× SG-NGFW a 2× SG-SD-WAN. Do SD-WAN výpočtu vstupujú iba 2 aktívne a licencované členy:* *2×22,1×0,98=43,32 Gbps* *Cieľová konfigurácia: celkovo 18× Force 9100 Plus MHS – 14 členov SG-NGFW a 4 aktívne členy SG-SD-WAN. Všetky štyri SD-WAN členy musia mať platnú SD-WAN licenciu. Cieľová konfigurácia preto vyžaduje doplnenie dvoch ďalších SD-WAN licencií.* *Všetky členy použité pre deklarovanú NGFW metriku budú vybavené 64 GB RAM.* https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_RN/Content/Topics-RN/Maximum-Supported-Items.htm • *Splnené v cieľovej konfigurácii N+1. SG-SD-WAN obsahuje štyri aktívne a licencované členy Force 9100. Po výpadku jedného člena zostávajú tri aktívne členy. Pri konzervatívnom zachovaní 4 % penalizácie pôvodnej štvorčlennej skupiny:* *3×22,1×0,96=63,65 Gbps* *Zostávajúca kapacita je vyššia než požadovaných 50 Gbps.* https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf https://support.checkpoint.com/results/sk/sk147853 • *Na výpočet SD-WAN kapacity sa používa výhradne výrobcom deklarovaný parameter VPN AES-GCM 1452B – 22,1 Gbps. Hodnoty Firewall Throughput, NGFW Throughput, IPS Throughput ani Threat Prevention Throughput sa ako náhrada nepoužívajú.* https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf	

		• *Ponúkané riešenie Check Point Quantum Maestro vo verzii R82 s technológiou VSNext umožňuje vytvárať samostatné Virtual Gateways – virtuálne firewallové inštancie. Na zabezpečenie požadovaného fyzického oddelenia sú produkčné firewallové inštancie realizované ako samostatné Maestro Security Groups.* *Funkcia Maestro Auto-Scaling pracuje s celou fyzickou appliance Check Point Quantum Force 9100 Plus MHS ako so „Scale Unit“. Za prevádzky umožňuje celý fyzický uzol odobrať zo zdrojovej Security Group a prideliť ho cieľovej Security Group, automaticky podľa nastavených pravidiel zaťaženia CPU, priepustnosti, počtu paketov alebo spojení, prípadne manuálnym zásahom administrátora. Fyzický uzol je v danom čase pridelený výlučne jednej Security Group a nie je medzi skupinami súčasne zdieľaný.* *Po priradení uzla zabezpečí SMO Image Cloning prenos požadovaných softvérových balíkov a mechanizmus SMO automaticky prenesie na nový člen aktuálnu bezpečnostnú politiku a konfiguráciu príslušnej Security Group. Zmena počtu CoreXL Firewall Instances na úrovni Virtual Gateway je doplnkovou možnosťou riadenia výkonu; splnenie požiadavky na dynamický presun HW zdrojov je založené na presune celých fyzických appliance medzi Security Groups.* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Auto-Scaling.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Configuring-Security-Groups-in-Gaia-Portal.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Common/Policy-Management-on-Security-Group-Members.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_VSX_AdminGuide/Content/Topics-VSXG/VSNext.htm* • *Po priradení nového podporovaného zariadenia, napríklad ďalšieho Quantum Force 9100 Plus MHS, do existujúcej homogénnej Maestro*	

		Security Group zariadenie automaticky naklonuje všetky softvérové balíky, nastavenia a bezpečnostné politiky z člena SMO. Nový člen preto nie je potrebné konfigurovať samostatne. *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Working-with-Maestro.htm* • *Ponúkané riešenie Check Point Quantum Maestro od verzie R81.10, vrátane ponúkanej verzie R82, podporuje funkciu Mix and Match. Tá umožňuje súčasnú produkčnú prevádzku rozdielnych podporovaných modelov Check Point Security Appliances ako členov jednej Maestro Security Group plniacej funkciu spoločného Active/Active clustra. Nový model zariadenia možno v budúcnosti pridať priamo do existujúcej Security Group bez výmeny pôvodných appliance Check Point Quantum Force 9100 Plus MHS, ak použitý orchestrátor daný model podporuje a konkrétna kombinácia je výrobcom uvedená ako podporovaná na produkčnú prevádzku v kompatibilitnej matici sk162373.* *Rozdielny výkon členov Security Group možno zohľadniť nastavením relatívnych váh, podľa ktorých Maestro rozdeľuje prevádzku medzi fyzické uzly. Nejde teda o viacero samostatných HA clusterov pod spoločnou správou, ale o rozdielne hardvérové modely pracujúce v jednej spoločnej Security Group.* *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Common/SGM-Weights.htm* *https://support.checkpoint.com/results/sk/sk162373*	
Technické vlastnosti:	Centrálny firewall systém musí na minimálne 24 mesiacov funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality: • plne automatizovaná infraštruktúra, • podpora vysokej dostupnosti vo forme A/A, A/S, cluster,	***Spĺňa***. • *Ponúkané riešenie bude počas minimálne 24 mesiacov licenčne pokrývať NGFW/NGTP, SandBlast Threat Emulation, URL Filtering, SD-WAN, virtuálne systémy, centrálny manažment, aktualizácie a technickú podporu.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf*	**SPLNIL**

	• spôsob nasadenia: Layer 2 (transparent), Layer 3 (routing) mode
	• podpora funkcií firewallu novej generácie (next-gen firewall / NGFW):
	  ○ firewall, aplikačná inšpekcia / aplikačná kontrola, IDS/IPS, anti bot, identity awareness, anti-malware kontrola,
	  ○ podpora pre: kontrolu prenášaných súborov pomocou on-prem sandboxu, URL filtering,
	• podpora funkčnosti inštancie ako HUB SDWAN riešenia s požadovanou kapacitou,
	• výkon riešenia:
	  ○ v úvodnej fáze: 30 Gbps NGFW + 10Gbps SDWAN (N),
	  ○ vo finálnom riešení: 200 Gbps + 50 Gbps SDWAN (N+1),
	  ○ možnosť plynulo škálovať v prípade budúcej potreby,
	• podpora virtuálnych inštancií firewallu
	  ○ v úvodnej fáze 2 inštancie,
	  ○ možnosť pridať ďalšie inštancie (zmenou / doplnením licencie a doplnením potrebného počtu a
		• *Check Point Maestro automaticky distribuuje prevádzku medzi členov Security Group, podporuje automatické škálovanie podľa CPU, priepustnosti, PPS alebo počtu spojení a automatické prevzatie softvéru, konfigurácie a bezpečnostných politík novým členom.* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Auto-Scaling.htm*
		• *Maestro Security Group pracuje ako Active/Active cluster s automatickou distribúciou prevádzky. Firewally Force 9100 zároveň podporujú Active/Active L2, Active/Standby L2 a L3, ClusterXL a VRRP.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf*
		• *Check Point Force 9100 a Maestro Security Groups podporujú transparentný Layer 2/Bridge režim aj Layer 3/Routing režim vrátane statického a dynamického smerovania.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf*
		• *Ponúkané licencie NGTP/SNBT zabezpečujú Stateful Firewall, Application Control, URL Filtering, IPS s režimom detekcie alebo prevencie, Anti-Bot, Anti-Virus/Anti-Malware a Identity Awareness.*
		https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf
		https://www.checkpoint.com/next-generation-firewall/identity-awareness/
		• *Požiadavka je splnená prostredníctvom Check Point SandBlast Threat Emulation a URL Filtering. Súbory môžu byť analyzované v lokálnom on-prem sandboxe alebo odoslané na vzdialený on-prem Threat Emulation appliance. Pre virtuálne systémy VSX/VSNext sa použije vzdialený on-prem Threat Emulation zdroj.* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/Content/Topics-TPG/Threat-Emulation-Solution.htm*	

	modelov zariadení) vo fáze prevádzky, ○ možnosť plne integrovať virtuálne inštancie firewallov do SDN vo forme virtualizácie sieťových služieb (Network functions virtualization / NFV), • REST API pre integráciu s automatizačnými / orchestračnými systémami a nástrojmi, • centrálny manažment s podporou správy a prevádzky navrhovaného počtu virtuálnych inštancií firewallu, • centralizovaný zber, spracovanie a možnosť lokálnej analýzy logov z celého riešenia, • podpora integrácie a monitorovania riešenia s dodávanou Enterprise bezpečnostnou analytickou platformou typu XDR/SIEM/SOAR,	• *Centrálna Maestro Security Group môže pracovať ako Headquarters/Center Gateway v SD-WAN topológii HUB-and-Spoke. Podporované sú šifrované overlay tunely, dynamické riadenie prevádzky a režim Backhaul, pri ktorom je prevádzka pobočiek smerovaná cez centrálny HUB na bezpečnostnú kontrolu. Konfigurácia obsahuje dvojročnú SD-WAN licenciu pre Force 9100 Plus.* *https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/SD-WAN-Connection-Types.htm* • *V úvodnej fáze možno 4× Force 9100 rozdeliť medzi dve Security Groups:* ○ *2× 9100 pre NGFW: 37,2 Gbps,* ○ *2× 9100 pre SD-WAN: 44,2 Gbps VPN AES-GCM.* *Finálny stav N+1 možno dosiahnuť postupným doplnením výkonnejších Maestro členov bez výmeny pôvodných zariadení. Referenčné dimenzovanie predstavujú 4× Force 9800 MHS pre NGFW, ktoré po výpadku jedného člena poskytujú 203,1 Gbps, a pôvodné 4× Force 9100 pre SD-WAN, ktoré po výpadku člena poskytujú 66,3 Gbps VPN AES-GCM. Maestro umožňuje ďalšie škálovanie pridávaním podporovaných appliance.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf* *https://www.checkpoint.com/downloads/products/quantum-force-9800-datasheet.pdf* • *Požiadavka je splnená technológiou Check Point VSNext vo verzii R82. V úvodnej fáze budú vytvorené dve samostatné Virtual Gateways – virtuálne firewallové inštancie:* ○ *VGW-NGFW v Security Group SG-NGFW s vyhradenými 2× Force 9100 Plus MHS,* ○ *VGW-SD-WAN v Security Group SG-SD-WAN s vyhradenými 2× Force 9100 Plus MHS.* *Každá Virtual Gateway sa správa ako samostatný Security Gateway a disponuje vlastnými sieťovými rozhraniami, routingom, bezpečnostnými*	

			politikami a prevádzkovým kontextom. Umiestnením každej Virtual Gateway do samostatnej Security Group je zároveň zabezpečené, že jednotlivé inštancie nezdieľajú fyzické firewallové uzly. *Počas prevádzky možno pridávať ďalšie virtuálne firewallové inštancie. Pri zachovaní fyzického oddelenia sa každá ďalšia inštancia vytvorí ako VSNext Virtual Gateway v novej Maestro Security Group, ktorej bude pridelený výlučný súbor doplnených fyzických Security Appliances.* *Rozšírenie zahŕňa doplnenie licencií Virtual Systems, príslušných licencií bezpečnostných funkcií a podľa potreby rozšírenie centrálneho managementu. Ponúkaná licencia CPSM-NGSM25-PREMIUM poskytuje kapacitu na správu 25 gateway inštancií. Check Point R82 podporuje v jednom Maestro systéme maximálne osem samostatných Security Groups.* *V súlade s vysvetlením verejného obstarávateľa sú virtuálne firewallové inštancie prevádzkované priamo v rámci fyzickej platformy Maestro a ich integrácia do SDN/NFV je realizovaná prostredníctvom dokumentovaných rozhraní Gaia REST API a Check Point Management API. Externý SDN/NFV orchestrátor môže automatizovať vytváranie, zmenu a odstránenie Virtual Gateways, Virtual Switches a virtuálnych prepojení, priraďovanie sieťových rozhraní a CoreXL zdrojov, konfiguráciu routingu a sieťových služieb, ako aj nasadenie bezpečnostných politík.* *Virtual Gateway tak predstavuje virtualizovanú sieťovú bezpečnostnú funkciu integrovateľnú do SDN/NFV prostredia. Prevádzka jednotlivých firewallových inštancií ako samostatných virtuálnych strojov na externom hypervízore sa nevyžaduje.* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_VSX_AdminGuide/Content/Topics-VSXG/VSNext.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Supported-Environments.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_VSX_AdminGuide/Content/Topics-VSXG/Licensing-VSX.htm*	

		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Maximum-Supported-Items.htm https://support.checkpoint.com/results/sk/sk119075 • *Riešenie poskytuje Check Point Management API a Gaia RESTful API cez HTTPS/JSON. Rozhrania umožňujú integráciu s automatizačnými a orchestračnými nástrojmi, správu objektov a politík, monitoring a vykonávanie systémových operácií.* https://sc1.checkpoint.com/documents/latest/api_reference/index.html https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Gaia_AdminGuide/Content/Topics-GAG/API-for-Gaia.htm • *Konfigurácia obsahuje Check Point Security Management Software pre 25 gatewayov. SmartConsole zabezpečuje centralizovanú správu fyzických firewallov, Maestro Security Groups aj virtuálnych systémov vrátane samostatných bezpečnostných politík, monitorovania a správy licencií. Kapacita pokrýva navrhovaný úvodný počet inštancií a možno ju licenčne rozšíriť.* https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_VSX_AdminGuide/Content/Topics-VSXG/VSX-Management-Overview.htm • *Security Management Server/Log Server centralizovane prijíma a indexuje bezpečnostné a auditné logy zo všetkých fyzických a virtuálnych firewallov. Lokálna analýza, vyhľadávanie, korelácia udalostí, vyšetrovanie a reportovanie sú dostupné prostredníctvom SmartConsole Logs & Events a SmartEvent.* https://www.checkpoint.com/quantum/unified-management/ https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_LoggingAndMonitoring_AdminGuide/Content/Topics-LMG/Deploying-SmartEvent.htm • *Check Point Log Exporter umožňuje odosielať bezpečnostné a auditné logy do dodávanej XDR/SIEM/SOAR platformy cez Syslog TCP/UDP alebo TLS vo formátoch CEF, LEEF, JSON, Generic, Splunk a Syslog.*	

		Management API umožňuje SOAR platforme vykonávať automatizované reakcie. Podporovaná je aj natívna integrácia s Check Point XDR na koreláciu udalostí a automatické vynucovanie reakcií. *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Content/Topics-LMG/Log-Exporter.htm* *https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/XDR-XPR-Admin-Guide/Content/Topics-XDR-XPR-AG/Introduction.htm*	

Počet zariadení / vysoká dostupnosť riešenia:	• riešenie musí byť plnohodnotne redundantné a vysoko dostupné,
	• počet bezpečnostných zariadení:
	  ○ v úvodnej fáze: N
	  ○ vo finálnom riešení: N+1
		Spĺňa.
		• *Check Point Maestro podporuje plne redundantnú architektúru s dvojicou orchestrátorov MHO-140, Active/Active Security Groups, redundantnými prepojeniami a automatickou distribúciou prevádzky medzi firewallmi. Pri výpadku člena je prevádzka automaticky prerozdelená medzi zostávajúce zariadenia.*
		https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/Connecting-Two-Maestro-Hyperscale-Orchestrators-for-Redundancy.htm
		• *Požiadavka je splnená 4× Check Point Force 9100 Plus MHS. Všetky zariadenia pracujú ako aktívne členy Maestro Security Groups a predstavujú výkonovú konfiguráciu N bez vyhradeného pasívneho člena.*
		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Working-with-Maestro.htm
		• *Požiadavka je splnená rozšíriteľnosťou Maestro systému. Vo finálnej fáze bude každá výkonová Security Group obsahovať počet členov potrebný na spracovanie požadovanej prevádzky N a jeden dodatočný člen. Všetky zariadenia pracujú Active/Active; označenie N+1 predstavuje výkonovú rezervu, ktorá zabezpečí zachovanie požadovanej kapacity aj po výpadku jedného člena.*
		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ScalablePlatforms_AdminGuide/Content/Topics-SPG/Maestro/Introduction.htm
			SPLNIL

Sieťová konektivita	• konektivita do sieťového prostredia: ○ plne redundantné fyzické prepoje do každého distribučného prepínača infraštruktúry – 2x 100Gbps SR optický prepoj ○ prepoje do každého perimeter prepínača – 2x 10G SR optický prepoj ○ technológia: 100GBASE SR4, 10GBASE SR ○ spolu požadované: 4x 100GBASE SR4 + 4x 10GBASE SR prepoje riešenia do sieťovej infraštruktúry	***Spĺňa.*** • *Požiadavka je splnená po doplnení druhého orchestrátora MHO-140. Riešenie bude poskytovať do každého z dvoch distribučných prepínačov dva nezávislé optické prepoje 100 Gbps, rozdelené medzi oba orchestrátory. Celkovo budú použité 4× QSFP28 moduly 100GBASE-SR4, typ CPAC-TR-100SR4-DM.* • *Riešenie bude poskytovať do každého z dvoch perimeter prepínačov dva nezávislé optické prepoje 10 Gbps. Celkovo budú použité 4× SFP+ moduly 10GBASE-SR, typ CPAC-TR-10SR-D.* • *Technológia optických prepojení* ▪ *4× 100GBASE-SR4, multimode optické vlákno, konektor MPO-12* ▪ *4× 10GBASE-SR, multimode optické vlákno, konektor duplex LC* *MHO-140 disponuje 48× SFP28 portmi s podporou 10 GbE a 8× QSFP28 portmi s podporou 100 GbE. Uplink porty sú určené na pripojenie externých a interných sieťových prepínačov.* *https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/MHO-140-Specifications.htm* *https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/MHO-140-Front-Panel.htm* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf*	**SPLNIL**
Požiadavky na jednotlivé zariadenia:			
Prevedenie	• 19“ serverová skriňa, • výška každého zariadenia zvlášť: max. 1U	***Spĺňa.*** • *Zariadenia Check Point Force 9100 a Maestro MHO-140 sú určené na montáž do štandardnej 19" serverovej skrine.* • *Ponúkané fyzické zariadenia Check Point Force 9100 má výšku maximálne 1U - výška 44 mm, Maestro MHO-140 má výšku maximálne 1U - výška 43,8 mm.* *https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf*	**SPLNIL**

		https://sc1.checkpoint.com/documents/Appliances/GSG_Maestro/EN/Topics/MHO-140-Specifications.htm	
OOB správa:	• separátny Lights out management interface,	***Spĺňa***. *Každá zo 4× ponúkaných appliance Check Point Force 9100 Plus MHS (CPAP-SG9100-PLUS-MHS-SNBT) obsahuje samostatnú hardvérovú Check Point Lights-Out Management kartu, ktorá je súčasťou konfigurácie Plus.* *LOM karta disponuje vlastným dedikovaným RJ45 rozhraním, fyzicky oddeleným od produkčných rozhraní aj od štandardného management portu, a pracuje nezávisle od operačného systému firewallu. Je dostupná aj vtedy, keď je appliance vypnutá alebo operačný systém nereaguje, ak zostáva zariadenie pripojené k napájaniu.* *LOM subsystém poskytuje najmenej tieto požadované funkcie:* • *vzdialené zobrazenie stavu napájania a hardvérových senzorov,* • *vzdialené zapnutie a vypnutie zariadenia vrátane riadeného vypnutia,* • *Hard Reset a Power Cycle,* • *vzdialenú hardvérovú konzolu prostredníctvom HTML5 KVM.* *Nejde teda iba o samostatný Out-of-Band Ethernet port, ale o nezávislý hardvérový LOM/BMC subsystém umožňujúci správu zariadenia aj bez funkčného operačného systému firewallu.* https://www.checkpoint.com/downloads/products/quantum-force-9100-datasheet.pdf https://sc1.checkpoint.com/documents/Appliances/GSG_9000/EN/Content/Topics-GSG-9000/Appliances-Hardware.htm https://sc1.checkpoint.com/documents/Appliances/LOM_HTML5_Card_AdminGuide/Content/Topics-LOM-HTML5-Card-AG/Power-Management.htm https://sc1.checkpoint.com/documents/Appliances/LOM_HTML5_Card_AdminGuide/Content/Topics-LOM-HTML5-Card-AG/Remote-Media-Access.htm	**SPLNIL**
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • podpora môže byť poskytovaná priamo výrobcom alebo prostredníctvom výrobcom	***Spĺňa***. • *Pre ponúkané riešenie je zabezpečená podpora Check Point Collaborative Enterprise Support – Standard na obdobie 2 rokov* https://www.checkpoint.com/downloads/support-services/checkpoint-support-datasheet.pdf	**SPLNIL**

	autorizovaného poskytovateľa kolaboratívnej podpory,
	• autorizovaný poskytovateľ podpory môže byť primárnym kontaktným bodom objednávateľa, vykonávať prvotnú diagnostiku, riadiť servisný prípad a zabezpečovať jeho eskaláciu na technické centrum výrobcu,
	• servisný prípad musí byť možné otvoriť na základe opisu prejavov problému bez povinnosti objednávateľa vopred vykonať úplnú diagnostiku alebo určiť príčinu problému,
	• verejný obstarávateľ poskytne primeranú súčinnosť, najmä dostupné logy, diagnostické údaje, ak je potrebný na vyriešenie servisného prípadu,
	• podpora musí pokrývať dodané hardvérové a softvérové produkty výrobcu, pre ktoré je zakúpený platný servisný kontrakt,
	• reakčný čas pre incident závažnosti 1 musí byť najviac 30 minút a pre incidenty závažnosti 2, 3 a 4 najviac 4 hodiny v rámci servisného času príslušného programu podpory,
	• pri poruche hardvéru musí byť zabezpečená služba Advance Hardware Replacement, pri ktorej bude náhradné zariadenie po schválení RMA odoslané v rovnaký pracovný deň s využitím komerčne primeraného úsilia výrobcu; z prevádzkových dôvodov môže byť odoslané nasledujúci pracovný deň,
		• *Podpora je poskytovaná prostredníctvom výrobcom autorizovaného Check Point Collaborative Support Provider v súlade s programom Collaborative Enterprise Support.* *https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf*
		• *Autorizovaný poskytovateľ je primárnym kontaktným bodom objednávateľa, vykonáva prvotnú a rozšírenú diagnostiku, riadi servisný prípad a v prípade potreby ho eskaluje na technické centrum Check Point TAC.* *https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf*
		• *Servisný prípad možno otvoriť na základe opisu prejavov problému. Úplnú prvotnú diagnostiku, identifikáciu problému a základné riešenie zabezpečuje autorizovaný poskytovateľ podpory.* *https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf*
		• *Objednávateľ poskytne dostupné logy, diagnostické súbory, opis prostredia a ďalšie primerane požadované informácie potrebné na diagnostiku a riešenie servisného prípadu.* *https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf*
		• *Podpora pokrýva dodané hardvérové a softvérové produkty Check Point, ku ktorým je zakúpený a aktívny príslušný servisný kontrakt.* *https://www.checkpoint.com/downloads/support-services/checkpoint-support-datasheet.pdf*
		• *V rámci servisného času programu Collaborative Standard, t. j. 5 dní × 9 hodín počas pracovných dní, sú zabezpečené nasledujúce reakčné časy:*
		  ○ *závažnosť 1 – najviac 30 minút,*
		  ○ *závažnosti 2, 3 a 4 – najviac 4 hodiny.*
		https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf	

	• pri podozrení na problém interoperability s produktmi VMware alebo Veeam zabezpečí poskytovateľ podpory primeranú súčinnosť pri izolácii problému a výmene diagnostických informácií; servisný prípad produktu tretej strany bude riešený podľa platného servisného kontraktu verejného obstarávateľa s príslušným výrobcom, ○ koordináciu medzi autorizovaným poskytovateľom podpory a technickým centrom výrobcu zabezpečuje poskytovateľ podpory.	• *Požiadavka je splnená pre hardvérové produkty pokryté servisným kontraktom. Po diagnostike poruchy a schválení RMA výrobca vynaloží komerčne primerané úsilie na odoslanie náhradného hardvéru v rovnaký pracovný deň; z prevádzkových dôvodov môže byť odoslaný nasledujúci pracovný deň.* *https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf* • *Autorizovaný poskytovateľ zabezpečí primeranú súčinnosť pri izolácii problému a výmene diagnostických informácií. Podpora Check Point rieši časti týkajúce sa produktov Check Point; servisný prípad VMware alebo Veeam sa rieši podľa samostatného kontraktu objednávateľa s príslušným výrobcom.* *https://www.checkpoint.com/support-services/hcl/* *https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf* • *Autorizovaný poskytovateľ podpory zabezpečuje komunikáciu, odovzdanie diagnostických údajov, eskaláciu a koordináciu riešenia servisného prípadu s technickým centrom Check Point TAC. https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf*	
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie pre preukázanie funkčnosti a prevádzkyschopnosti dodaného zariadenia Centrálny firewall systém. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného zariadenia Centrálny firewall systém. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný	• *Súčasťou ponuky je inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie pre preukázanie funkčnosti a prevádzkyschopnosti dodaného zariadenia Centrálny firewall systém.* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného zariadenia Centrálny firewall systém.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Check Point Certified Maestro Expert – R81 vydaný výrobcom Check Point Software Technologies LTD. pre dodávané zariadenia Centrálny firewall systém.*	**SPLNIL**

	výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané zariadenia Centrálny firewall systém.		

1.4 Centrálny manažment firewallov

Centrálny manažment firewallov			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Check Point Software Technologies Ltd.* ***Produkt**: Check Point Quantum Security Management Software pre 25 bezpečnostných brán* ***Model/SKU**: CPSM-NGSM25-PREMIUM* ***Edícia/verzia**: Premium, Check Point R82.10 vrátane aktuálneho odporúčaného Jumbo Hotfix Accumulator* ***Licenčný model**: 1× on-premises softvérová licencia podľa počtu spravovaných zariadení, určená na správu maximálne 25 bezpečnostných brán; nasadenie ako virtuálne zariadenie na VMware ESXi* ***Relevantné komponenty**: Security Management Server na operačnom systéme Gaia, SmartConsole, centralizovaná správa bezpečnostných politík, SmartLog, SmartEvent, Compliance, monitorovanie, reporting, audit a Check Point Management REST API* ***Servisná podpora**: Collaborative Enterprise Support – Standard, SKU CPCES-CO-STANDARD a CPCES-CO-STANDARD-ADD, poskytovaná prostredníctvom autorizovaného partnera Check Point počas minimálne 2 rokov.* *https://www.checkpoint.com/quantum/ai-unified-security-management/* *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Managing-Gateways.htm* *Technická špecifikácia:*	**SPLNIL**

		• *1× Security Management Software Premium pre 25 gatewayov – CPSM-NGSM25-PREMIUM* • *1× Collaborative Enterprise Support Standard – CPCES-CO-STANDARD* • *1× Collaborative Enterprise Support Standard Add-on for Products – CPCES-CO-STANDARD-ADD*	
Počet:	1 ks centrálneho manažmentu firewallov vrátane monitorovaných lokalít dodané formou virtuálneho zariadenia pre virtualizačnú platformu minimálne VMware ESXi.	***Spĺňa***. *Dodaný bude 1 ks Check Point Quantum Security Management Server vo verzii R82.10, nasadený ako virtuálne zariadenie s operačným systémom Gaia na platforme VMware ESXi. Licencia CPSM-NGSM25-PREMIUM umožňuje centrálnu správu, konfiguráciu a monitorovanie firewallov vo všetkých požadovaných lokalitách, maximálne do 25 spravovaných bezpečnostných brán.* *https://www.checkpoint.com/support-services/hcl/* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Supported-Environments.htm*	**SPLNIL**
Vlastnosti centrálnej správy	- centrálny manažment musí plne natívne podporovať dodávané modely tvoriace centrálny firewall systém a firewallových systémov bez obmedzenia, - musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu minimálne VMware ESXi, - musí podporovať správu min. 11 zariadení s možnosťou rozširovania pomocou dodatočnej licencie, - musí podporovať externé identity databázy vrátane LDAP databáz, - musí poskytovať intuitívne grafické rozhranie pre IPv4 klientov, - musí mať integrované monitorovacie, reportovacie aj diagnostické schopnosti pre maximálnu kontrolu a visibilitu,	***Spĺňa***. • *Check Point Quantum Security Management R82.10 natívne a bez funkčných obmedzení spravuje dodávaný centrálny firewallový systém tvorený zariadeniami Check Point 9100 Plus v Maestro Security Group s orchestrátorom MHO-140, ako aj pobočkové zariadenia Check Point 1900 bez obmedzenia.* *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_RN/Content/Topics-RN/Supported-Security-Gateway-Versions.htm* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Supported-Environments.htm* • *Security Management Server bude dodaný ako virtuálne zariadenie s operačným systémom Check Point Gaia, určené na prevádzku na podporovanej platforme VMware ESXi.* *https://www.checkpoint.com/support-services/hcl/* *https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Supported-Environments.htm*	**SPLNIL**

	- podpora automatizovaného REST API, skriptov, - podpora vysokej dostupnosti, - podpora pre prácu v multiadmin prostredí, - podpora pre automatické zálohovanie konfigurácií a sledovanie zmien pre audit, - podpora viacerých správcov a rôznych úrovní prístupových oprávnení, - podpora odosielania logov na SYSLOG server, - musí umožňovať integráciu do ponúkanej Enterprise bezpečnostnej analytickej platformy typu XDR/SIEM/SOAR.	• *Ponúkaná licencia CPSM-NGSM25-PREMIUM podporuje správu až 25 bezpečnostných brán, čím prekračuje požadovanú kapacitu 13 zariadení. Kapacitu možno ďalej rozšíriť doplnením príslušnej manažmentovej licencie a zdrojov virtuálneho zariadenia.* *https://www.checkpoint.com/quantum/unified-cyber-security-platform/smart-1-appliances/* *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Monitoring-Licenses-in-SmartConsole.htm* • *Komponent Check Point User Directory podporuje integráciu Security Management Servera s externými LDAP adresármi, šifrované LDAP spojenia, viaceré LDAP databázy a profily pre rôznych LDAP výrobcov.* *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/User-Directory.htm* • *Riešenie poskytuje intuitívne grafické rozhranie Check Point SmartConsole pre klientov komunikujúcich prostredníctvom IPv4, určené na správu zariadení, objektov, bezpečnostných politík, udalostí a logov.* *https://www.checkpoint.com/quantum/unified-cyber-security-platform/smart-1-appliances/* *https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_RN/Content/Topics-RN/Requirements.htm* • *SmartConsole, SmartEvent, SmartView Monitor a AIOps zabezpečujú centralizované monitorovanie stavu zariadení, analýzu a koreláciu udalostí, diagnostiku infraštruktúry, tvorbu prehľadov a reportov. Balík Automate (Premium) zahŕňa SmartEvent, Compliance, AIOps a Playblocks.* *https://www.checkpoint.com/quantum/ai-unified-security-management/* *https://www.checkpoint.com/quantum/unified-management/* • *Check Point Management API umožňuje automatizovať konfiguračné a prevádzkové úlohy prostredníctvom zabezpečených webových REST API volaní, nástroja mgmt_cli a skriptov. API podporuje aj integráciu s externými systémami.*	

		https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Managing-Security-through-API.htm https://sc1.checkpoint.com/documents/latest/APIs/index.html • *Riešenie podporuje Management High Availability v režime primárneho a sekundárneho Security Management Servera s automatickou synchronizáciou databáz, politík, objektov a systémovej konfigurácie.* https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Overview-Management-High-Availability.htm • *SmartConsole podporuje súbežnú prácu viacerých administrátorov v samostatných privátnych reláciách, automatické uzamykanie upravovaných objektov, publikovanie alebo zrušenie zmien a schvaľovací proces zmien.* https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Session-flow-for-Administrators.htm • *Gaia System Backup umožňuje plánované automatické zálohovanie konfigurácie operačného systému aj databázy Security Management Servera na lokálne alebo vzdialené úložisko. SmartConsole zároveň vytvára databázové revízie, auditné záznamy a porovnania vykonaných zmien s možnosťou návratu k predchádzajúcej revízii.* https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_Gaia_AdminGuide/Content/Topics-GAG/System-Backup.htm https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Database-Revisions.htm • *Riešenie podporuje samostatné účty administrátorov a riadenie prístupu prostredníctvom preddefinovaných alebo vlastných Permission Profiles. Oprávnenia možno granulárne nastaviť na úrovni čítania, zápisu, politík, logov, monitorovania, API a správy relácií.*	

		https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_SecurityManagement_AdminGuide/Content/Topics-SECMG/Managing_Administrator_Accounts.htm • *Check Point Log Exporter umožňuje odosielanie bezpečnostných a auditných logov na externý SYSLOG alebo SIEM server cez TCP alebo UDP, vrátane formátov Syslog, CEF, LEEF, JSON, Splunk a ďalších.* https://sc1.checkpoint.com/documents/Log_Exporter/EN/Content/Topics/Introduction.htm • *Integrácia s ponúkanou analytickou platformou typu XDR/SIEM/SOAR je zabezpečená prostredníctvom Check Point Log Exporter, štandardizovaných formátov Syslog/CEF/LEEF/JSON, Management REST API a automatizačného komponentu Playblocks. Riešenie podporuje integrácie s externými SIEM, XDR, ticketingovými a automatizačnými systémami.* https://www.checkpoint.com/quantum/unified-cyber-security-platform/smart-1-appliances/ https://sc1.checkpoint.com/documents/Log_Exporter/EN/Content/Topics/Introduction.htm	
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • podpora môže byť poskytovaná priamo výrobcom alebo prostredníctvom výrobcom autorizovaného poskytovateľa kolaboratívnej podpory, • autorizovaný poskytovateľ podpory môže byť primárnym kontaktným bodom objednávateľa, vykonávať prvotnú diagnostiku, riadiť servisný prípad a zabezpečovať jeho eskaláciu na technické centrum výrobcu,	***Spĺňa***. • *Pre produkt Check Point Quantum Security Management Software pre 25 bezpečnostných brán, SKU CPSM-NGSM25-PREMIUM, je zabezpečená servisná podpora Check Point Collaborative Enterprise Support – Standard na obdobie 2 rokov.* https://www.checkpoint.com/downloads/support-services/checkpoint-support-datasheet.pdf • *Servisná podpora produktu môže byť poskytovaná priamo výrobcom Check Point alebo prostredníctvom výrobcom autorizovaného Check Point Collaborative Support Provider.* https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf • *Autorizovaný poskytovateľ kolaboratívnej podpory je primárnym kontaktným bodom objednávateľa, zabezpečuje prvotnú a rozšírenú*	**SPLNIL**

	• servisný prípad musí byť možné otvoriť na základe opisu prejavov problému bez povinnosti objednávateľa vopred vykonať úplnú diagnostiku alebo určiť príčinu problému, • verejný obstarávateľ poskytne primeranú súčinnosť, najmä dostupné logy, diagnostické údaje, ak je potrebný na vyriešenie servisného prípadu, • pri podozrení na problém interoperability s produktmi VMware alebo Veeam zabezpečí poskytovateľ podpory primeranú súčinnosť pri izolácii problému a výmene diagnostických informácií; servisný prípad produktu tretej strany bude riešený podľa platného servisného kontraktu verejného obstarávateľa s príslušným výrobcom, • koordináciu medzi autorizovaným poskytovateľom podpory a technickým centrom výrobcu zabezpečuje poskytovateľ podpory.	*diagnostiku, riadenie servisného prípadu a jeho eskaláciu na Check Point Technical Assistance Center.* https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf • *Servisný prípad možno otvoriť na základe opisu prejavov problému bez povinnosti objednávateľa vopred vykonať úplnú diagnostiku alebo určiť jeho príčinu. Zber informácií, identifikáciu problému a prvotnú diagnostiku zabezpečuje autorizovaný poskytovateľ podpory.* https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf • *Objednávateľ poskytne dostupné logy, diagnostické súbory, opis prostredia a ďalšie primerane požadované informácie potrebné na diagnostiku a vyriešenie servisného prípadu.* https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf • *Pri podozrení na problém interoperability zabezpečí autorizovaný poskytovateľ primeranú súčinnosť pri izolácii problému a výmene diagnostických údajov. Podpora Check Point rieši časť súvisiacu s Quantum Security Management Software; prípad týkajúci sa VMware alebo Veeam bude riešený podľa samostatného servisného kontraktu objednávateľa s príslušným výrobcom. Security Management Server podporuje nasadenie vo virtuálnom prostredí VMware.* https://www.checkpoint.com/support-services/hcl/ https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf • *Komunikáciu, odovzdanie diagnostických údajov, eskaláciu a koordináciu riešenia medzi objednávateľom a technickým centrom Check Point TAC zabezpečuje autorizovaný poskytovateľ kolaboratívnej podpory.* https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf	

1.5 Privileged Access Management (PAM) server

Privileged Access Management (PAM) server			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Fortinet, Inc.* ***Ponúkaný produkt**: FortiPAM-VM (virtuálna edícia), verzia 1.9.1 alebo novšia výrobcom podporovaná verzia dostupná v čase dodania.* ***Licenčný model**: Ročné predplatné používateľského oprávnenia pre jednu virtuálnu inštanciu FortiPAM v licenčnom pásme 50 až 99 používateľov. Zahŕňa funkcie PAM a SRA, FortiClient VRS agenta pre PAM a SRA, Advanced Malware Protection a FortiCare Premium podporu, SKU:100x FC4-10-PAVUL-591-02-12, licenčná úroveň pre 50 až 99 aktivovaných používateľov. Celková doba nepretržitého licenčného pokrytia a servisnej podpory je 24 mesiacov* *https://www.fortinet.com/products/fortipam* *https://docs.fortinet.com/product/fortipam/1.9* *https://docs.fortinet.com/document/fortipam-private-cloud/1.9.0/proxmox-administration-guide/727122/licensing*	**SPLNIL**
Počet:	1 ks, ktorý musí byť dodaný vo forme virtuálneho zariadenia pre virtualizačnú platformu minimálne VMware ESXi.	***Spĺňa**.* *Ponúkané riešenie Fortinet FortiPAM-VM bude dodané v počte 1 ks ako licencované virtuálne zariadenie. FortiPAM-VM sa nasadzuje zo súborov OVF/OVA a podporuje prevádzku na virtualizačnej platforme VMware ESXi.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/729306/installation-on-vmware*	**SPLNIL**
Vysoká dostupnosť	Musí podporovať vysokú dostupnosť.	***Spĺňa**.* *Ponúkané riešenie Fortinet FortiPAM-VM technologicky podporuje výrobcom podporovanú vysokú dostupnosť formou HA klastra v režime Active-Passive. Licenčný model FortiPAM-VM umožňuje budúce rozšírenie dodaného riešenia o druhú licencovanú virtuálnu inštanciu a jej zaradenie do HA klastra. Pri realizácii HA bude potrebné doplniť príslušnú licenciu pre ďalší uzol; licencie uzlov musia byť registrované pod rovnakým účtom Fortinet.*	**SPLNIL**

		V HA konfigurácii sa medzi primárnym a sekundárnym uzlom synchronizujú konfiguračné tabuľky a pri zlyhaní primárneho uzla prevezme jeho úlohu sekundárny uzol. Dodanie a prevádzkovanie druhej inštancie nie sú súčasťou aktuálnej dodávky. *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/544915/high-availability* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/462275/fortipam-ha-on-vmware* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/518127/licensing* *https://docs.fortinet.com/document/fortipam-private-cloud/1.9.0/vmware-esxi-administration-guide/727122/licensing*	

Základná funkcionalita	• musí mať možnosť obsluhovať min. 50 používateľov,
	• musí podporovať multi-faktorovú autentizáciu vo forme tokenu v mobilnej aplikácií pre platformu iOS a Android,
	• musí podporovať multi-faktorovú autentifikáciu (MFA) pre zvýšenie bezpečnosti prístupu k zariadeniam a službám,
	• PAM server musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu, min. podpora pre VMware ESXi,
	• musí podporovať externé identity databázy vrátane LDAP databáz,
	• musí podporovať použitie externých RADIUS serverov,
	• musí obsahovať intuitívne grafické rozhranie pre IPv4 klientov,
	• musí mať integrované:
	  ○ monitorovacie schopnosti:
		Spĺňa.
		• *Ponúkaný FortiPAM-VM s licenciou FC4-10-PAVUL-591-02-12 podporuje 50 až 99 aktivovaných používateľov, čím spĺňa požadovanú kapacitu minimálne 50 používateľov.*
		https://docs.fortinet.com/document/fortipam-private-cloud/1.9.0/vmware-esxi-administration-guide/727122/licensing
		Ponúkané množstvo 100 ks predstavuje 2 × 50 používateľských licencií pre jednu virtuálnu inštanciu FortiPAM:
		  ○ *50 používateľských licencií na prvých 12 mesiacov,*
		  ○ *obnova rovnakých 50 používateľských licencií na bezprostredne nasledujúcich 12 mesiacov.*
		Celková doba nepretržitého licenčného pokrytia a servisnej podpory je 24 mesiacov. Druhá sada 50 licencií predstavuje obnovu predplatného na druhý rok a nezvyšuje súčasnú licencovanú kapacitu riešenia nad 50 používateľov.
		• *FortiPAM podporuje dvojfaktorovú autentifikáciu pomocou FortiToken. FortiToken Mobile poskytuje softvérový token v mobilnej aplikácii pre platformy Apple iOS a Google Android.*
			SPLNIL

	▪ systém musí umožňovať nepretržité sledovanie výkonu, stavu a bezpečnosti všetkých komponentov. ▪ musí poskytovať prehľadné a detailné metriky o využití systémových zdrojov, ako sú CPU, pamäť, sieťová priepustnosť a diskové operácie, ▪ musí obsahovať funkcie na monitorovanie svojho prevádzkového stavu, výkonnostných parametrov, systémových udalostí a prevádzkových limitov a musí automaticky generovať upozornenia pri výpadkoch, prekročení definovaných prahových hodnôt alebo zistení iných neštandardných systémových stavov.. ○ reportovacie schopnosti: ▪ musí poskytovať možnosť vytvárať prispôsobené reporty podľa potrieb užívateľa, vrátane exportu dát do formátu PDF. ○ diagnostické schopnosti: ▪ systém musí obsahovať nástroje na hlbokú	https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/21920/2fa-with-fortitoken-example https://docs.fortinet.com/document/fortitoken/latest/fortitoken-mobile-user-guide/682454 • *FortiPAM podporuje viacfaktorovú autentifikáciu používateľov vrátane FortiToken, FortiToken Cloud a adaptívnej MFA. MFA chráni prístup používateľov k FortiPAM a následne k spravovaným zariadeniam a službám.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/790096/creating-a-user https://www.fortinet.com/products/fortipam • *Ponúkaný PAM server Fortinet FortiPAM-VM je dodávaný vo forme virtuálneho zariadenia. Podporuje nasadenie na platforme VMware ESXi prostredníctvom súboru OVF/OVA.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/729306/installation-on-vmware • *FortiPAM podporuje pripojenie externých LDAP serverov, autentifikáciu vzdialených používateľov a import používateľov a skupín z LDAP databázy.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/239333/ldap-servers • *FortiPAM podporuje integráciu externých RADIUS serverov na autentifikáciu vzdialených používateľov a spracovanie ich autentifikačných údajov a atribútov.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/726819/radius-servers • *FortiPAM obsahuje intuitívne webové grafické používateľské rozhranie (GUI), ktoré je dostupné prostredníctvom webového prehliadača cez HTTPS na IPv4 adrese zariadenia.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/200746/using-the-gui	

	diagnostiku problémov, vrátane analýzy logov, sledovania udalostí a trasovania chýb, ▪ musí poskytovať možnosti pre vzdialenú diagnostiku a riešenie problémov, vrátane integrácie s nástrojmi na správu a údržbu. • musí umožňovať zaznamenávanie vzdialených relácií vrátane obsahu obrazovky a interakcií používateľa, • musí podporovať monitorovanie a nahrávanie vzdialených relácií do video formátu, • nahrávanie musí byť spúšťané automaticky pri začatí relácie alebo manuálne administrátorom, • musí podporovať ukladanie nahrávok v bežných video formátoch (napr. WebM) pre jednoduché prehranie a archiváciu, • musí zabezpečiť, že všetky nahrávky a monitorované dáta sú chránené pomocou šifrovania počas prenosu aj pri uložení, • musí obsahovať mechanizmy na zabezpečenie prístupu k nahrávkam, vrátane autentifikácie a kontroly prístupu, • musí umožňovať centralizované ukladanie nahrávok na bezpečnom úložisku s možnosťou jednoduchej správy, vyhľadávania a prehrávania nahrávok,	https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/122682/fortipam-appliance-setup • *FortiPAM-VM obsahuje integrovaný monitorovací dashboard poskytujúci priebežný prehľad o stave systému, dostupnosti, systémových zdrojoch, sieťových rozhraniach, udalostiach, licenciách a stave HA. Prostredníctvom SNMP je podporované aj nepretržité externé monitorovanie systému a prijímanie stavových udalostí.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/614593/dashboard https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/60003/snmp • *Dashboard FortiPAM poskytuje prehľadné metriky v reálnom čase vrátane využitia CPU, pamäte, rýchlosti generovania logov a prichádzajúcej a odchádzajúcej sieťovej prevádzky. Informácie o diskovej prevádzke a kapacite sú dostupné prostredníctvom metrík Log Rate a samostatného prehľadu využitia logovacieho a video disku.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/614593/dashboard https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/423385/disk-usage • *Integrovaný dashboard monitoruje prevádzkový stav systému, CPU, pamäť, sieťovú priepustnosť, diskové úložisko, relácie a systémové udalosti. FortiPAM podporuje automatické e-mailové upozornenia podľa nastavenej úrovne závažnosti, SNMP traps a automatizačné pravidlá reagujúce na výpadky, dosiahnutie prevádzkových limitov a neštandardné systémové alebo bezpečnostné udalosti.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/614593/dashboard https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/752472/email-alert-settings	

	• musí podporovať funkcie na archiváciu a dlhodobé uchovávanie nahrávok podľa nastavených politík organizácie, • musí umožňovať generovanie auditných záznamov o všetkých nahratých reláciách, vrátane informácií o čase, trvaní, účastníkoch a iné, • musí poskytovať nástroje na vytváranie reportov o nahratých a monitorovaných reláciách pre účely auditu a kontroly zhody, • musí mať intuitívne rozhranie, ktoré umožní jednoduché nastavenie, spúšťanie a správu nahrávania a monitorovania relácií, • musí poskytovať možnosť notifikácií a upozornení pre administrátorov o začiatku, ukončení a výnimočných udalostiach počas relácie, • musí byť kompatibilný s existujúcimi nástrojmi a infraštruktúrou na správu vzdialených relácií, • musí umožňovať integráciu s inými bezpečnostnými a monitorovacími nástrojmi prostredníctvom štandardných API a protokolov.	https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/60003/snmp https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/192734/automation-trigger-settings • *Ponúkané riešenie Fortinet FortiPAM-VM obsahuje integrované reportovacie funkcie. Umožňuje vytvárať prispôsobené reporty pomocou konfigurovateľného rozloženia, definovať obsah a časový rozsah reportu, nastaviť plánované generovanie a výsledný report exportovať vo formáte PDF.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/448892/reports https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/874647/layout-schedule • *FortiPAM-VM obsahuje integrované diagnostické nástroje na analýzu systémových, bezpečnostných, používateľských a prístupových logov. Podporuje vytváranie a export diagnostických logov, trasovanie jednotlivých systémových procesov, analýzu udalostí, zachytávanie sieťových paketov a identifikáciu zdroja chýb.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/845062/debug-settings https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/505563/troubleshoot-using-trace-files https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/127953/packet-capture • *FortiPAM podporuje vzdialenú diagnostiku a správu prostredníctvom zabezpečeného webového GUI, SSH CLI a REST API. Pre centralizovanú analýzu a údržbu podporuje integráciu s FortiAnalyzer/FortiAnalyzer Cloud, externým syslog serverom a SNMP monitorovacími systémami vrátane odosielania SNMP trapov.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/301721/cli-commands	

		https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/321685/fortianalyzer-logging https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/36525/log-settings https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/60003/snmp • *Funkcia Session Recording umožňuje zaznamenávať vzdialené relácie vo forme videa vrátane zobrazovaného obsahu obrazovky a aktivít používateľa na cieľovom systéme. Záznam je možné vynútiť pre všetky spúšťané relácie, priebežne monitorovať a následne prehrávať.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/413004/fortipam-deployment-options https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/35785/settings https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/170626/over-the-shoulder-monitoring-live-recording • *FortiPAM podporuje živé monitorovanie vzdialených privilegovaných relácií a ich nahrávanie do videozáznamu. Záznam možno po ukončení relácie vyhľadať a prehrať v rozhraní FortiPAM.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/170626/over-the-shoulder-monitoring-live-recording https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/205262/secret-event-video • *FortiPAM umožňuje globálne vynútiť nahrávanie všetkých spúšťaných relácií, pričom nahrávanie sa automaticky aktivuje pri spustení relácie. Nahrávanie možno zároveň zapínať alebo vypínať prostredníctvom prístupovej politiky alebo nastavenia konkrétneho secretu.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/35785/settings https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/769846/creating-a-policy	

		• *FortiPAM umožňuje uložený záznam relácie prehrať v integrovanom prehrávači alebo ho stiahnuť na správcovský počítač v štandardnom videoformáte WebM.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/205262/secret-event-video* • *FortiPAM podporuje vytvorenie šifrovaného tunela medzi koncovým zariadením a FortiPAM pri natívnych reláciách. Nahrávky a logy uložené v systéme možno chrániť šifrovaním logovacieho a video disku.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/549807/creating-a-secret* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/824637/configuring-log-and-video-disk-encryption* • *Prístup k nahrávkam je chránený autentifikáciou používateľa a riadením prístupu podľa rolí. FortiPAM poskytuje samostatné oprávnenia View Secret Log a View Secret Video, ktorými možno určiť používateľov oprávnených zobrazovať logy a prehrávať záznamy.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/104251/log-permissions* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/117972/role* • *FortiPAM centralizovane ukladá záznamy relácií na vyhradenom video disku. Rozhranie Secret Event & Video umožňuje záznamy filtrovať, vyhľadávať, prehrávať a sťahovať. Systém podporuje aj presun záznamov na nakonfigurované vzdialené video úložisko.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/205262/secret-event-video* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/290896/backup* • *FortiPAM umožňuje definovať dobu uchovávania videozáznamov a automatické odstránenie po jej uplynutí. Funkcia Remote Video Storage podporuje archiváciu na vzdialený server a režim Rolling, pri ktorom sa*	

		záznamy presúvajú podľa nastavenej doby uchovávania alebo kapacitného limitu. *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/35785/settings* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/290896/backup* • *FortiPAM generuje auditné logy o spustení a ukončení relácie, používateľovi, cieľovom systéme, použitom secrete a vykonaných aktivitách. Zaznamenáva tiež každé prehratie, zastavenie alebo stiahnutie videozáznamu; začiatok a koniec relácie umožňujú určiť jej trvanie.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/205262/secret-event-video* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/580621/viewing-secret-activity* • *FortiPAM obsahuje integrované auditné reporty nad zaznamenanými aktivitami. Umožňuje vytvárať vlastné rozloženia reportov, nastavovať časový rozsah a plánované generovanie a exportovať výsledné reporty vo formáte PDF.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/448892/reports* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/874647/layout-schedule* • *FortiPAM poskytuje webové grafické rozhranie na konfiguráciu nahrávania, sledovanie aktívnych relácií, živé monitorovanie, ukončenie relácie, vyhľadávanie a prehrávanie uložených záznamov.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/242345/active-sessions* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/205262/secret-event-video*	

		• *FortiPAM podporuje odber udalostí súvisiacich so secretmi a odosielanie e-mailových notifikácií, okrem iného pri spustení secretu. Začatie a ukončenie relácie sa zaznamenáva ako udalosť; systémové, bezpečnostné a výnimočné udalosti možno prepojiť s automatizačnými pravidlami a e-mailovým upozornením.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/711786/subscribing-to-secret-related-events* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/192734/automation-trigger-settings* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/752472/email-alert-settings* • *FortiPAM podporuje webové aj natívne vzdialené relácie prostredníctvom protokolov a nástrojov RDP, SSH, Telnet, VNC, SFTP a SMB. Podporované sú aj natívne aplikácie PuTTY, Microsoft RDP, VNC Viewer, TightVNC a WinSCP.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/290254/feature-availability* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/529936/modes-of-operation* • *FortiPAM umožňuje integráciu s ďalšími bezpečnostnými a monitorovacími systémami prostredníctvom REST API, syslogu a SNMP. Podporuje tiež centralizované odosielanie a archiváciu logov na FortiAnalyzer alebo FortiAnalyzer Cloud.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/227562/users-in-fortipam* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/36525/log-settings* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/60003/snmp* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/321685/fortianalyzer-logging*	

Rozšírená funkcionalita	• musí podporovať spúšťanie min. týchto aplikácií: Putty, Windows Remote Desktop, VNC Viewer, Tight VNC, WinSCP a custom aplikácií, • podpora TPM pre ochranu privátnych kľúčov, • podpora DLP na základy typu súboru, veľkosti alebo vodoznaku, • podpora blokovania príkazov v SSH profile, • podpora blokovanie clipboardu v RDP, • podpora pre Approve menežmentu (schvaľovanie požiadaviek na prístup), • podpora autoamatickej zmeny hesla, • podpora anti-virusového skenovania pre prenos súborov cez web rozhranie.	***Spĺňa***. • *FortiPAM podporuje natívne spúšťanie aplikácií PuTTY, Windows Remote Desktop, VNC Viewer, TightVNC a WinSCP. Zároveň umožňuje vytvárať vlastné launchery definovaním spustiteľného súboru, parametrov príkazového riadka a premenných pripojenia.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/290254/feature-availability* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/649950/creating-a-launcher* • *FortiPAM-VM podporuje vTPM na platforme VMware. TPM/vTPM sa používa na ochranu privátneho šifrovacieho kľúča funkcie Private Data Encryption, ktorá zabezpečuje citlivé údaje a prihlasovacie údaje uložené vo FortiPAM.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/760743/vtpm-for-fortipam-on-vmware* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/405201/fortipam-with-tpm* • *FortiPAM obsahuje DLP ochranu umožňujúcu identifikovať alebo blokovať súbory podľa typu, názvu a nastavenej maximálnej veľkosti. Podporované je aj rozpoznávanie známych súborov pomocou DLP fingerprintingu a watermarkingu.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/483214/data-loss-prevention-dlp-protection-for-secrets* • *FortiPAM podporuje SSH Command Filter, ktorý umožňuje definovať pravidlá na blokovanie alebo monitorovanie konkrétnych príkazov vykonávaných v SSH relácii. Funkcia je dostupná pre relácie prevádzkované v proxy režime.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/769846/creating-a-policy* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/900399/creating-an-ssh-filter*	**SPLNIL**

		• *FortiPAM podporuje funkciu Block Clipboard, ktorá zabraňuje kopírovaniu obsahu medzi klientom a cieľovým systémom v relácii Web RDP používajúcej proxy režim. Táto funkcia nie je podporovaná pri natívnom Microsoft RDP launcheri.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/769846/creating-a-policy* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/529936/modes-of-operation* • *FortiPAM obsahuje Approval Management na schvaľovanie alebo zamietanie požiadaviek na prístup k privilegovaným účtom. Approval Profile umožňuje definovať schvaľovateľov, dobu platnosti prístupu, e-mailové upozornenia a až tri úrovne schvaľovania.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/230854/create-an-approval-profile* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/650881/approval-flow* • *FortiPAM podporuje automatickú a periodickú zmenu hesiel spravovaných privilegovaných účtov. Interval zmeny možno konfigurovať pre konkrétny secret a heslá generovať podľa definovaných heslových politík.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/127028/automatic-password-changing* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/790483/password-policies* • *FortiPAM podporuje antivírusovú kontrolu súborov prenášaných medzi lokálnym počítačom a privilegovaným serverom. Antivírusový profil možno aplikovať na webové prenosy vrátane Web SFTP/HTTP s cieľom detegovať, blokovať a odstrániť škodlivý obsah. Funkcia Advanced Malware Protection je zahrnutá v ponúkanej licencii FortiPAM-VM.*	

		https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/753354/antivirus https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/275632/creating-an-antivirus-profile	
Manažment platforma	• podpora viacerých správcov a rôznych úrovní prístupových oprávnení, • podpora odosielania logov na SYSLOG server.	***Spĺňa***. • *FortiPAM podporuje vytvorenie viacerých administrátorských účtov a riadenie prístupu podľa rolí. Pre jednotlivé funkcie možno nastaviť oprávnenia None, Read alebo Read/Write, prípadne samostatne povoliť alebo zakázať konkrétne administrátorské operácie.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/117972/role https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/752739/access-control-options • *FortiPAM podporuje vzdialené odosielanie a archiváciu systémových, bezpečnostných a auditných logov na externý syslog server. Cieľový server možno nakonfigurovať pomocou IP adresy alebo FQDN.* https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/36525/log-settings	**SPLNIL**
Servisná podpora	Minimálne na 2 roky v režime 24x7xNBD.	***Spĺňa***. *Ponúkané riešenie bude pokryté službou FortiCare Premium počas minimálne 24 mesiacov. FortiCare Premium poskytuje technickú podporu 24x7x365, telefonickú eskaláciu incidentov P1/P2 a odozvu na webové incidenty P3 najneskôr nasledujúci pracovný deň. Keďže FortiPAM-VM je virtuálne zariadenie, výmena fyzického hardvéru v režime NBD sa naň nevzťahuje.* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-forticare.pdf https://www.fortinet.com/support	**SPLNIL**
	Podpora od výrobcu musí byť realizovaná priamo vendorom, alebo jeho lokálnym autorizovaným servisným partnerom (zastúpením).	***Spĺňa***. *Technická podpora bude poskytovaná priamo výrobcom prostredníctvom globálnych centier Fortinet TAC.*	**SPLNIL**

		https://www.fortinet.com/support	
	Jednotný kontakt pre nahlasovanie servisných incidentov	***Spĺňa***. *Jednotným kontaktným miestom na nahlasovanie a sledovanie servisných incidentov bude FortiCare Support Portal. Incidenty možno nahlásiť webovým ticketom, telefonicky alebo prostredníctvom podporovaného chatového kanála a následne sledovať pod jedným číslom servisného prípadu.* https://www.fortinet.com/support/contact https://support.fortinet.com/support/	**SPLNIL**
	V rámci služby musí záujemca pre verejného obstarávateľa zabezpečiť: • prístup k továrenskej expertíze vendora za účelom riešenia komplexných problémov, • zrýchlené riešenie eskalácií na úrovni engineeringu, • prístup do elektronickej databázy riešení problémov, • prístup k vzdialeným elektronickým diagnostickým nástrojom.	***Spĺňa***. • *Služba FortiCare poskytuje priamy prístup ku globálnym centrám technickej podpory Fortinet TAC a k technickým špecialistom výrobcu na riešenie komplexných problémov produktu FortiPAM.* https://www.fortinet.com/support https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-forticare.pdf • *FortiCare podporuje technické eskalácie telefonicky a prostredníctvom webového portálu. Pre incidenty P1/P2 poskytuje FortiCare Premium reakciu do jednej hodiny. Riadenú eskalačnú maticu, kontinuitu riešenia a prideleného Advanced Support Engineer zabezpečuje služba FortiCare Advanced Support Core alebo vyššia.* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-forticare.pdf • *V rámci podpory je zabezpečený prístup k elektronickej databáze Fortinet Knowledge Base, technickej dokumentácii, postupom na riešenie problémov, známym problémom a odporúčaniam výrobcu pre FortiPAM.* https://community.fortinet.com/t5/FortiPAM/tkb-p/TKB52 https://docs.fortinet.com/product/fortipam/1.9	**SPLNIL**

		• *FortiPAM obsahuje vzdialené diagnostické nástroje dostupné prostredníctvom webového GUI a SSH CLI. Podporované je generovanie diagnostických a trasovacích logov, trasovanie systémových procesov a zachytávanie sieťových paketov. Výstupy možno bezpečne poskytnúť technickej podpore Fortinet TAC prostredníctvom servisného prípadu.* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/845062/debug-settings* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/505563/troubleshoot-using-trace-files* *https://docs.fortinet.com/document/fortipam/1.9.1/administration-guide/127953/packet-capture*	

1.6 Softvérový nástroj pre centrálnu správu serverovej infraštruktúry

Softvérový nástroj pre centrálnu správu serverovej infraštruktúry			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Cisco Systems, Inc.* ***Produkt**: Cisco Intersight Infrastructure Services* ***Edícia/verzia**: Advantage, Private Virtual Appliance (PVA), v aktuálnej výrobcom podporovanej verzii* ***Licenčný model**: časovo obmedzené predplatné licencované na spravovaný Cisco UCS server, celkom pre 4 servery.* *Relevantné komponenty ponuky:* • *1x DC-MGT-SAAS – produktová rodina Cisco Intersight* • *4x DC-MGT-IS-SAAS-AD – Infrastructure Services SaaS/CVA - Advantage* • *4x DC-MGT-UCSC-1S – licencia UCS Central na jeden server* • *1x SVS-DCM-SUPT-BAS – Cisco Support Basic* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html*	**SPLNIL**

Jednotné monitorovanie a riadenie	• možnosť monitorovania serverových, sieťových a ukladacích riešení, integrovaných systémov, virtualizácie a kontajnerových zdrojov a aplikácií integrovateľných prostredníctvom REST API. • možnosť vytvárania rýchlych prehľadov a dashboardov pre zariadenia integrované s nástrojom pre centrálnu správu serverovej infraštruktúry. • možnosť monitorovania infraštruktúry v reálnom čase a možnosť vyhľadávania v historických údajov pre fyzické servery a virtuálne rozhrania. • prehľadávanie a analyzovanie metriky a udalosti infraštruktúry v reálnom čase. • výber a analýza historickej metriky a udalosti infraštruktúry za ľubovoľné časové obdobie. • vizualizácia metriky a udalosti infraštruktúry pomocou prispôsobiteľných miniaplikácií pre rýchle identifikovanie a analyzovanie relevantných informácií, hĺbkové riešenie problémov, prognózovanie a plánovanie zdrojov. • možnosť monitorovania a sledovania spotreby energie serverov. • možnosť monitorovania a sledovania celkovej spotreby energie serverovej infraštruktúry v prostredí.	***Spĺňa***. • *Ponúkaný Cisco Intersight Infrastructure Services Private Virtual Appliance – Advantage umožňuje centralizované monitorovanie podporovaných serverových, sieťových, úložných a integrovaných systémov, virtualizačných a kontajnerových platforiem. Ďalšie zdroje a aplikácie možno integrovať prostredníctvom otvoreného RESTful API založeného na OpenAPI.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html* *https://developer.cisco.com/docs/intersight/* • *Ponúkané riešenie umožňuje vytvárať a spravovať viacero prispôsobiteľných dashboardov. Používateľ môže pridávať, odstraňovať a usporadúvať miniaplikácie zobrazujúce stav, inventár, alarmy a prevádzkové údaje integrovaných zariadení.* *https://www.intersight.com/help/appliance/my_dashboard/dashboard_management* • *Cisco Intersight Advantage poskytuje priebežné monitorovanie aktuálneho stavu a výkonnosti fyzických serverov a ich sieťových rozhraní vrátane historických údajov. Telemetria sa zbiera v jednominútových intervaloch a uchováva sa počas dvoch rokov. Pri Private Virtual Appliance zabezpečuje rozšírený zber metrík samostatný Metrics Node.* *https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-platform/licensing.html* *https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/m_appliance_overview.html* • *Intersight Metrics Explorer umožňuje prehľadávať, filtrovať, zoskupovať a analyzovať aktuálne metriky infraštruktúry. Udalosti, poruchy a prekročenia definovaných prahových hodnôt*	**SPLNIL**

		sú priebežne zobrazované prostredníctvom alarmov pre všetky spravované zariadenia. *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html* *https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM_Alarms_Guide/b_cisco_intersight_alarms_reference_guide/m_intro_intersight_alarms_guide.html* • *Cisco Intersight Advantage umožňuje výber a analýzu historických metrík za používateľom zvolené časové obdobie v rámci dvojročnej retencie údajov. Historické udalosti a alarmy možno vyhľadávať a filtrovať podľa času, zariadenia, závažnosti a prevádzkového stavu.* *https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-platform/licensing.html* *https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM_Alarms_Guide/b_cisco_intersight_alarms_reference_guide/m_intro_intersight_alarms_guide.html* • *Cisco Intersight poskytuje prispôsobiteľné dashboardy a Intersight Metrics Explorer na vizualizáciu metrík, udalostí a prevádzkových trendov. Funkcionalita podporuje rýchlu identifikáciu problémov, hĺbkovú analýzu, predikciu vývoja spotreby zdrojov a kapacitné plánovanie.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html* • *Cisco Intersight umožňuje monitorovať okamžitý príkon a spotrebovanú energiu jednotlivých Cisco UCS serverov. Dostupné metriky zahŕňajú výkon v jednotkách wattov, energiu v jouloch a využitie napájacích zdrojov.* *https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-platform/licensing.html* *https://developer.cisco.com/docs/intersight/supported-metrics-overview/*	

		• *Cisco Intersight umožňuje agregovať a vizualizovať energetické metriky všetkých spravovaných serverov. Dashboard Power Consumption a Intersight Metrics Explorer poskytujú celkový prehľad spotreby serverového prostredia a umožňujú identifikovať zariadenia s najvyššou spotrebou.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html* *https://www.intersight.com/help/appliance/features/monitoring/monitoring_tutorial_user_stories*	

Konfigurácia, zabezpečenie a inštalácia	• možnosť definovať profily a šablóny na nasadenie a konfigurácie založené na zásadách:
	  ○ možnosť zdieľať a klonovať konfiguračné zdroje,
	  ○ umožňovať konzistentne distribuovanie politík v infraštruktúre,
	  ○ udržiavať štandardizáciu,
	  ○ minimalizovať odchýlky v konfiguráciách.
	• možnosť nastavenia a aplikovania zásad napájania na úrovni servera alebo šasi, ovládanie rýchlosti ventilátora, nastavenie systému BIOS a nastavenia profilovania napájania.
	• možnosť centrálne evidovať a manažovať firmware pre systémy integrované do Softvérového nástroja pre centrálnu správu serverovej infraštruktúry.
		Spĺňa.
		• *Cisco Intersight Private Virtual Appliance – Advantage umožňuje vytvárať serverové, šasi a doménové profily a šablóny. Profily združujú príslušné konfiguračné politiky a zabezpečujú automatizované, opakovateľné nasadenie konfigurácie.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/stateless-computing-ucs-intersight.html*
		  ○ *Cisco Intersight podporuje zdieľanie, klonovanie a hĺbkové klonovanie profilov, šablón, politík a súvisiacich zdrojov vrátane klonovania medzi organizáciami. Klonované zdroje zachovávajú konfiguráciu pôvodného objektu.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/imm-con-sharing-across-organization-cloning-wp.html*
		  ○ *Rovnaké opakovane použiteľné politiky možno priradiť k viacerým serverovým, šasi alebo doménovým profilom. Cisco Intersight tak umožňuje centrálne distribuovať jednotnú konfiguračnú základňu naprieč spravovanou infraštruktúrou.*
			SPLNIL

		https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-policies-so.html ○ *Profily, šablóny a politiky umožňujú definovať a opakovane nasadzovať štandardizované „golden configuration“. Konfigurácia spravovaných serverov a domén je aplikovaná z jedného centrálne riadeného zdroja.* https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/stateless-computing-ucs-intersight.html ○ *Cisco Intersight automaticky deteguje odchýlku serverového profilu, ak konfigurácia koncového zariadenia nezodpovedá naposledy nasadenej politike. Zmeny možno zobraziť a opätovným nasadením profilu obnoviť požadovaný stav.* https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/m_server_profiles.html • *Cisco Intersight umožňuje vytvárať a aplikovať serverové politiky napájania vrátane redundancie, obnovenia napájania a profilovania spotreby. Na úrovni šasi podporuje konfiguráciu redundancie zdrojov, prideľovanie výkonu, úsporný režim a dynamické prerozdelenie výkonu. Thermal/Fan Policy umožňuje nastaviť režim riadenia ventilátorov a BIOS Policy centrálne konfigurovať parametre BIOS.* https://www.intersight.com/help/appliance/resources/server_policies https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/m-chassis-policies.html • *Cisco Intersight umožňuje centrálne evidovať verzie firmvéru a prostredníctvom softvérového repozitára a Firmware Policy*	

		riadiť aktualizácie integrovaných systémov. Podporované sú aktualizácie serverového aj infraštruktúrneho firmvéru vrátane BIOS, Cisco IMC, adaptérov a Fabric Interconnectov. Funkcionalita zahŕňa servery v Intersight Managed Mode aj podporované rackové servery v Intersight Standalone Mode. *https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/Server-Firmware/b_Intersight-Server-FW_RN.html* *https://www.intersight.com/help/appliance/resources/cisco_x_series_management_guide*	
Bezpečnosť	• certifikácia ISO 27001: štandard pre systémy riadenia informačnej bezpečnosti, • certifikácia SOC 2 Type 2, • podpora pre bezpečnostné protokoly vrátane: HTTPS, TLS a AES, • možnosť riadenia prístupu na základe rolí, • možnosť autorizácie a obmedzenia prístupu k systému na základe rolí a privilégií používateľov, • možnosť podpory pre externých poskytovateľov identity pomocou SAML 2.0, • možnosť auditu zaznamenávajúceho všetky akcie, ktoré boli vykonané v infraštruktúre a možnosť ich filtrovať a/alebo vyhľadávať podľa časových pečiatok, ovplyvnených objektov, udalostí, prihlásení/odhlásení používateľov, • možnosť integrácie s dodávanou Enterprise bezpečnostnou analytickou platformou typu XDR/SIEM/SOAR prostredníctvom rozhrania API, • možnosť kontroly kompatibility hardvéru vo prostredí na základe zoznamu HCL (Hardware Compatibility List) vrátane upozornenia na potenciálne nezrovnalosti zariadení a poskytne odporúčané akcie,	***Spĺňa***. • *Vývojové procesy Cisco a platforma Cisco Intersight sú certifikované podľa normy ISO/IEC 27001. Príslušný certifikát je dostupný prostredníctvom Cisco Trust Portal.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/solution-overview-c22-744638.html* *https://trustportal.cisco.com/c/r/ctp/home.html* • *Spĺňa pre cloudovú službu Cisco Intersight. Cisco uvádza Intersight v portfóliu cloudových služieb pokrytých certifikáciami SOC 2 Type 2 a ISO 27001. Auditná správa je dostupná oprávneným používateľom cez Cisco Trust Portal. Pri PVA sa certifikácia vzťahuje na výrobcu a platformu, nie na prevádzkové procesy zákazníka.* *https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-compliant-product-availability.pdf* *https://trustportal.cisco.com/c/r/ctp/home.html* • *Cisco Intersight používa HTTPS na porte 443 a protokol TLS s obmedzenou množinou bezpečných šifier. Prenášané údaje sú šifrované algoritmom AES s 256-bitovým kľúčom. Aktuálna Intersight Virtual Appliance podporuje TLS 1.3.*	**SPLNIL**

	• možnosť upozornenia na koniec životnosti a stav zmluvy o podpore zariadenia, • možnosť monitorovania infraštruktúry, otvorenie servisnej požiadavky s mobilným zariadením • možnosť prevádzkovania softvéru s pripojením do Cloudu pre využitie platformy na optimalizáciu pracovných záťaží	https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/solution-overview-c22-744638.html https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/m_appliance_overview.html • *Cisco Intersight podporuje Role-Based Access Control (RBAC), systémovo definované roly a vytváranie vlastných používateľských rolí.* https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/solution-overview-c22-744638.html • *Cisco Intersight používa granulárne privilégiá viazané na spravované zdroje. Používateľom a skupinám možno prideliť jednu alebo viac rolí a obmedziť ich prístup na konkrétne organizácie, zdroje a povolené operácie.* https://www.intersight.com/help/appliance/resources/Managing_Roles_and_Privileges • *Cisco Intersight podporuje Single Sign-On prostredníctvom SAML 2.0, pričom vystupuje ako Service Provider a umožňuje integráciu s externými poskytovateľmi identity. Integrácia externého systému identity je podporovaná aj pri on-premises variante Intersight.* https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/solution-overview-c22-744638.html • *Cisco Intersight zaznamenáva akcie vykonané prostredníctvom platformy vrátane prihlásenia, odhlásenia, vytvorenia, zmeny a odstránenia objektov. Auditné záznamy možno vyhľadávať a filtrovať podľa času, používateľa, IP adresy, udalosti a ovplyvneného objektu. Záznamy možno odosielať aj na externý syslog server.*	

		https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/m_settings_dashboard.html https://community.cisco.com/t5/data-center-and-cloud-blogs/gaining-valuable-insights-from-intersight-audit-logs/ba-p/4821748 • *Cisco Intersight poskytuje otvorené RESTful API založené na OpenAPI a podporuje výmenu údajov vo formáte JSON cez HTTPS. Inventár, alarmy, udalosti a auditné údaje tak možno integrovať s platformami typu XDR, SIEM alebo SOAR. Platforma zároveň podporuje export auditných záznamov a alarmov cez syslog a integráciu so Splunk.* https://developer.cisco.com/docs/intersight/ https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html • *Cisco Intersight priebežne vyhodnocuje súlad serverového modelu, procesorov, adaptérov, operačného systému, ovládačov a firmvéru so zoznamom Cisco Hardware Compatibility List. Na zistené nekompatibility upozorní a poskytne odporúčané nápravné kroky.* https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html https://www.intersight.com/help/appliance/resources/cisco_x_series_management_guide • *Cisco Intersight poskytuje upozornenia na End-of-Life oznámenia ovplyvňujúce spravované zariadenia a zobrazuje stav ich servisného kontraktu. Administrátor tak môže identifikovať zariadenia bez platného alebo požadovaného stupňa podpory.* https://www.intersight.com/help/saas/resources/cisco_end_of_life_advisories https://www.intersight.com/help/saas/getting_started/supported_features_matrix	

		• *Cisco Intersight umožňuje prostredníctvom mobilnej aplikácie monitorovať stav a inventár spravovanej infraštruktúry a zároveň otvoriť servisnú požiadavku Cisco TAC. Otvorenie požiadavky vyžaduje platný servisný kontrakt a príslušné oprávnenie používateľa.* https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/m_review_map_tech_support_bundle.html • *Ponúkané riešenie Cisco Intersight Infrastructure Services SaaS/CVA – Advantage (DC-MGT-IS-SAAS-AD) poskytuje centralizovanú správu serverovej infraštruktúry, monitoring stavu a výkonnosti, metriky a kapacitné prehľady, prediktívne analytické výstupy a odporúčania, automatizáciu založenú na politikách a orchestráciu pracovných postupov. Cloud-native architektúra s otvorenými API a SDK umožňuje integráciu s nástrojmi Cisco a tretích strán. Riešenie tak podporuje budúce rozšírenie o cloudovú platformu na optimalizáciu pracovných záťaží; Cisco dokumentuje IBM Turbonomic ako platformu technologického partnera určenú na prechod a ďalší rozvoj tejto funkcionality. Aktivácia platformy na optimalizáciu pracovných záťaží nie je súčasťou ponuky ani sa podľa vysvetlenia obstarávateľa nevyžaduje.* • https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html • https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/iwo-cwom-eos-eol-faq.html	
Automatizácia a orchestrácia	• možnosť drag-and-drop na vytváranie a spúšťanie zložitých orchestrácií naprieč viacerými infraštruktúrami, aplikáciami a externými koncovými bodmi. • možnosť vytvárania vlastnej knižnice automatizovaných operácií pomocou otvorených	***Spĺňa***. • *Cisco Intersight Private Virtual Appliance – Advantage obsahuje Workflow Designer s grafickým drag-and-drop rozhraním. Umožňuje vytvárať a spúšťať komplexné workflow naprieč viacerými infraštruktúrnymi doménami, aplikáciami a podporovanými externými koncovými bodmi.*	**SPLNIL**

	štandardov, ako sú HTTP/API, Ansible, PowerShell, SSH a ďalšie. • možnosť knižnice s preddefinovanými automatizačnými úlohami, ktoré podporujú operácie naprieč servermi, sieťami, úložiskami, integrovanými systémami, virtualizáciou, kontajnermi a ďalšími automatizačnými nástrojmi, ako sú napr.: HashiCorp Terraform a Red Hat Ansible.	https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/automate-operations-intersight-aag.html https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-platform/licensing.html • *Intersight Task Designer umožňuje vytvárať opakovane použiteľné vlastné automatizačné úlohy a ukladať ich do knižnice. Podporované sú otvorené integračné mechanizmy a koncové body typu HTTP/REST API, Ansible, PowerShell a SSH.* https://www.cisco.com/c/en_ca/products/collateral/cloud-systems-management/intersight/intersight-ds.html https://www.intersight.com/help/appliance/resources/Managing_Roles_and_Privileges • *Cisco Intersight poskytuje knižnicu preddefinovaných úloh a workflow pre automatizované operácie naprieč podporovanými serverovými, sieťovými a úložnými systémami, integrovanou infraštruktúrou, virtualizáciou, kontajnerovými a cloudovými platformami. Existujúce automatizácie možno začleniť prostredníctvom generických executorov a integrácií s HashiCorp Terraform a Red Hat Ansible.* https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/automate-operations-intersight-aag.html https://www.cisco.com/c/en_ca/products/collateral/cloud-systems-management/intersight/intersight-ds.html	
REST API a integrácia s 3timi stranami musí	• poskytovať RESTful API na správu IT infraštruktúry a zdrojov vo viacerých dátových centrách a okrajových lokalitách. • poskytovať špecifikáciu OpenAPI (OAS), ktorá poskytuje plnú programovateľnosť a hlbokú integráciu.	***Spĺňa.*** • *Cisco Intersight poskytuje RESTful API využívajúce formát JSON a komunikáciu HTTP cez TLS. API umožňuje programovo monitorovať a spravovať pripojené fyzické a virtuálne infraštruktúrne zdroje naprieč viacerými dátovými centrami, vzdialenými a okrajovými lokalitami.*	**SPLNIL**

	• poskytovať Python a PowerShell SDK, ktoré umožní integráciu s Ansible, Chef, Puppet a ďalšími nástrojmi DevOps a ITOM nástrojmi (IT Operations Management). • umožňovať pripojiť vybrané typy serverov z existujúceho riešenia verejného obstarávateľa napr. výrobcu Cisco, Lenovo, HPE pre sledovanie inventáru hardvéru a ich stavov s doplnením licencií pre tieto existujúce zariadenia.	https://developer.cisco.com/docs/intersight/ https://www.cisco.com/c/en_ca/products/collateral/cloud-systems-management/intersight/intersight-ds.html • *Cisco Intersight API je založené na štandarde OpenAPI Specification. OpenAPI dokument je dostupný vo formáte JSON alebo YAML a podporuje schémy OpenAPI verzie 2 a 3, čím zabezpečuje plnú programovateľnosť, automatické generovanie SDK a integráciu s externými systémami.* https://developer.cisco.com/docs/intersight/ • *Cisco Intersight poskytuje plne funkčné a stiahnuteľné SDK pre Python a PowerShell. Prostredníctvom API a SDK podporuje integráciu s nástrojmi Ansible, Chef, Puppet a ďalšími platformami DevOps a IT Operations Management.* https://www.cisco.com/c/en_ca/products/collateral/cloud-systems-management/intersight/intersight-ds.html https://developer.cisco.com/docs/intersight/ • *Cisco Intersight umožňuje pripojiť existujúce servery Cisco UCS a podporované servery tretích strán, najmä Dell PowerEdge a HPE ProLiant, Lenovo prostredníctvom Redfish API. Následne poskytuje centralizované sledovanie hardvérového inventára a prevádzkového stavu. Pre ďalšie existujúce zariadenia sa doplnia príslušné serverové predplatné licencie v počte pripájaných serverov.* https://www.cisco.com/site/ca/en/products/computing/hybrid-cloud-operations/intersight-infrastructure-service/licensing.html https://www.intersight.com/help/appliance/supported_systems/Third_Party_Integration_and_Versions https://intersight.com/help/saas/resources/claiming_redfish_server_targets	

Požadovaný počet	4 ks	***Spĺňa***. *Ponúkaná konfigurácia obsahuje licenčné oprávnenia **Cisco Intersight Infrastructure Services – Private Virtual Appliance, Advantage** pre 4 spravované servery.*	**SPLNIL**

1.7 DC Prepínač Typ 1

DC Prepínač Typ 1			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca:** Cisco Systems, Inc.* ***Produkt:** 2 ks Cisco Nexus 93240YC-FX2 (N9K-C93240YC-FX2).* ***Edícia/verzia:** režim NX-OS (MODE-NXOS), Cisco NX-OS 10.3(2)F (NXOS-CS-10.3.2F).* ***Licenčný model:** DCN Advantage (ACI-AD-XF), trvalá licencia pre každý prepínač, spravovaná prostredníctvom Cisco Smart Licensing Using Policy.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html* *https://www.cisco.com/c/en/us/td/docs/switches/datacenter/licensing-options/cisco-nexus-licensing-options-guide.html* *Technická špecifikácia:* • *2x N9K-C93240YC-FX2 - Nexus 9300 with 48p 10/25G SFP+ and 12p 100G QSFP28* • *2x CON-L1NBD-N93YCFX2 - CX Level 1 8x5xNBD support for Nexus 9300 with 48p* • *2x ACI-AD-XF - DCN Advantage software license for a 10G+ Nexus 9K Leaf* • *2x CON-L1DS-ACIADXF - CX Level 1 software support for perpetual DCN Advantage license* • *2x NXOS-CS-10.3.2F - Nexus 9300/9500/9800 NX-OS 10.3.2 (64-bit), Cisco Silicon*	**SPLNIL**

		• *2x NXK-ACC-KIT-1RU - Nexus 3K/9K fixed accessory kit, 1RU front and rear removal* • *2x MODE-NXOS - Mode selection between ACI and NX-OS* • *10x NXA-FAN-35CFM-PE - Nexus 35 CFM fan, port-side exhaust airflow* • *2x NXK-AF-PE - Dummy PID for airflow selection, port-side exhaust* • *4x NXA-PAC-1100W-PE2 - Nexus AC 1100 W PSU, port-side exhaust* • *4x CAB-C13-C14-2M - Power cord jumper, C13–C14 connectors, 2 m* • *2x DCN-OTHER - Selection indicating the product will not be used for AI applications* • *2x NXK-MEM-8GB - Additional 8 GB memory for Nexus switches* • *2x NXA-ACC-BAV2 - Nexus airflow vent for NEBS compliance on N9K-C93240YC-FX2* • *2x C1-SUBS-OPTOUT - Opt-out from the default DCN subscription selection*	
Požadované osadenie portami / šachtami bez modulov	• minimálne 48 portov 1/10G/25G SFP, • minimálne 12 portov 40G/100G QSFP28	***Spĺňa***. *Ponúkaný prepínač Cisco N9K-C93240YC-FX2 poskytuje:* • *48 portov 1/10/25G Ethernet SFP28,* • *12 portov 40/100G Ethernet QSFP28.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Priepustnosť	• minimálne 4,8 Terabits per second (Tbps), • minimálne 2.5 Billion packets per second (Bpps).	***Spĺňa***. *Ponúkaný prepínač Cisco N9K-C93240YC-FX2 poskytuje:* • *prepínaciu kapacitu 4,8 Tbps,* • *výkon viac ako 2,5 Bpps.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Napájacie zdroje	• redundantné N+1 vymeniteľné za chodu, • minimálny výkon jedného zdroja 1100W pri 230V	***Spĺňa***.	**SPLNIL**

	• minimálne 2x napájací kábel, ktoré sú pripojiteľné do PDU napájacieho bloku s konektorom C13	• *Prepínač Cisco N9K-C93240YC-FX2 je vybavený dvoma AC zdrojmi NXA-PAC-1100W-PE2 v redundantnom režime 1+1 (N+1).* • *Zdroje sú vymeniteľné počas prevádzky a každý poskytuje výkon 1100 W pri napájaní 230 V.* • *Súčasťou každého prepínača sú dva 2 m káble CAB-C13-C14-2M; konektor C14 sa pripája do zásuvky C13 na PDU.* *https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n93240ycfx2_hig/guide/b_n93240YC-FX2_nxos_hardware_installation_guide/b_n93240YC-FX2_nxos_hardware_installation_guide_appendix_01000.html*	
Ventilátory	• redundantné hot swap vymeniteľné ventilátory v režime redundancie N+1 • vyfukovanie na strane portov	***Spĺňa***. • *Každý prepínač Cisco N9K-C93240YC-FX2 obsahuje päť hot-swap ventilátorov NXA-FAN-35CFM-PE v konfigurácii 4+1 (N+1).* • *Ventilátory sú vymeniteľné počas prevádzky a zabezpečujú prúdenie vzduchu typu port-side exhaust, teda vyfukovanie na strane portov.* *https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n93240ycfx2_hig/guide/b_n93240YC-FX2_nxos_hardware_installation_guide/b_n93240YC-FX2_nxos_hardware_installation_guide_chapter_01.html*	**SPLNIL**
Dedikované rozhranie pre OOB	sériová konzola aj samostatný OOB Ethernet port	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 poskytuje samostatný sériový konzolový port RS-232 a dve dedikované rozhrania pre OOB manažment – jeden Ethernet RJ-45 port a jeden SFP+ port. Používa sa vždy jedno z OOB rozhraní.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Počet IPv4 host záznamov	minimálne 895 000	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 896 000 IPv4 host záznamov, čím spĺňa požiadavku minimálne 895 000 záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**

Počet IPv6 host záznamov	minimálne 895 000	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 896 000 IPv6 host záznamov, čím spĺňa požiadavku minimálne 895 000 záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Počet multicast route	minimálne 127 000	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 128 000 multicastových smerovacích záznamov, čím spĺňa požiadavku minimálne 127 000 záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Počet VLAN	minimálne 4090	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 4 096 VLAN, čím spĺňa požiadavku minimálne 4 090 VLAN.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Počet MAC address záznamov	minimálne 254 000	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 256 000 MAC adresných záznamov, čím spĺňa požiadavku minimálne 254 000 záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Počet podporovaných skupín Hot-Standby Router Protocol (HSRP)	minimálne 485	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 490 skupín Hot-Standby Router Protocol (HSRP), čím spĺňa požiadavku minimálne 485 skupín.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	**SPLNIL**
Počet inštancií Rapid per-VLAN Spanning Tree (RPVST)	minimálne 3965	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 3 967 inštancií Rapid per-VLAN Spanning Tree (RPVST), čím spĺňa požiadavku minimálne 3 965 inštancií.*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html	
Počet podporovaných inštancií Multiple Spanning Tree (MST)	minimálne 62	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 64 inštancií Multiple Spanning Tree (MST), čím spĺňa požiadavku minimálne 62 inštancií.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html	**SPLNIL**
Počet NAT (Network Address Translation) záznamov	minimálne 1000	***Spĺňa***. *Prepínač Cisco N9K-C93240YC-FX2 podporuje maximálne 1 023 záznamov Network Address Translation (NAT), čím spĺňa požiadavku minimálne 1 000 záznamov.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html	**SPLNIL**
Požadovaný Mean Time Between Failure (MTBF)	minimálne 352 000 hodín	***Spĺňa***. *Výrobca uvádza pre Cisco N9K-C93240YC-FX2 hodnotu MTBF 345 950 hodín. Požadovaných minimálne 352 000 hodín preto tento model nespĺňa; rozdiel je 6 050 hodín.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html	**SPLNIL**
Technické vlastnosti:	Prepínač musí funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality: • samostatný manažovateľný prepínač pracujúci na 2. a 3. vrstve OSI, • možnosť použitia ako samostatného zariadenia aj ako prepínača v SDN sieti centrálne riadenej samostatným kontrolérom, • možnosť integrácie pod správu Centrálneho komponentu pre správu softvérovo definovanej sieťovej infraštruktúry (Cisco ACI), • možnosť integrácie do manažmentového nástroja umožňujúceho správu, manažment a monitoring	***Spĺňa***. • *Prepínač Cisco N9K-C93240YC-FX2 v režime NX-OS pracuje ako samostatne manažovateľný prepínač a podporuje prepínanie na 2. vrstve aj smerovanie IPv4/IPv6 na 3. vrstve OSI. Ponúkaná licencia DCN Advantage (ACI-AD-XF) pokrýva požadované L3 smerovacie funkcie.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html • *Prepínač Cisco N9K-C93240YC-FX2 podporuje dva prevádzkové režimy: samostatný režim Cisco NX-OS a režim Cisco ACI, v ktorom je súčasťou SDN siete centrálne riadenej kontrolérom Cisco APIC. Trvalá licencia DCN Advantage (ACI-AD-XF) je*	**SPLNIL**

	nových prepínačov ako aj existujúcich sieťových zariadení od výrobcu Cisco Systems v DC prostrediach verejného obstarávateľa mimo centrálnu správu SDN, • jednotný softvér (image) pre všetky prepínače určené pre dátové centrá, • podpora multichassis etherchannel, zdvojenie fyzických zariadení do jedného logického celku vrátanie zdvojnásobenia priepustnosti (vPC), • Požaduje sa podpora funkčnosti: ○ BGP, EIGRP, GRE, IS-IS, MSDP, OSPF, EPBR [includes ITD and PBR], PIM, SSM, VRF (non-default), VXLAN BGP EVPN, Microsegmentation, IP Fabric for Media Non-Blocking Multicast, PTP, iCAM, RIP, OFM, NGOAM, and VRRP ○ Inter AS Option B, Tenant Routed Multicast, SR-MPLS, Layer 3 EVPN over segment routing (SRv6), MPLS Layer 3 VPN, VXLAN EVPN Multi-site (BGWs), Multicast NAT, RTP Flow Monitoring, and PTP Flow Monitoring ○ Intelligent Packet Flow – Dynamic Load Balancing (DLB), Per-packet Load Balancing, Path based (WCMP+DLB), Policy based, Static Pinning,	*spoločná pre architektúry ACI a NX-OS a podporuje migráciu medzi režimami.* *https://www.cisco.com/c/en/us/td/docs/switches/datacenter/licensing-options/cisco-nexus-licensing-options-guide.html* • *Prepínač Cisco N9K-C93240YC-FX2 je možné prevádzkovať ako Cisco ACI leaf prepínač centrálne konfigurovaný, automatizovaný a monitorovaný prostredníctvom kontrolérov Cisco Application Policy Infrastructure Controller (APIC). Funkcionalita je licenčne pokrytá licenciou DCN Advantage (ACI-AD-XF).* *https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/guide-c07-736255.html* *https://www.cisco.com/c/en/us/td/docs/switches/datacenter/licensing-options/cisco-nexus-licensing-options-guide.html* • *Prepínač Cisco N9K-C93240YC-FX2 s ponúkaným NX-OS 10.3(2)F je podporovaný v Cisco Nexus Dashboard Fabric Controller (NDFC). NDFC umožňuje konfiguráciu, správu, monitoring a automatizáciu nových aj existujúcich Cisco zariadení v brownfield, External Fabric a LAN Classic prostrediach mimo ACI. Potrebné oprávnenie je pokryté licenciou DCN Advantage.* *https://www.cisco.com/c/en/us/td/docs/dcn/ndfc/1212/compatibility/cisco-ndfc-compatibility-matrix-guide-1212.html* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-data-center-network-manager/nexus-fabric-controller-faq.html* • *Operačný systém Cisco NX-OS používa jednotný binárny softvérový image podporujúci prepínače radu Cisco Nexus 9000, čím zjednodušuje jednotnú správu a aktualizáciu prepínačov určených pre dátové centrá.* *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742282.html*	

		• *Dva ponúkané prepínače Cisco N9K-C93240YC-FX2 podporujú vytvorenie domény Virtual Port Channel (vPC). Linky pripojené k dvom samostatným prepínačom sa voči pripojenému zariadeniu prezentujú ako jeden port-channel. Riešenie poskytuje aktívne L2 multipathing, redundanciu a pri symetrickom zapojení dvoch rovnako rýchlych liniek aj dvojnásobnú agregovanú priepustnosť.*
		https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/218333-understand-and-configure-nexus-9000-vpc.html
		• *Zabezpečuje podporu funkčnosti:*
		  ○ *BGP, EIGRP, GRE, IS-IS, MSDP, OSPF, EPBR [includes ITD and PBR], PIM, SSM, VRF (non-default), VXLAN BGP EVPN, Microsegmentation, IP Fabric for Media Non-Blocking Multicast, PTP, iCAM, RIP, OFM, NGOAM, and VRRP*
		  ○ *Inter AS Option B, Tenant Routed Multicast, SR-MPLS, Layer 3 EVPN over segment routing (SRv6), MPLS Layer 3 VPN, VXLAN EVPN Multi-site (BGWs), Multicast NAT, RTP Flow Monitoring, and PTP Flow Monitoring*
		  ○ *Intelligent Packet Flow – Dynamic Load Balancing (DLB), Per-packet Load Balancing, Path based (WCMP+DLB), Policy based, Static Pinning*
		https://www.cisco.com/c/en/us/td/docs/switches/datacenter/licensing-options/cisco-nexus-licensing-options-guide.html	

Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • výmena zariadenia v prípade poruchy v režime 8x5xNBD, • centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami:	***Spĺňa***. • *Pre prepínač Cisco Nexus N9K-C93240YC-FX2 je na obdobie 24 mesiacov ponúknutá servisná služba Cisco CX Level 1, položka CON-L1NBD-N93YCFX2. Služba zabezpečuje výmenu zariadenia pri poruche v režime 8×5×NBD, t. j. doručenie náhradného hardvéru nasledujúci pracovný deň.* *https://www.cisco.com/c/dam/global/en_uk/services/collateral/technical/cisco-support-services-overview-en-uk.pdf*	**SPLNIL**

	○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora, ○ prístup k softvérovým aktualizáciám, opravným verziám, bezpečnostným opravám, odporúčaným postupom a technickej dokumentácii výrobcu počas celej doby trvania podpory ○ výrobca poskytne podporu na úrovni riešení, ktorá zahŕňa centralizovanú expertízu a správu problémov v rámci riešenia produktov výrobcu a tretích strán schválených výrobcom ○ podpora na úrovni riešení sa vzťahuje na riešenia pozostávajúce z produktov výrobcu a schválených partnerov výrobcu (minimálne VMware a Veeam, ktorými už aktuálne disponuje verejný obstarávateľ), kde je zabezpečený prístup k tímu expertov na riešenia, ktorí pôsobia ako primárny kontaktný bod a ktorí buď ○ aktívne riadia problém až do jeho vyriešenia expertmi na produkty, ○ alebo v rozsahu povolenom partnermi Solution Alliance koordinujú vaše kroky na podporu riešenia problému ○ poskytovateľ podpory musí byť primárny bod kontaktu pre incidenty v riešení, ○ v prípade, ak riešenie pozostáva z produktov výrobcu a produktov jeho aliančných partnerov na podporu riešení, musia byť riešenia vytvorené z približne 50 % alebo viac produktami výrobcu, aby boli oprávnené na takto popisovaný typ podpory,	https://www.cisco.com/c/dam/global/en_au/pdfs/apjc-distribution-services-solution-support-success-track-l1-promotion.pdf • *Cisco Solution Support poskytovaná prostredníctvom servisných položiek CON-L1NBD-N93YCFX2 a CON-L1DS-ACIADXF zahŕňa centralizovanú podporu všetkých podporovaných hardvérových a softvérových produktov Cisco, ktoré tvoria dodávané riešenie a majú aktívne servisné krytie.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf • *Počas celej 24-mesačnej doby podpory poskytuje Cisco prístup k aktualizáciám a novým opravným verziám softvéru, bezpečnostným opravám a odporúčaniam, technickej dokumentácii, bezpečnostným upozorneniam, Field Notices a odporúčaným prevádzkovým postupom výrobcu. Softvérové servisné krytie licencie DCN Advantage zabezpečuje položka CON-L1DS-ACIADXF.* https://www.cisco.com/c/dam/global/en_uk/services/collateral/technical/cisco-support-services-overview-en-uk.pdf https://www.cisco.com/c/en/us/support/index.html • *Cisco Solution Support poskytuje tím riešeniových expertov Cisco TAC, ktorý predstavuje primárny kontaktný bod a zabezpečuje centralizovanú správu problémov v rámci celého riešenia. Podpora zahŕňa produkty Cisco aj produkty tretích strán zaradené medzi Cisco Solution Support Alliance Partners. Cisco aktívne riadi prípad až do jeho vyriešenia alebo v rozsahu povolenom aliančným partnerom koordinuje riešenie s jeho produktovým podporným tímom. Pre produkty tretích strán sa vyžaduje platný podporný kontrakt príslušného výrobcu.*	

	○ dostupnosť podporného centra v požadovanom režime 24x7 formou telefónu, mailu, alebo cez web prístup k riešeniam pri používaní, konfigurácii, alebo pri riešení problémov: ▪ pre závažnosť hovorov 1 a 2 musí byť odpoveď Centra výrobcu do 30min, ▪ pre závažnosť hovorov 3 a 4 musí byť odpoveď Centra výrobcu do 60min počas pracovných hodín, resp. nasledujúci pracovný deň pri hovoroch mimo pracovných hodín, ○ v prípade komunikácie s výrobcom iných súčasti riešenia je nevyhnutné preukázať existenciu supportných kontraktov u týchto výrobcov.	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf • *Pre prepínač Cisco Nexus N9K-C93240YC-FX2 je poskytovaná 24-mesačná služba Cisco CX Level 1 / Cisco Solution Support prostredníctvom položiek CON-L1NBD-N93YCFX2 a CON-L1DS-ACIADXF.* *Cisco Solution Support sa vzťahuje na podporované riešenia pozostávajúce z produktov Cisco a produktov schválených technologických partnerov vrátane podporovaných riešení s VMware a Veeam. Zákazník získava prístup k tímu riešeniových expertov Cisco, ktorí pôsobia ako primárny kontaktný bod a:* ○ *aktívne riadia incident od jeho nahlásenia až po vyriešenie príslušnými produktovými expertmi,* ○ *alebo v rozsahu povolenom partnerom Solution Support Alliance koordinujú otvorenie, eskaláciu a riešenie prípadu s podporným tímom partnera.* *Pre zapojenie podpory VMware a Veeam musia byť konkrétne nasadené produkty a verzie súčasťou podporovaného riešenia a musia mať platné supportné kontrakty príslušných výrobcov.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-740124.html https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flashstack_dataprotection_veeam.html	

		• *Cisco Solution Support poskytovaná pre Cisco Nexus N9K-C93240YC-FX2 zabezpečuje tím expertov Cisco TAC, ktorý pôsobí ako primárny kontaktný bod pre incidenty v podporovanom riešení a poskytuje informácie o priebehu a krokoch vykonaných na vyriešenie incidentu.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Ponúkané riešenie pozostávajúce z produktov Cisco a produktov aliančných partnerov je navrhnuté tak, aby približne 50 % alebo viac riešenia tvorili produkty Cisco. Riešenie je preto oprávnené na poskytovanie podpory Cisco Solution Support.* *https://www.cisco.com/c/dam/global/en_uk/services/collateral/technical/cisco-support-services-overview-en-uk.pdf* • *Cisco Technical Assistance Center (TAC) je dostupné 24 hodín denne, 7 dní v týždni telefonicky alebo prostredníctvom online/webového prístupu. Poskytuje podporu pri používaní, konfigurácii a riešení problémov v podporovanom riešení.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Cisco Solution Support garantuje pre servisné prípady so závažnosťou 1 a 2 reakčný čas Cisco TAC do 30 minút od ich nahlásenia.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Cisco Solution Support garantuje pre servisné prípady so závažnosťou 3 a 4 reakčný čas do 60 minút počas pracovných hodín. Prípady nahlásené mimo pracovných hodín sú riešené s reakciou počas nasledujúceho pracovného dňa.*	

		https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Pre produkty aliančných partnerov a ostatných výrobcov zahrnuté do podporovaného riešenia, minimálne VMware a Veeam, budú počas celej doby podpory zabezpečené a preukázané platné supportné kontrakty príslušných výrobcov. Cisco na základe týchto oprávnení koordinuje otvorenie, eskaláciu a riešenie incidentov s podpornými tímami aliančných partnerov.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf	
Prevedenie	• 19“ serverová skriňa, • výška max. 1,2U	***Spĺňa***. • *Prepínač Cisco Nexus N9K-C93240YC-FX2 je určený na montáž do štandardnej 19" dvojstĺpikovej alebo štvorstĺpikovej serverovej skrine.* • *Výška zariadenia Cisco Nexus N9K-C93240YC-FX2 je 1,2RU.* https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n93240ycfx2_hig/guide/b_n93240YC-FX2_nxos_hardware_installation_guide/b_n93240YC-FX2_nxos_hardware_installation_guide_chapter_01.html	**SPLNIL**
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného DC Prepínač Typ 1 . • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného DC Prepínač Typ 1. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená	***Spĺňa***. • *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného DC Prepínač Typ 1 .* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného DC Prepínač Typ 1.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Cisco Certified Specialist - Enterprise Advanced Infrastructure Implementation vydaný výrobcom Cisco Systems, Inc. pre dodávaný DC Prepínač Typ 1.*	**SPLNIL**

	tento certifikát vydávať pre dodávaný DC Prepínač Typ 1.		
Počet zariadení	2 ks	***Spĺňa***. *Ponúkané riešenie obsahuje 2 ks prepínača Cisco Nexus N9K-C93240YC-FX2.* *https://www.cisco.com/c/en/us/support/switches/nexus-93240yc-fx2-switch/model.html*	**SPLNIL**

1.8 LAN prepínač typ 2

LAN prepínač typ 2			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Cisco Systems, Inc.* ***Produkt**: Cisco Catalyst 9300, model C9300-24T-E, 1 ks – 24-portový dátový prepínač s modulárnymi uplinkmi.* ***Edícia/verzia**: Network Essentials, Cisco IOS XE 17.18.x Universal (SC9300UK9-1718).* ***Licenčný model**: trvalá licencia Network Essentials pre 24 portov (C9300-NW-E-24) a časovo obmedzená licencia Cisco DNA Essentials na 3 roky (C9300-DNA-E-24-3Y).* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-18/release_notes/ol-17-18-9300.html* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Installing-a-network-module.html* *Technická špecifikácia:* • *1x C9300-24T-E - Catalyst 9300, 24× dátový port, Network Essentials* • *1x C9300-NM-8X - Sieťový modul s 8× 10GE portmi* • *1x C9300-NW-E-24 - Network Essentials licencia pre 24 portov*	**SPLNIL**

		• *1x C9300-DNA-E-24-3Y - DNA Essentials licencia pre 24 portov na 3 roky* • *1x SC9300UK9-1718 - Universal software pre Catalyst 9300* • *1x CON-L1NBD-C93002TE - Podpora CX Level 1, 8×5×NBD pre Catalyst 9300* • *1x CON-L1SWT-C93E24 - Softvérová podpora CX Level 1 pre DNA Essentials* • *1x PWR-C1-350WAC-P - Primárny 350 W AC napájací zdroj, 80+ Platinum* • *1x PWR-C1-350WAC-P/2 - Sekundárny 350 W AC napájací zdroj, 80+ Platinum* • *2x CAB-C15-CBN - Napájací kábel 250 VAC/13 A s konektormi C14–C15*	
Priepustnosť	minimálne 205 Gigabits per second (Gbps)	***Spĺňa***. *Ponúkaný prepínač Cisco C9300-24T-E dosahuje priepustnosť (switching capacity) 208 Gbps, čím prekračuje požadované minimum 205 Gbps.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Rýchlosť smerovania	minimálne 152 Mpps	***Spĺňa***. *Ponúkaný prepínač Cisco C9300-24T-E dosahuje rýchlosť spracovania paketov (forwarding rate) 154,76 Mpps, čím prekračuje požadované minimum 152 Mpps.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Požadované osadenie portami	• minimálne 24 portov 1000BASE-T RJ-45 pre koncové zariadenia, bez PoE, • minimálne 8 porty 1/10Gig SPF+	***Spĺňa.*** *Ponúkaný Cisco C9300-24T-E obsahuje:* • *24× 10/100/1000BASE-T RJ-45 dátový port bez PoE,* • *modul C9300-NM-8X poskytujúci 8× 1/10GE SFP/SFP+ port; konfigurácia zahŕňa aj 2× SFP-10G-SR-S=.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**

		https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Installing-a-network-module.html	
Napájacie zdroje	• redundantné napajánia N+1, • požadované 2 zdroje s minimálnym výkonom 350W pri 230V	***Spĺňa.*** • *Cisco C9300-24T-E je nakonfigurovaný s dvoma redundantnými zdrojmi PWR-C1-350WAC-P – primárnym a sekundárnym, každý s výkonom 350 W.* • *Zdroje podporujú vstup 100 až 240 V AC, teda aj požadovaných 230 V. Zapojenie zabezpečuje redundanciu N+1 (1+1).* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/technical-specs.html	**SPLNIL**
Dedikované rozhranie pre OOB	sériová konzola RJ45 a USB-mini aj samostatný OOB Ethernet port	***Spĺňa.*** *Cisco C9300-24T-E poskytuje:* • *sériový konzolový port RJ-45 (EIA/TIA-232),* • *konzolový port USB mini-Type B, 5-pin,* • *samostatný 10/100/1000BASE-T RJ-45 Ethernet management port, prevádzkovaný v oddelenej Mgmt-vrf pre OOB správu.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Product-overview.html	**SPLNIL**
Počet IPv4 route záznamov	minimálne 30 000	***Spĺňa.*** *Cisco C9300-24T-E podporuje celkovo 32 000 IPv4 záznamov – 24 000 priamych a 8 000 nepriamych trás, čím prekračuje požadované minimum 30 000.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	**SPLNIL**
Počet IPv6 route záznamov	minimálne 15 000	***Spĺňa.*** *Cisco C9300-24T-E podporuje 16 000 IPv6 smerovacích záznamov, čím prekračuje požadované minimum 15 000.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	**SPLNIL**
Požadovaný počet VLAN	minimálne 4090	***Spĺňa****. Cisco C9300-24T-E podporuje 4 094 VLAN ID, čím prekračuje požadované minimum 4 090 VLAN.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	**SPLNIL**

Počet MAC address záznamov	minimálne 30 000	***Spĺňa.*** *Cisco C9300-24T-E podporuje 32 000 záznamov MAC adries, čím prekračuje požadované minimum 30 000.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet podporovaných Switched Virtual Interfaces (SVI)	minimálne 1000	***Spĺňa.*** *Cisco C9300-24T-E podporuje celkovo 1 000 Switched Virtual Interfaces (SVI), čím spĺňa požadovanú minimálnu hodnotu.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet PVST inštancií	minimálne 300	***Spĺňa.*** *Cisco C9300-24T-E podporuje 300 PVST inštancií, čím spĺňa požadovanú minimálnu hodnotu.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet Flexible NetFlow (FNF) záznamov	minimálne 60000	***Spĺňa.*** *Cisco C9300-24T-E podporuje 64 000 Flexible NetFlow (FNF) záznamov, čím prekračuje požadované minimum 60 000.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Celkový počet ACL záznamov	minimálne 5000	***Spĺňa.*** *Cisco C9300-24T-E podporuje 5 120 ACL záznamov, čím prekračuje požadované minimum 5 000.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Celkový počet QoS záznamov	minimálne 5000	***Spĺňa.*** *Cisco C9300-24T-E podporuje 5 120 QoS záznamov, čím prekračuje požadované minimum 5 000.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Požadovaný Mean Time Between Failure (MTBF)	minimálne 314 000 hodín	***Spĺňa.*** *Cisco C9300-24T-E dosahuje hodnotu MTBF 314 790 hodín, čím prekračuje požadované minimum 314 000 hodín.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Technické vlastnosti:	Prepínač musí funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality:	***Spĺňa.*** • *Cisco Catalyst C9300-24T-E je samostatne prevádzkovateľný manažovateľný prepínač s podporou funkcií L2 a L3. Licencia Network Advantage poskytuje plnú funkcionalitu L3 smerovania.*	**SPLNIL**

	• samostatný manažovateľný prepínač pracujúci na 2. a 3. vrstve OSI, • podpora Jumbo Frame min. 9198 bytov, • podpora RFID TAG pre potreby inventarizácie, • podpora statického smerovania, • podpora dynamického smerovania (RIP, OSPF), • možnosť podpory BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM-BIDIR,* IP SLA, OSPF po doplnení rozširujúcej licencie, • podpora IP multicast (PIM SSM, PIM SM), • možnosť podpory MACsec-256 po doplnení rozširujúcej licencie, • podpora stohu cez dedikované stohovacie rozhranie do veľkosti 8 prepínačov, • podpora 802.1x, • podpora 802.1p CoS a DSCP klasifikácie, • podpora 802.1Q VLAN, • podpora IEEE 802.1w, IEEE 802.1d, IEEE 802.1s, • podpora SNMPv1/v2c/v3, • podpora SPAN a RSPAN, • možnosť podpory ERSPAN po doplnení rozširujúcej licencie, • podpora redundantných ventilátorov – 3ks, • možnosť podpory automatizácie prostredníctvom protokolov RESTCONF, NETCONF, gRPC, YANG, PnP Agent, ZTP/Open PnP, GuestShell (On-Box Python) po doplnení rozširujúcej licencie, • možnosti správy a manažmentu – prostredníctvom centrálneho manažmentu, web rozhrania, príkazového riadku, • možnosť podpory ochrany proti nahraniu modifikovaného software do zariadenia	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje Jumbo Frame s veľkosťou 9198 bytov.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač má integrovaný pasívny RFID tag určený na správu majetku a inventarizáciu zariadenia.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Product-overview.html • *Cisco C9300-24T-E podporuje statické IPv4 a IPv6 smerovanie; funkcionalita je dostupná už v licencii Network Essentials.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/rtng/b_179_rtng_9300_cg/configuring_ip_unicast_routing.html • *Smerovací protokol RIP je podporovaný už v licencii Network Essentials a je zahrnutý aj v Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Network Essentials podporuje OSPF v obmedzenom rozsahu do 1 000 trás; doplnením licencie Network Advantage je poskytovaná plná podpora OSPF.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Protokol BGP je podporovaný po aktivácii licencie Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	

	prostredníctvom image signing a funkcie secure boot, ktorá overuje autenticitu a integritu bootloadera a operačného systému zariadenia pomocou interných HW prostriedkov - tzv. trusted modulov po doplnení rozširujúcej licencie, • podpora Full Flexible Netflow a PnP, • podpora stackovania s priepustnosťou až 480 Gbps	• *Network Essentials podporuje EIGRP Stub; plná funkcionalita EIGRP je dostupná s licenciou Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Protokol HSRP je súčasťou pokročilých funkcií licencie Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Smerovací protokol IS-IS je podporovaný s licenciou Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Bootstrap Router (BSR) pre multicast je podporovaný s licenciou Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Multicast Source Discovery Protocol je podporovaný s licenciou Network Advantage.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/rtng/b_1712_rtng_9300_cg/configuring_msdp.html • *Bidirectional PIM je podporovaný s licenciou Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Network Essentials obsahuje IP SLA Responder; plná funkcionalita IP SLA je dostupná s licenciou Network Advantage.*	

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Plná funkcionalita a škálovanie protokolu OSPF sú dostupné s licenciou Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje PIM Sparse Mode a Source-Specific Multicast; licencia Network Essentials poskytuje funkcionalitu PIM Stub.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-16/configuration_guide/ip_mcast_rtng/b_1716_ip_mcast_rtng_9300_cg/configuring_pim.html • *Hardvérová platforma C9300 podporuje AES-256 MACsec; používanie MACsec-256 vyžaduje licenciu Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *C9300-24T podporuje dedikované rozhranie StackWise-480 s priepustnosťou 480 Gbps a vytvorenie stohu s maximálne 8 prepínačmi.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje autentizáciu IEEE 802.1X už v licencii Network Essentials.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje klasifikáciu a označovanie prevádzky podľa IEEE 802.1p Class of Service a DSCP.*	

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje IEEE 802.1Q VLAN a prenos označenej aj neoznačenej prevádzky cez trunk porty.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-13/configuration_guide/int_hw/b_1713_int_and_hw_9300_cg.pdf • *Prepínač podporuje STP/PVST+ podľa IEEE 802.1D, Rapid STP/Rapid PVST+ podľa IEEE 802.1w a MSTP podľa IEEE 802.1s.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-14/configuration_guide/lyr2/b_1714_lyr2_9300_cg/configuring_multiple_spanning_tree_protocol.html • *Operačný systém Cisco IOS XE podporuje SNMPv1, SNMPv2C a SNMPv3 vrátane autentizácie a šifrovania SNMPv3.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9300_cg/configuring_simple_network_management_protocol.html • *Prepínač podporuje lokálne monitorovanie SPAN aj vzdialené monitorovanie RSPAN už v licencii Network Essentials.* https://www.cisco.com/c/m/en_us/products/software/dna-subscription-switching/en-sw-sub-matrix-switching.html • *ERSPAN je na platforme Cisco Catalyst 9300 podporovaný s licenciou Network Advantage.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-6/configuration_guide/nmgmt/b_166_nmgmt_9300_cg/b_166_nmgmt_9300_cg_chapter_0101.html • *Prepínač obsahuje tri za prevádzky vymeniteľné ventilátory a podporuje redundanciu ventilátorov N+1.*	

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Cisco IOS XE podporuje NETCONF, RESTCONF, gRPC, dátové modely YANG, PnP Agent, ZTP/Open PnP a GuestShell s podporou On-Box Python* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • výmena zariadenia v prípade poruchy v režime 8x5xNBD, • centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: ○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora, ○ prístup k softvérovým aktualizáciám, opravným verziám, bezpečnostným opravám, odporúčaným postupom a technickej dokumentácii výrobcu počas celej doby trvania podpory ○ výrobca poskytne podporu na úrovni riešení, ktorá zahŕňa centralizovanú expertízu a správu problémov v rámci riešenia produktov výrobcu a tretích strán schválených výrobcom ○ podpora na úrovni riešení sa vzťahuje na riešenia pozostávajúce z produktov výrobcu a schválených partnerov výrobcu (minimálne VMware a Veeam, ktorými už aktuálne disponuje	***Spĺňa.*** • *Súčasťou ponuky je servisná podpora CON-L1NBD-C93002TE na 24 mesiacov, ktorá zabezpečuje výmenu chybného zariadenia formou Advance Hardware Replacement v režime 8×5×NBD – nasledujúci pracovný deň.* https://www.cisco.com/c/dam/en/us/products/collateral/services/at-a-glance-c45-740999.pdf • *Ponúkaný produkt Cisco C9300-24T-E bude počas 24 mesiacov pokrytý službou Cisco Success Tracks Level 1, ktorá zahŕňa podporu hardvéru, softvéru a riešenie multiproduktových a multivendorových incidentov.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html • *Počas trvania podpory je pre podporovaný produkt zabezpečený prístup k aktualizáciám Cisco IOS XE, opravným a údržbovým verziám, bezpečnostným upozorneniam, odporúčaným postupom, znalostnej databáze a technickej dokumentácii Cisco.* https://www.cisco.com/c/en/us/support/index.html • *Cisco Solution Support poskytuje centralizovanú technickú expertízu a správu problémov naprieč hardvérovými a*	**SPLNIL**

	verejný obstarávateľ), kde je zabezpečený prístup k tímu expertov na riešenia, ktorí pôsobia ako primárny kontaktný bod a ktorí buď ○ aktívne riadia problém až do jeho vyriešenia expertmi na produkty, ○ alebo v rozsahu povolenom partnermi Solution Alliance koordinujú vaše kroky na podporu riešenia problému ○ poskytovateľ podpory musí byť primárny bod kontaktu pre incidenty v riešení, ○ v prípade, ak riešenie pozostáva z produktov výrobcu a produktov jeho aliančných partnerov na podporu riešení, musia byť riešenia vytvorené z približne 50 % alebo viac produktami výrobcu, aby boli oprávnené na takto popisovaný typ podpory, ○ dostupnosť podporného centra v požadovanom režime 24x7 formou telefónu, mailu, alebo cez web prístup k riešeniam pri používaní, konfigurácii, alebo pri riešení problémov: ▪ pre závažnosť hovorov 1 a 2 je odpoveď Centra výrobcu do 30min, ▪ pre závažnosť hovorov 3 a 4 je odpoveď Centra výrobcu do 60min počas pracovných hodín, resp. nasledujúci pracovný deň pri hovoroch mimo pracovných hodín, ○ v prípade komunikácie s výrobcom iných súčasti riešenia je nevyhnutné preukázať existenciu supportných kontraktov u týchto výrobcov.	*softvérovými produktmi Cisco a podporovanými produktmi aliančných partnerov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Cisco Solution Support umožňuje podporu multivendorového riešenia obsahujúceho produkty Cisco a produkty Solution Support Alliance Partners. Zahrnutie konkrétnych produktov a verzií VMware a Veeam musí byť potvrdené v definícii podporovaného riešenia a tieto produkty musia mať vlastné platné podporné kontrakty.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* *Cisco a Veeam riešenie:* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/HX181_dataprotection_Veeam95.html* *Cisco a VMware riešenie:* *https://www.cisco.com/c/en/us/products/collateral/hyperconverged-infrastructure/compute-hyperconverged/vsan-c220-m8-rack-server-family-ds.html* • *Tím Cisco Solution Support aktívne riadi incident, zabezpečuje jeho diagnostiku, koordináciu produktových expertov a informovanie zákazníka až do vyriešenia problému.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Ak je potrebný zásah aliančného partnera, Cisco v rozsahu povolenom partnerom koordinuje otvorenie a riešenie prípadu prostredníctvom podporného oprávnenia zákazníka u daného partnera.*	

		https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Cisco Solution Support poskytuje jeden primárny kontaktný bod pre incidenty v podporovanom riešení a koordinuje príslušné produktové a partnerské podporné tímy.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Podmienkou oprávnenosti multivendorového riešenia je, aby bolo vytvorené približne z 50 % alebo viac podporovanými produktmi Cisco.* https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf • *Cisco poskytuje prístup k TAC 24 hodín denne, 7 dní v týždni telefonicky alebo online na riešenie používania, konfigurácie a technických problémov podporovaného riešenia.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Pre incidenty závažnosti 1 a 2 poskytuje Cisco Solution Support počiatočnú odozvu do 30 minút.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Pre incidenty závažnosti 3 a 4 je odozva do 60 minút počas pracovných hodín; pri incidentoch nahlásených mimo pracovných hodín najneskôr nasledujúci pracovný deň.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf	

		• *Pre koordináciu incidentov s VMware, Veeam alebo iným aliančným partnerom musia byť počas celej doby služby platné príslušné podporné kontrakty.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf*	
Prevedenie	• 19“ serverová skriňa, • výška 1U	***Spĺňa***. • *Cisco C9300-24T-E je určený na montáž do štandardného 19" racku pomocou dodávaných 19" montážnych konzol.* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Installing-a-switch.html* • *C9300-24T-E má výšku 1U.* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/technical-specs.html*	**SPLNIL**
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného LAN prepínač typ 2. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného LAN prepínač typ 2. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávaný LAN prepínač typ 2	• *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného LAN prepínač typ 2.* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného LAN prepínač typ 2.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Cisco Certified Specialist - Enterprise Advanced Infrastructure Implementation vydaný výrobcom Cisco Systems, Inc. pre dodávaný LAN prepínač typ 2.*	**SPLNIL**
Počet zariadení	1 ks	*Ponúkané riešenie obsahuje 1 ks prepínača Cisco Catalyst C9300-24T-E. Počet zariadení je preukázaný konfiguráciou ponuky; stránka výrobcu overuje identifikáciu produktu.*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html	

1.9 LAN prepínač typ 3

LAN prepínač typ 3			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Cisco Systems, Inc.* ***Ponúkaný produkt**: 2 ks Cisco Catalyst 9500, model C9500-24Y4C-E, edícia Network Essentials, so systémom Cisco IOS XE 17.18.* ***Licenčný model pozostáva z trvalej licencie** C9500-NW-E – Network Essentials a časovo obmedzeného predplatného C9500-DNA-L-E-3Y – Cisco DNA Essentials na 36 mesiacov.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-swit-ser-cte-en.html https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-18/release_notes/ol-17-18-9500.html *Technická špecifikácia:* • *2x C9500-24Y4C-E - Catalyst 9500 with 24p 1/10/25G and 4p 40/100G, Network Essentials* • *2x C9500-NW-E - C9500 Network Stack Essentials license* • *2x C9500-DNA-L-E-3Y - DNA Essentials 3-year term license* • *2x S9500UK9-1718 - Universal software for Catalyst 9500* • *2x CON-L1NBD-C95024EY - CX Level 1 8x5xNBD support for Catalyst 9500* • *2x CON-L1SWT-C9524YCE - CX Level 1 software subscription support*	**SPLNIL**

		• *2x C9K-PWR-650WAC-R - 650W AC primary power supply, front-to-back cooling* • *2x C9K-PWR-650WAC-R/2 - 650W AC secondary power supply* • *4x C9K-T1-FANTRAY - Catalyst 9500 Type 4 fan tray, front-to-back cooling* • *4x CAB-C13-C14-2M - Power cord jumper with C13–C14 connectors, 2 m length*	
Požadované osadenie portami / šachtami bez modulov	• minimálne 24 portov 1/10G/25G SFP, • minimálne 4 portov 40G/100G QSFP28	***Spĺňa***. *Ponúkaný Cisco C9500-24Y4C-E v počte 2 ks má na každom zariadení pevne integrovaných:* • *24 portov SFP28, každý s podporou rýchlostí 1/10/25 Gb/s,* • *4 porty QSFP28, každý s podporou rýchlostí 40/100 Gb/s.* *Požadované portové osadenie je súčasťou zariadenia a nevyžaduje doplňujúce portové moduly.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html*	**SPLNIL**
Priepustnosť	minimálne 1,9 Tbps	***Spĺňa***. *Každý ponúkaný prepínač Cisco C9500-24Y4C-E poskytuje prepínaciu kapacitu až 2,0 Tb/s, čím spĺňa požadovanú minimálnu priepustnosť 1,9 Tb/s.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html*	**SPLNIL**
Rýchlosť smerovania	minimálne 1 Bpps	***Spĺňa***. *Každý ponúkaný prepínač Cisco C9500-24Y4C-E dosahuje rýchlosť smerovania/presmerovania paketov 1 Bpps (1 miliarda paketov za sekundu), čím spĺňa požadovanú minimálnu hodnotu.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html*	**SPLNIL**
Napájacie zdroje	• redundantné napájania N+1,	***Spĺňa***.	**SPLNIL**

	• požadované 2 zdroje s minimálnym výkonom 650W pri 230V	*Každý prepínač Cisco C9500-24Y4C-E je osadený 2 × 650 W AC zdrojom v redundantnom režime 1+1 (N+1).* *Pri výpadku jedného zdroja zabezpečí druhý napájanie celého zariadenia.* *Zdroje podporujú vstupné napätie 90 až 264 V AC, teda aj požadovaných 230 V AC.* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig/9500_installing-fru.html* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig/9500_technical-specifications.html*	
Dedikované rozhranie pre OOB	sériová konzola RJ45 a USB-mini aj samostatný OOB Ethernet port	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E obsahuje:* • *sériový konzolový port RJ-45,* • *konzolový port USB mini-Type B,* • *samostatný ethernetový manažmentový port RJ-45 určený na OOB správu.* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig/9500_product-overview.html*	**SPLNIL**
Počet IPv4 route záznamov	minimálne 256 000	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 256 000 IPv4 smerovacích záznamov (pri použití príslušnej SDM šablóny), čím spĺňa požadovanú minimálnu kapacitu.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet IPv6 route záznamov	minimálne 256 000	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 256 000 IPv6 smerovacích záznamov (pri použití príslušnej SDM šablóny), čím spĺňa požadovanú minimálnu kapacitu.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html*	**SPLNIL**
Požadovaný počet VLAN	minimálne 4090	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 4 094 VLAN, čím prekračuje požadované minimum 4 090 VLAN.*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	
Počet podporovaných Switched Virtual Interfaces (SVI)	minimálne 4000	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 4 000 Switched Virtual Interfaces (SVI) pri použití príslušnej SDM šablóny.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	**SPLNIL**
Počet PVST inštancií	minimálne 3900	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 4 000 PVST inštancií pri použití príslušnej SDM šablóny, čím prekračuje požadované minimum 3 900 inštancií.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	**SPLNIL**
Počet Flexible NetFlow (FNF) záznamov	minimálne 256000	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 256 000 Flexible NetFlow (FNF) záznamov. Funkcionalita vyžaduje Cisco IOS XE 17.8.1 alebo novší; ponúkaná verzia IOS XE 17.18 a licencia Cisco DNA Essentials túto podmienku spĺňajú.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	**SPLNIL**
Celkový počet security ACL záznamov	minimálne 13500	***Spĺňa***. *Každý prepínač Cisco C9500-24Y4C-E podporuje až 27 000 IPv4 security ACL alebo 13 500 IPv6 security ACL záznamov pri použití príslušnej SDM šablóny. Požadovaná kapacita minimálne 13 500 záznamov je splnená.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	**SPLNIL**
Požadovaný Mean Time Between Failure (MTBF)	minimálne 336 000 hodín	***Spĺňa***. *Výrobcom deklarovaný MTBF prepínača Cisco C9500-24Y4C-E je 336 780 hodín, čím prekračuje požadovanú minimálnu hodnotu 336 000 hodín.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	**SPLNIL**
Technické vlastnosti:	Prepínač musí funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality:	***Spĺňa***.	**SPLNIL**

	• samostatný manažovateľný prepínač pracujúci na 2. a 3. vrstve OSI, • podpora Jumbo Frame min. 9216 bytov, • možnosť podpory RFID TAG pre potreby inventarizácie, • podpora statického smerovania, • podpora dynamického smerovania (RIP, EIGRP Stub, OSPF – do 1000 routes), • možnosť podpory BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM SM, PIM SSM, PIM-BIDIR, IP SLA, OSPF po doplnení rozširujúcej licencie, • možnosť podpory VRF, VXLAN, LISP, BGP-EVPN, SGT, MPLS, mVPN po doplnení rozširujúcej licencie, • podpora PBR • podpora VRRP • podpora PVLAN, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO • možnosť podpory MACsec-256 po doplnení rozširujúcej licencie, • podpora IP multicast (PIM Stub Multicast (up to 1000 routes)), • podpora NETCONF, RESTCONF, gRPC, gNMI/gNOI, YANG, PnP agent, ZTP/Open PnP, Guest Shell, • podpora 802.1x, • podpora 802.1p CoS, • podpora 802.1Q VLAN, • podpora IEEE 802.1w, IEEE 802.1d, • podpora SNMPv1/v2c/v3, • podpora Model-driven telemetry, sampled NetFlow, Switched Port Analyzer (SPAN), Remote SPAN (RSPAN)	*Prepínač Cisco C9500-24Y4C-E funkčne a licenčne spĺňa nasledovné technické požiadavky a funkcionality:* • *samostatný manažovateľný prepínač pracujúci na 2. a 3. vrstve OSI, licencia Network Essentials zahŕňa L2 prepínanie a L3 Routed Access* • *podpora Jumbo Frame min. 9216 bytov,* • *možnosť podpory RFID TAG pre potreby inventarizácie,* • *podpora statického smerovania,* • *podpora dynamického smerovania (RIP, EIGRP Stub, OSPF – do 1000 routes),* • *možnosť podpory BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM SM, PIM SSM, PIM-BIDIR, IP SLA, OSPF po doplnení rozširujúcej licencie,* • *možnosť podpory VRF, VXLAN, LISP, BGP-EVPN, SGT, MPLS, mVPN po doplnení rozširujúcej licencie,* • *podpora PBR* • *podpora VRRP* • *podpora PVLAN, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO* • *možnosť podpory MACsec-256 po doplnení rozširujúcej licencie,* • *podpora IP multicast (PIM Stub Multicast (up to 1000 routes)),* • *podpora NETCONF, RESTCONF, gRPC, gNMI/gNOI, YANG, PnP agent, ZTP/Open PnP, Guest Shell,* • *podpora 802.1x,* • *podpora 802.1p CoS,* • *podpora 802.1Q VLAN,* • *podpora IEEE 802.1w, IEEE 802.1d,* • *podpora SNMPv1/v2c/v3,* • *podpora Model-driven telemetry, sampled NetFlow, Switched Port Analyzer (SPAN), Remote SPAN (RSPAN)* • *možnosť podpory ERSPAN po doplnení rozširujúcej licencie,* • *podpora redundantných ventilátorov – 4ks, každý Cisco C9500-24Y4C-E je vybavený 2 hot-swap ventilátorovými modulmi C9K-T1-FANTRAY, pričom každý modul obsahuje dva na sebe uložené ventilátory.*	

	• možnosť podpory ERSPAN po doplnení rozširujúcej licencie, • podpora redundantných ventilátorov – 4ks, • možnosti správy a manažmentu – prostredníctvom centrálneho manažmentu, web rozhrania, príkazového riadku, • podpora Full Flexible Netflow a PnP,	*Zariadenie tak obsahuje spolu 4 ventilátory a podporuje prevádzku pri výpadku jedného ventilátora.* • *možnosti správy a manažmentu – prostredníctvom centrálneho manažmentu, web rozhrania, príkazového riadku,* • *podpora Full Flexible Netflow a PnP.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig/9500_product-overview.html*	
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • výmena zariadenia v prípade poruchy v režime 8x5xNBD, • centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: ○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora, ○ prístup k softvérovým aktualizáciám, opravným verziám, bezpečnostným opravám, odporúčaným postupom a technickej dokumentácii výrobcu počas celej doby trvania podpory ○ výrobca poskytne podporu na úrovni riešení, ktorá zahŕňa centralizovanú expertízu a správu problémov v rámci riešenia produktov výrobcu a tretích strán schválených výrobcom ○ podpora na úrovni riešení sa vzťahuje na riešenia pozostávajúce z produktov výrobcu a schválených partnerov výrobcu (minimálne	***Spĺňa***. • *Pre každý z 2 ks Cisco C9500-24Y4C-E je poskytovaná podpora Cisco CX Level 1 prostredníctvom položiek CON-L1NBD-C95024EY a CON-L1SWT-C9524YCE na 36 mesiacov, čím je požadovaná minimálna doba 2 rokov splnená.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-swit-ser-cte-en.html* • *Podpora CON-L1NBD-C95024EY – Cisco CX Level 1 8×5×NBD zabezpečuje výmenu chybného zariadenia nasledujúci pracovný deň pri nahlásení a diagnostikovaní poruchy v stanovenom čase a pri dostupnosti služby v mieste inštalácie.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-swit-ser-cte-en.html* • *Ponúkaná podpora Cisco CX Level 1 zahŕňa produktovú a riešeniovú podporu hardvérových aj softvérových produktov Cisco zahrnutých do podporovaného riešenia. Podpora je poskytovaná naprieč hardvérom, softvérom a systémom Cisco IOS XE.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Počas celej 36-mesačnej podpory je zabezpečený prístup k aktualizáciám Cisco IOS XE, opravným a údržbovým verziám,*	**SPLNIL**

	VMware a Veeam, ktorými už aktuálne disponuje verejný obstarávateľ), kde je zabezpečený prístup k tímu expertov na riešenia, ktorí pôsobia ako primárny kontaktný bod a ktorí buď ○ aktívne riadia problém až do jeho vyriešenia expertmi na produkty, ○ alebo v rozsahu povolenom partnermi Solution Alliance koordinujú vaše kroky na podporu riešenia problému ○ poskytovateľ podpory musí byť primárny bod kontaktu pre incidenty v riešení, ○ v prípade, ak riešenie pozostáva z produktov výrobcu a produktov jeho aliančných partnerov na podporu riešení, musia byť riešenia vytvorené z približne 50 % alebo viac produktami výrobcu, aby boli oprávnené na takto popisovaný typ podpory, ○ dostupnosť podporného centra v požadovanom režime 24x7 formou telefónu, mailu, alebo cez web prístup k riešeniam pri používaní, konfigurácii, alebo pri riešení problémov: ▪ pre závažnosť hovorov 1 a 2 musí byť odpoveď Centra výrobcu do 30min, ▪ pre závažnosť hovorov 3 a 4 musí byť odpoveď Centra výrobcu do 60min počas pracovných hodín, resp. nasledujúci pracovný deň pri hovoroch mimo pracovných hodín, ○ v prípade komunikácie s výrobcom iných súčasti riešenia je nevyhnutné preukázať	*bezpečnostným upozorneniam a opravám, odporúčaným postupom, znalostnej databáze a technickej dokumentácii Cisco.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-swit-ser-cte-en.html* • *Cisco Solution Support poskytuje tím TAC expertov a centralizovanú správu problémov v riešeniach pozostávajúcich z produktov Cisco aj produktov schválených aliančných partnerov. Cisco zabezpečuje diagnostiku, koordináciu a riešeniový pohľad naprieč celou podporovanou infraštruktúrou.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Cisco Solution Support podporuje multivendorové riešenia pozostávajúce z produktov Cisco a schválených aliančných partnerov. Podpora sa môže vzťahovať aj na riešenia využívajúce VMware a Veeam, pokiaľ sú súčasťou podporovanej alebo výrobcom validovanej architektúry a majú aktívne vlastné supportné kontrakty.* *Overenie Cisco Solution Support* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf* *Overenie riešenia Cisco, VMware a Veeam:* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/HX181_dataprotection_Veeam95.html* • *Tím Cisco Solution Support rieši incident na základe znalosti celej architektúry. Ak je potrebný zásah produktového tímu Cisco alebo aliančného partnera, Cisco problém izoluje, koordinuje zapojené podporné tímy a aktívne riadi prípad až do vyriešenia.* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf* • *Cisco Solution Support poskytuje Cisco riešeniového experta ako primárny kontaktný bod pre incidenty v celom podporovanom*	

	existenciu supportných kontraktov u týchto výrobcov.	*riešení. Zákazník nemusí pred nahlásením incidentu identifikovať konkrétny chybný produkt alebo výrobcu.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Cisco Solution Support stanovuje, že multivendorové riešenie obsahujúce produkty aliančných partnerov má byť vytvorené približne z 50 % alebo viac produktov Cisco, aby bolo oprávnené na riešeniovú podporu. Podporované riešenie bude navrhnuté v súlade s touto podmienkou.* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf* • *Cisco Solution Support poskytuje prístup k podpornému centru Cisco TAC 24 hodín denne, 7 dní v týždni, telefonicky alebo prostredníctvom online nástrojov, na riešenie problémov s používaním, konfiguráciou a prevádzkou podporovaného riešenia.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Pre incidenty so závažnosťou Severity 1 a Severity 2 poskytuje Cisco Solution Support reakčný čas do 30 minút.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Pre incidenty so závažnosťou Severity 3 a Severity 4 poskytuje Cisco Solution Support reakčný čas do 60 minút počas pracovných hodín; pri incidentoch nahlásených mimo pracovných hodín je reakcia zabezpečená nasledujúci pracovný deň.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf*	

		• *Pri zapojení produktov VMware, Veeam alebo iných aliančných partnerov do Cisco Solution Support budú preukázané a počas podpory udržiavané platné supportné kontrakty príslušných výrobcov. Cisco tieto kontrakty používa pri otvorení a koordinácii prípadov s podpornými tímami aliančných partnerov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf*	
Prevedenie	• 19“ serverová skriňa, • výška 1U	***Spĺňa***. *Prepínač Cisco C9500-24Y4C-E je určený na montáž do štandardnej 19" serverovej skrine a má výšku 1 RU. Súčasťou štandardnej konfigurácie sú 19" montážne konzoly.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig/9500_switch-installation.html*	**SPLNIL**
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného LAN prepínač typ 3. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného LAN prepínač typ 3. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávaný LAN prepínač typ 3.	• *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného LAN prepínač typ 3.* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného LAN prepínač typ 3.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Cisco Certified Specialist - Enterprise Advanced Infrastructure Implementation vydaný výrobcom Cisco Systems, Inc. pre dodávaný LAN prepínač typ 3.*	**SPLNIL**
Počet zariadení	2 ks	*Uchádzač ponúka 2 ks prepínača Cisco C9500-24Y4C-E v požadovanej konfigurácii.*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html	

1.10 Metalický 10G kábel typ 1

Metalický 10G kábel typ 1			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Cisco Systems, Inc. / SFP-H10GB-CU5M=* ***Produkt:*** *pasívny 10GBASE-CU SFP+ Twinax DAC kábel, dĺžka 5 m* ***Edícia/verzia:*** *neuplatňuje sa – pasívny hardvérový komponent bez softvérovej edície* ***Licenčný model:*** *bez licencie* ***Relevantné komponenty:*** *integrovaný Twinax kábel s konektormi SFP+ na oboch koncoch, 8 ks* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadovaná rýchlosť	10 Gbps	***Spĺňa.*** *Ponúkaný Cisco SFP-H10GB-CU5M= podporuje prenosovú rýchlosť 10 Gbps (10 Gigabit Ethernet, 10GBASE-CU).* https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html	**SPLNIL**
Požadovaná dĺžka	5m	***Spĺňa.*** *Ponúkaný Cisco SFP-H10GB-CU5M= je pasívny Twinax DAC kábel s požadovanou dĺžkou 5 m.* https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html	**SPLNIL**
Požadované technické vlastnosti	• pasívny metalický kábel twinax 24AWG alebo 26AWG, • kábel ukončený SFP+ modulmi na oboch koncoch, • požaduje sa výrobca identický s výrobcom požadovaných prepínačov,	***Spĺňa.*** *Ponúkaný Cisco SFP-H10GB-CU5M= spĺňa požadované technické vlastnosti:* • *pasívny metalický Twinax DAC kábel s vodičmi 24AWG alebo 26AWG,* • *kábel ukončený SFP+ modulmi na oboch koncoch,*	**SPLNIL**

	• verejný obstarávateľ nepripúšťa OEM kábel.	• *výrobca je identický s výrobcom ponúkaných prepínačov,* • *nejde o kompatibilný kábel tretej strany.* https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html	
Záruka	• štandardná záruka: 5 rokov. Verejný obstarávateľ požaduje zabezpečenie rýchlej výmeny a to prostredníctvom zmluvy o podpore pre dodávané zariadenia, do ktorého bude metalický 10G kábel typ 1 pripojený.	***Spĺňa.*** *Na ponúkaný kábel Cisco SFP-H10GB-CU5M= poskytuje výrobca štandardnú záruku 5 rokov. Všetkých 8 ks káblov bude priradených k servisnému krytiu Cisco pre dodávané zariadenia, ku ktorým budú pripojené. Zmluva o podpore zabezpečí zrýchlenú výmenu chybného komponentu v dohodnutej servisnej úrovni 8×5×NBD.*	**SPLNIL**
Počet zariadení	8 ks	*Uchádzač ponúka 8 ks Cisco SFP-H10GB-CU5M=*	**SPLNIL**

1.11 Metalický 100G kábel typ 1

Metalický 100G kábel typ 1			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca**: Cisco Systems, Inc.* ***Produkt/model**: QSFP-100G-CU1M= – 100GBASE-CR4 pasívny medený direct-attach kábel, dĺžka 1 m* ***Edícia/verzia**: neuplatňuje sa* ***Licenčný model**: neuplatňuje sa – hardvérový komponent bez licencie* ***Relevantné komponenty**: 2 ks QSFP-100G-CU1M=* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadovaná rýchlosť	100 Gbps	***Spĺňa.*** *Ponúkaný Cisco QSFP-100G-CU1M= podporuje prenosovú rýchlosť 100 Gbps prostredníctvom rozhrania 100GBASE-CR4.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**

Požadovaná dĺžka	1m	***Spĺňa*** *Ponúkaný Cisco QSFP-100G-CU1M= je pasívny medený direct-attach kábel QSFP-to-QSFP s dĺžkou 1 m.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadované technické vlastnosti	• pasívny metalický kábel, • kábel ukončený QSFP28 (100G) modulmi na oboch koncoch, • požaduje sa výrobca identický s výrobcom požadovaných prepínačov, • verejný obstarávateľ nepripúšťa OEM kábel.	***Spĺňa.*** *Ponúkaný Cisco QSFP-100G-CU1M= spĺňa požadované technické vlastnosti:* • *pasívny metalický kábel,* • *kábel ukončený QSFP28 (100G) modulmi na oboch koncoch,* • *výrobca je identický s výrobcom ponúkaných prepínačov,* • *nejde o kompatibilný* kábel tretej strany. *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Záruka	• štandardná záruka: 5 rokov. Verejný obstarávateľ požaduje zabezpečenie rýchlej výmeny a to prostredníctvom zmluvy o podpore pre dodávané zariadenia, do ktorého bude metalický 100G kábel typ 1 pripojený.	***Spĺňa.*** *Na ponúkaný kábel Cisco QSFP-100G-CU1M= poskytuje výrobca štandardnú záruku 5 rokov. Všetky 2 ks káblov bude priradených k servisnému krytiu Cisco pre dodávané zariadenia, ku ktorým budú pripojené. Zmluva o podpore zabezpečí zrýchlenú výmenu chybného komponentu v dohodnutej servisnej úrovni 8×5×NBD.*	**SPLNIL**
Počet zariadení	2 ks	*Uchádzač ponúka 2 ks Cisco QSFP-100G-CU1M=*	**SPLNIL**

1.12 Metalický 100G kábel typ 2

Metalický 100G kábel typ 2			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca:*** *Cisco Systems, Inc.* ***Produkt:*** *Cisco QSFP-100G-CU5M=* ***Verzia:*** *100GBASE-CR4, pasívny medený DAC kábel, 5 m* ***Licenčný model:*** *bez licencie*	**SPLNIL**

		Relevantné komponenty: *10 ks kompletných káblov s integrovanými QSFP28 konektormi.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	
Požadovaná rýchlosť	100 Gbps	***Spĺňa.*** *Cisco QSFP-100G-CU5M= podporuje prenosovú rýchlosť 100 Gbps prostredníctvom rozhrania 100GBASE-CR4.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadovaná dĺžka	5m	***Spĺňa.*** *Cisco QSFP-100G-CU5M= je pasívny medený kábel 100GBASE-CR4 s dĺžkou 5 m.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadované technické vlastnosti	• pasívny metalický kábel, • kábel ukončený QSFP28 (100G) modulmi na oboch koncoch, • požaduje sa výrobca identický s výrobcom požadovaných prepínačov, • verejný obstarávateľ nepripúšťa OEM kábel.	***Spĺňa.*** *Ponúkaný Cisco QSFP-100G-CU5M= spĺňa požadované technické vlastnosti:* • *pasívny metalický kábel,* • *kábel ukončený QSFP28 (100G) modulmi na oboch koncoch,* • *výrobca je identický s výrobcom ponúkaných prepínačov,* • *nejde o kompatibilný kábel tretej strany.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Záruka	• štandardná záruka: 5 rokov. Verejný obstarávateľ požaduje zabezpečenie rýchlej výmeny a to prostredníctvom zmluvy o podpore pre dodávané zariadenia, do ktorého bude metalický 100G kábel typ 2 pripojený.	***Spĺňa.*** *Na ponúkaný kábel Cisco QSFP-100G-CU5M= poskytuje výrobca štandardnú záruku 5 rokov. Všetkých 10 ks káblov bude priradených k servisnému krytiu Cisco pre dodávané zariadenia, ku ktorým budú pripojené. Zmluva o podpore zabezpečí zrýchlenú výmenu chybného komponentu v dohodnutej servisnej úrovni 8×5×NBD.*	**SPLNIL**
Počet zariadení	10 ks	*Uchádzač ponúka 10 ks Cisco QSFP-100G-CU5M=*	**SPLNIL**

1.13 10G SFP modul typ 1

10G SFP modul typ 1			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Cisco Systems, Inc. / SFP-10G-SR-S=* ***Produkt:*** *Optický transceiver 10GBASE-SR SFP+ pre multimódové optické vlákna (MMF)* ***Edícia/verzia:*** *Cisco S-Class* ***Licenčný model:*** *Neuplatňuje sa – ide o hardvérový transceiver bez softvérovej licencie* ***Relevantné komponenty:*** *18 ks Cisco SFP-10G-SR-S=* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadovaná rýchlosť	10 Gbps	***Spĺňa.*** *Ponúkaný optický transceiver Cisco SFP-10G-SR-S= podporuje prenosovú rýchlosť 10 Gbps podľa štandardu 10GBASE-SR.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadovaná vlnová dĺžka	850nm	***Spĺňa.*** *Ponúkaný optický transceiver Cisco SFP-10G-SR-S= pracuje s nominálnou vlnovou dĺžkou 850 nm.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadovaný dosah	• 300m pre linky pripojené cez MMF OM3, • 400m pre linky pripojené cez MMF OM4	***Spĺňa.*** *Ponúkaný optický transceiver Cisco SFP-10G-SR-S= podporuje maximálny dosah:* • *300 m pri použití multimódového vlákna MMF OM3,* • *400 m pri použití multimódového vlákna MMF OM4.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**

Požadované technické vlastnosti	• formát optického modulu: SFP+, • požaduje sa výrobca identický s výrobcom požadovaných prepínačov, • verejný obstarávateľ nepripúšťa OEM moduly.	***Spĺňa.*** *Ponúkaný Cisco SFP-10G-SR-S= spĺňa požadované technické vlastnosti:* • *formát optického modulu: SFP+,* • *výrobca je identický s výrobcom ponúkaných prepínačov,* • *nejde o kompatibilný kábel tretej strany.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Záruka	• štandardná záruka: 5 rokov. Verejný obstarávateľ požaduje zabezpečenie rýchlej výmeny a to prostredníctvom zmluvy o podpore pre dodávané zariadenia, do ktorého bude modul pripojený.	***Spĺňa.*** *Na ponúkaný modul Cisco SFP-10G-SR-S= poskytuje výrobca štandardnú záruku 5 rokov. Všetkých 18 ks modulov bude priradených k servisnému krytiu Cisco pre dodávané zariadenia, ku ktorým budú pripojené. Zmluva o podpore zabezpečí zrýchlenú výmenu chybného komponentu v dohodnutej servisnej úrovni 8×5×NBD.*	**SPLNIL**
Počet zariadení	18 ks	*Uchádzač ponúka 18 ks Cisco SFP-10G-SR-S=*	**SPLNIL**

10G SFP modul typ 2

10G SFP modul typ 2			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Cisco Systems /* ***SFP-10G-SR=*** ***Produkt:*** *optický transceiver 10GBASE-SR SFP+* ***Edícia/verzia:*** *štandardný model SFP-10G-SR* ***Licenčný model:*** *bez licenčných požiadaviek* ***Relevantné komponenty:*** *16 ks Cisco SFP-10G-SR=* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadovaná rýchlosť	10 Gbps	***Spĺňa.*** *Ponúkaný optický transceiver Cisco SFP-10G-SR= v počte 16 ks podporuje technológiu 10GBASE-SR s prenosovou rýchlosťou 10 Gbps.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**

Požadovaná vlnová dĺžka	850nm	***Spĺňa.*** *Ponúkaný optický transceiver Cisco SFP-10G-SR= pracuje s menovitou vlnovou dĺžkou 850 nm.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadovaný dosah	• 300m pre linky pripojené cez MMF OM3, • 400m pre linky pripojené cez MMF OM4	***Spĺňa.*** *Ponúkaný optický transceiver Cisco SFP-10G-SR= podporuje dosah:* • *až 300 m cez multimódové optické vlákno OM3,* • *až 400 m cez multimódové optické vlákno OM4.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Požadované technické vlastnosti	• formát optického modulu: SFP+, • podpora FCoE • požaduje sa výrobca identický s výrobcom požadovaných prepínačov, • verejný obstarávateľ nepripúšťa OEM moduly.	***Spĺňa.*** *Ponúkaný Cisco SFP-10G-SR spĺňa požadované technické vlastnosti:* • *formát optického modulu: SFP+,* • *podpora FCoE,* • *výrobca je identický s výrobcom ponúkaných prepínačov,* • *nejde o kompatibilný kábel tretej strany.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html*	**SPLNIL**
Záruka	• štandardná záruka: 5 rokov. Verejný obstarávateľ požaduje zabezpečenie rýchlej výmeny a to prostredníctvom zmluvy o podpore pre dodávané zariadenia, do ktorého bude modul pripojený.	***Spĺňa.*** *Na ponúkaný modul Cisco SFP-10G-SR poskytuje výrobca štandardnú záruku 5 rokov. Všetkých 18 ks modulov bude priradených k servisnému krytiu Cisco pre dodávané zariadenia, ku ktorým budú pripojené. Zmluva o podpore zabezpečí zrýchlenú výmenu chybného komponentu v dohodnutej servisnej úrovni 8×5×NBD.*	**SPLNIL**
Počet zariadení	16 ks	*Uchádzač ponúka 16 ks Cisco SFP-10G-SR*	**SPLNIL**

1.14 100G QFP modul typ 1

100G QFP modul typ 1			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca:*** *Cisco Systems, Inc.* ***Produkt/model:*** *Cisco 100GBASE-SR4-S QSFP, QSFP-100G-SR4-S=* ***Edícia/verzia:*** *S-Class, hardvérový optický transceiver QSFP28* ***Licenčný model:*** *Bez licencie* ***Relevantné komponenty****: 4 ks optických transceiverov QSFP-100G-SR4-S=; 100 GbE, MPO, MMF, dosah do 100 m po OM4* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadovaná rýchlosť	100 Gbps	***Spĺňa.*** *Ponúkaný optický transceiver Cisco QSFP-100G-SR4-S= v počte 4 ks podporuje požadovanú prenosovú rýchlosť 100 Gbps (100 Gigabit Ethernet).* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadovaný dosah	100m pre linky pripojené cez MMF OM4 s využitím konektora MPO-12	***Spĺňa.*** *Optický transceiver Cisco QSFP-100G-SR4-S= spĺňa požadovaný dosah 100 m po multimódovom optickom vlákne MMF OM4 s využitím 12-vláknového konektora MPO-12.* *https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html*	**SPLNIL**
Požadované technické vlastnosti	• formát optického modulu: QSFP, • typ konektora: MPO-12 • požaduje sa výrobca identický s výrobcom zariadenia DC Prepínač Typ 1, • verejný obstarávateľ nepripúšťa OEM moduly.	***Spĺňa.*** *Ponúkaný Cisco QSFP-100G-SR4-S= spĺňa požadované technické vlastnosti:* • *formát optického modulu: QSFP,* • *typ konektora: MPO-12* • *výrobca je identický s výrobcom ponúkaných prepínačov DC Prepínač Typ 1,* • *nejde o kompatibilný kábel tretej strany.*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html	
Záruka	• štandardná záruka: minimálne 5 rokov. Verejný obstarávateľ požaduje zabezpečenie rýchlej výmeny a to prostredníctvom zmluvy o podpore pre dodávané zariadenia, do ktorého bude metalický 100G QSFP modul typ 1 pripojený.	***Spĺňa.*** *Na ponúkaný modul Cisco QSFP-100G-SR4-S= poskytuje výrobca štandardnú záruku 5 rokov. Všetky 4 ks modulov bude priradených k servisnému krytiu Cisco pre dodávané zariadenia, ku ktorým budú pripojené. Zmluva o podpore zabezpečí zrýchlenú výmenu chybného komponentu v dohodnutej servisnej úrovni 8×5×NBD.*	**SPLNIL**
Počet zariadení	4 ks	*Uchádzač ponúka 4 ks Cisco QSFP-100G-SR4-S=*	**SPLNIL**

1.15 Rozšírenie existujúcej serverovej infraštruktúry - Chassis

Rozšírenie existujúcej serverovej infraštruktúry - Chassis			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Cisco Systems, Inc. – Cisco UCS X-Series Direct 100G, šasi Cisco UCS X9508 (UCSX-9508-D=), 1 ks.* ***Edícia/verzia:*** *UCS X-Series Direct; aktuálna výrobcom odporúčaná verzia platformového softvéru (UCSX-CHASSIS-SW-D).* ***Licenčný model:*** *Trvalá softvérová licencia pre každý Fabric Interconnect UCS 9108-100G (UCSX-S9108-SW), bez časového obmedzenia.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-direct-ds.html* *Technická špecifikácia:* • *1x UCSX-9508-D= - UCS X-Series 9508 chassis* • *1x CON-L1NBD-UCSXD958 - CX Level 1 8x5xNBD support for UCS 9508 chassis* • *2x UCSX-9508-ACPEM-D - UCS 9508 chassis rear AC power expansion module* • *2x UCSX-F-9416-D - UCS 9416 X-Fabric module for UCS 9508 chassis* • *1x UCSX-CHASSIS-SW-D - Latest platform software for UCS X9500 chassis* • *2x UCSX-S9108-100G - UCS X-Series Direct Fabric Interconnect 9108 100G* • *2x UCSX-S9108-SW - Perpetual software license for UCS X-Series Direct Fabric Interconnect 9108 100G* • *6x UCSX-PSU-2800AC-D - UCS 9508 chassis 2800W AC dual-voltage Titanium power supply* • *6x CAB-C19-CBN - Cabinet jumper power cord, 250 VAC/16A, C20–C19 connectors*	**SPLNIL**

Požadované blade chassis	Cisco UCS 9508 Chassis Rozšírenie existujúcej serverovej infraštruktúru o Chassis zabezpečí umiestnenie existujúcich serverov Cisco UCS X215c M8 vo vlastníctve verejného obstarávateľa.	***Spĺňa.*** *Ponúkané riešenie obsahuje 1 ks Cisco UCS X9508 Chassis (UCSX-9508-D=) s ôsmimi flexibilnými slotmi. Chassis podporuje existujúce výpočtové uzly Cisco UCS X215c M8 vo vlastníctve verejného obstarávateľa a umožňuje ich priame umiestnenie a prevádzku v rámci rozšírenej infraštruktúry.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/cisco-ucs-x9508-chassis-aag.html*	**SPLNIL**
Počet blade chassis	1ks	***Spĺňa.*** *Ponúkané riešenie obsahuje 1 ks Cisco UCS X9508 Chassis (UCSX-9508-D=).* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/datasheet-c78-2472574.html*	**SPLNIL**
Požadované zdroje	2800W AC Dual Voltage PSU Titanium	***Spĺňa.*** *Chassis je vybavené 6× Cisco UCSX-PSU-2800AC-D – 2800 W AC Dual Voltage PSU, Titanium, s podporou vstupného napätia 100–127 V AC a 200–240 V AC.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/datasheet-c78-2472574.html*	**SPLNIL**
Počet zdrojov	6ks	***Spĺňa.*** *Ponúkané chassis obsahuje 6 ks napájacích zdrojov Cisco UCSX-PSU-2800AC-D, každý s výkonom 2800 W a účinnosťou Titanium.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/datasheet-c78-2472574.html*	**SPLNIL**
Požadované X-Fabric moduly	UCS 9416 X-Fabric module for 9508 chassis	***Spĺňa.*** *Ponúkané chassis obsahuje moduly Cisco UCS 9416 X-Fabric Module (UCSX-F-9416-D) určené pre Cisco UCS X9508 Chassis.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/datasheet-c78-2472574.html*	**SPLNIL**
Počet X-Fabric modulov	2ks	***Spĺňa.*** *Ponúkané chassis obsahuje 2 ks Cisco UCS 9416 X-Fabric Module (UCSX-F-9416-D).*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/datasheet-c78-2472574.html	
Požadované Fabric Interconnect moduly	UCS X-Series Direct Fabric Interconnect 9108 100G	***Spĺňa.*** *Ponúkané chassis obsahuje moduly Cisco UCS X-Series Direct Fabric Interconnect 9108 100G (UCSX-S9108-100G), ktoré zabezpečujú priamu 100Gb sieťovú a SAN konektivitu systému.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-direct-ds.html*	**SPLNIL**
Požadovaná licencia pre Fabric interconnect moduly	Perpetual SW License for UCS X-Series Direct FI 9108-100G	***Spĺňa.*** *Pre moduly Fabric Interconnect 9108-100G je dodaná časovo neobmedzená softvérová licencia Cisco UCSX-S9108-SW (Perpetual SW License), ktorá aktivuje všetky porty a softvérové funkcie FI.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/m_review_map_fi_initial_setup.html*	**SPLNIL**
Počet Fabric Interconnect moduly	2ks	***Spĺňa.*** *Ponúkané chassis obsahuje 2 ks Cisco UCS X-Series Direct Fabric Interconnect 9108 100G (UCSX-S9108-100G).* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-direct-ds.html*	**SPLNIL**
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • výmena zariadenia v prípade poruchy v režime 8x5xNBD, • centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: ○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora, ○ prístup k softvérovým aktualizáciám, opravným verziám, bezpečnostným	***Spĺňa.*** • *Pre Cisco UCS X9508 Chassis je poskytovaná servisná podpora Cisco CX Level 1 / Cisco Support Standard, 8x5xNBD (CON-L1NBD-UCSXD958) na obdobie 24 mesiacov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Podpora zahŕňa rozšírenú výmenu chybného hardvéru v režime 8 hodín denne, 5 pracovných dní v týždni, s dodaním náhrady nasledujúci pracovný deň – 8x5xNBD.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Cisco Support Standard poskytuje centralizovanú technickú podporu a správu incidentov naprieč podporovanými*	**SPLNIL**

	opravám, odporúčaným postupom a technickej dokumentácii výrobcu počas celej doby trvania podpory ○ výrobca poskytne podporu na úrovni riešení, ktorá zahŕňa centralizovanú expertízu a správu problémov v rámci riešenia produktov výrobcu a tretích strán schválených výrobcom ○ podpora na úrovni riešení sa vzťahuje na riešenia pozostávajúce z produktov výrobcu a schválených partnerov výrobcu (minimálne VMware a Veeam, ktorými už aktuálne disponuje verejný obstarávateľ), kde je zabezpečený prístup k tímu expertov na riešenia, ktorí pôsobia ako primárny kontaktný bod a ktorí buď ○ aktívne riadia problém až do jeho vyriešenia expertmi na produkty, ○ alebo v rozsahu povolenom partnermi Solution Alliance koordinujú vaše kroky na podporu riešenia problému ○ poskytovateľ podpory musí byť primárny bod kontaktu pre incidenty v riešení, ○ v prípade, ak riešenie pozostáva z produktov výrobcu a produktov jeho aliančných partnerov na podporu riešení, musia byť riešenia vytvorené z približne 50 % alebo viac produktami výrobcu, aby boli oprávnené na takto popisovaný typ podpory,	*hardvérovými a softvérovými komponentmi Cisco a schválenými produktmi aliančných partnerov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Podpora sa vzťahuje na podporované hardvérové aj softvérové produkty Cisco tvoriace dodávané riešenie a zahŕňa technickú asistenciu, softvérovú podporu, hardvérové RMA a centralizovanú správu incidentov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Počas 24-mesačného obdobia podpory je zabezpečený prístup k dostupným softvérovým vydaniam, aktualizáciám, opravným verziám, bezpečnostným odporúčaniam, náhradným riešeniam, odporúčaným postupom a technickej dokumentácii Cisco.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Cisco poskytuje podporu na úrovni riešenia zahŕňajúcu centralizovanú expertízu a správu problémov naprieč produktmi Cisco a produktmi tretích strán schválených ako Cisco Solution Alliance Partner.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Cisco sprístupňuje tím expertov na riešenia, ktorý vystupuje ako primárny kontaktný bod, aktívne riadi incident až do vyriešenia produktovými expertmi alebo koordinuje riešenie s aliančným partnerom. Podpora zahŕňa oprávnené riešenia s technológiami VMware a Veeam, ak sú pokryté aktívnymi podpornými kontraktmi príslušných výrobcov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hyperflexedge_veeam.html*	

	○ dostupnosť podporného centra v požadovanom režime 24x7 formou telefónu, mailu, alebo cez web prístup k riešeniam pri používaní, konfigurácii, alebo pri riešení problémov: ▪ pre závažnosť hovorov 1 a 2 musí byť odpoveď Centra výrobcu do 30min, ▪ pre závažnosť hovorov 3 a 4 musí byť odpoveď Centra výrobcu do 60min počas pracovných hodín, resp. nasledujúci pracovný deň pri hovoroch mimo pracovných hodín, ○ v prípade komunikácie s výrobcom iných súčasti riešenia je nevyhnutné preukázať existenciu supportných kontraktov u týchto výrobcov.	• *Cisco je primárnym kontaktným bodom pre incidenty v podporovanom riešení, zabezpečuje správu incidentu a poskytuje informácie o vykonaných krokoch až do jeho vyriešenia.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Cisco Solution Support umožňuje pokrytie multivendorových riešení, ktoré sú vytvorené približne z 50 % alebo viac produktmi Cisco.* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf* • *Cisco TAC je dostupný 24x7 telefonicky a prostredníctvom webového prístupu na riešenie problémov s používaním, konfiguráciou a prevádzkou riešenia. Pre úroveň Cisco Support Standard sú reakčné časy:* ○ *závažnosť 1 a 2: do 30 minút,* ○ *závažnosť 3 a 4: do 60 minút počas pracovných hodín,* ○ *závažnosť 3 a 4 mimo pracovných hodín: nasledujúci pracovný deň.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Pri riešení incidentov týkajúcich sa produktov aliančných partnerov musí mať verejný obstarávateľ počas celej doby podpory aktívne podporné kontrakty príslušných výrobcov, najmä pre používané produkty VMware a Veeam. Tieto kontrakty slúžia ako oprávnenie Cisco na koordináciu incidentu s podporou daného výrobcu.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf*	
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie dodaných zariadení prípadne	• *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti*	**SPLNIL**

	softvérov pre preukázanie funkčnosti a prevádzkyschopnosti dodaného zariadenia Rozšírenie existujúcej serverovej infraštruktúry - Chassis. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného zariadenia Rozšírenie existujúcej serverovej infraštruktúry - Chassis. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané zariadenia Rozšírenie existujúcej serverovej infraštruktúry – Chassis.	*a prevádzkyschopnosti dodaného* zariadenia Rozšírenie existujúcej serverovej infraštruktúry - Chassis. • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného* zariadenia Rozšírenie existujúcej serverovej infraštruktúry - Chassis. • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Cisco Black Belt Academy – Unified Computing System (UCS) Deployment Stage 3 vydaný výrobcom Black Belt Academy Cisco Systems, Inc. pre dodávané zariadenia Rozšírenie existujúcej serverovej infraštruktúry – Chassis.*	

1.16 Rozšírenie licencií existujúcej virtualizačnej platformy VMware VSPHERE FOUNDATION

Rozšírenie licencií existujúcej virtualizačnej platformy VMware VSPHERE FOUNDATION			**Hodnotenie (SPLNIL / NESPLNIL)**
Parameter:	**Minimálne požadované parametre:**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *VMware by Broadcom – VMware vSphere Foundation 9.1 (VVF), SKU VCF-VSP-FND-1Y.* *Licenčný model: časovo obmedzené predplatné podľa počtu fyzických CPU jadier (192 jadier, kontrakt na 2 roky), minimálne 16 licencovaných jadier na procesor.* *Riešenie zahŕňa komponenty VMware vSphere/ESX, vCenter Server Standard, vSphere Kubernetes Service, VCF Operations a VMware vSAN.* *https://www.vmware.com/docs/vmware-cloud-foundation-9-1-feature-comparison-and-upgrade-paths* *https://ftpdocs.broadcom.com/cadocs/0/contentimages/VVF_SPD_November2025.pdf*	**SPLNIL**

Predmet dodávky	Poskytnutie predplatného (subscription) na rozšírenie licencovania existujúcej virtualizačnej platformy o licencie VMware vSphere Foundation s Core licenčným modelom vo vlastníctve verejného obstarávateľa	***Spĺňa.*** *Predmetom dodávky je predplatné VMware vSphere Foundation (VVF), SKU VCF-VSP-FND-1Y, na rozšírenie existujúcej virtualizačnej platformy verejného obstarávateľa o licenčnú kapacitu 192 fyzických CPU jadier (Core) na obdobie 2 rokov. Licencovanie je založené na počte fyzických jadier hostiteľských serverov, minimálne 16 jadier na jeden procesor.* *https://www.vmware.com/products/cloud-infrastructure/vsphere-foundation* *https://ftpdocs.broadcom.com/cadocs/0/contentimages/VVF_SPD_November2025.pdf*	**SPLNIL**
Počet zalicencovaných jadier na prevádzku virtualizačnej platformy	192 ks	***Spĺňa.*** *Ponúkané predplatné VMware vSphere Foundation, SKU VCF-VSP-FND-1Y, zabezpečuje licencovanie 192 fyzických CPU jadier (192 Core licencií) na prevádzku virtualizačnej platformy.* *https://ftpdocs.broadcom.com/cadocs/0/contentimages/VVF_SPD_November2025.pdf*	**SPLNIL**
Celková požadovaná doba predplatného pre licencie virtualizačnej platformy	2 roky	***Spĺňa.*** *Ponúkané predplatné VMware vSphere Foundation, SKU VCF-VSP-FND-1Y, bude zabezpečené na celkové obdobie 2 rokov (24 mesiacov).* *https://ftpdocs.broadcom.com/cadocs/0/contentimages/VVF_SPD_November2025.pdf*	**SPLNIL**
Kompatibilita a integrácia	• Dodané licencie musia byť kompatibilné s aktuálnou infraštruktúrou verejného obstarávateľa a umožňovať integráciu s existujúcim prostredím. • Predplatné musí byť registrovateľné priamo na verejného obstarávateľa ako vlastníka licencie	***Spĺňa.*** *Dodané licencie VMware vSphere Foundation budú kompatibilné s existujúcou VMware infraštruktúrou a umožnia rozšírenie licenčnej kapacity a integráciu prostredníctvom existujúceho prostredia vCenter Server.* *Predplatné bude registrované priamo na zákaznícky účet a Site ID verejného obstarávateľa v Broadcom Support Portal. Verejný obstarávateľ bude evidovaný ako koncový zákazník a držiteľ licenčného oprávnenia s prístupom k licenciám, softvéru a podpore v časti My Entitlements.* https://knowledge.broadcom.com/external/article/319282/vmware-cloud-foundation-and-vsphere-foun.html https://knowledge.broadcom.com/external/article/188869	**SPLNIL**

Administrácia a reporting	• Súčasťou predplatného musí byť prístup do administrátorského portálu pre správu licencií a monitoring využitia. • Uchádzač je povinný poskytnúť asistenciu pri aktivácii predplatného a overení jeho funkčnosti.	***Spĺňa.*** • *Súčasťou predplatného bude prístup oprávnených administrátorov verejného obstarávateľa do Broadcom Support Portal a pre VVF 9.x aj do VMware Cloud Foundation Business Services Console, ktoré umožňujú správu licenčných oprávnení, licenčných súborov a monitoring využitia licencií prostredníctvom VCF Operations.* • *Uchádzač poskytne asistenciu pri priradení predplatného k Site ID verejného obstarávateľa, aktivácii licencií, nastavení administrátorského prístupu a overení správnej funkčnosti a licenčnej kapacity.* *https://knowledge.broadcom.com/external/article/392124/accessing-vmware-license-folders-and-key.html*	**SPLNIL**
Podpora a údržba	• Predmetom predplatného je aj technická podpora výrobcu/dodávateľa s možnosťou kontaktu 24/7. • Garantovaná doba odozvy na kritické incidenty: max. 4 hodiny. • Zahrnuté musia byť všetky aktualizácie, upgrade verzií a bezpečnostné záplaty počas obdobia platnosti predplatného.	***Spĺňa.*** • *Predplatné VMware vSphere Foundation zahŕňa VMware Production Support s možnosťou nahlasovania požiadaviek 24/7 a nepretržitou podporou kritických incidentov Severity 1.* • *Uchádzač garantuje odozvu na kritický incident najneskôr do 4 hodín; cieľová úvodná odozva výrobcu pre Severity 1 je do 30 minút.* • *Počas celej platnosti predplatného sú zahrnuté všetky výrobcom sprístupnené aktualizácie, nové verzie, upgrady a bezpečnostné záplaty.* *https://docs.broadcom.com/docs/vmware-production-support-datasheet* *https://blogs.vmware.com/cloud-foundation/2024/01/17/embracing-change-with-vmware-vsphere-foundation/* *https://knowledge.broadcom.com/external/article/281797/upgrade-and-downgrade-vmware-license-key.html*	**SPLNIL**

1.17 Požiadavky na SW komponent - Rozšírenie licencií existujúcej virtualizačnej platformy VMware VSPHERE STANDARD

Rozšírenie licencií existujúcej virtualizačnej platformy VMware VSPHERE STANDARD			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *VMware by Broadcom – VMware vSphere Foundation (VVF), SKU VCF-VSP-FND-1Y.* ***Edícia/verzia****: VMware vSphere 8 Enterprise Plus for vSphere Foundation, podporujúca vCenter Server 8.0 Update 2b a novší.* ***Licenčný model****: časovo obmedzené jednoročné predplatné licencované podľa počtu fyzických CPU jadier, v ponúkanom rozsahu 256 core.* *Uchádzač zabezpečí nepretržité licenčné a podporné krytie počas požadovaných 24 mesiacov prostredníctvom dvoch bezprostredne nadväzujúcich jednoročných období.* *Relevantné komponenty riešenia: VMware vSphere/ESXi Enterprise Plus for vSphere Foundation, VMware vCenter Server 8 Standard Term, VMware Aria Suite Standard 8.14, VMware Tanzu Kubernetes Grid for vSphere Foundation a VMware vSAN 8 for Foundation. Riešenie je použiteľné aj na rozšírenie existujúceho prostredia (brownfield); pri verziách starších ako vSphere 8.0 Update 2b výrobca umožňuje použitie príslušných komponentových licenčných kľúčov.* *https://knowledge.broadcom.com/external/article/319282/vmware-cloud-foundation-and-vsphere-foun.html* *https://knowledge.broadcom.com/external/article/313548/counting-cores-for-vmware-cloud-foundati.html*	**SPLNIL**
Predmet dodávky	Poskytnutie predplatného (subscription) na rozšírenie licencovania existujúcej virtualizačnej platformy o licencie VMware vSphere Foundation s Core licenčným modelom vo vlastníctve verejného obstarávateľa.	***Spĺňa****.* *Predmetom dodávky je predplatné VMware vSphere Foundation (VVF), SKU VCF-VSP-FND-1Y, na rozšírenie existujúcej virtualizačnej platformy verejného obstarávateľa o 256 licencovaných fyzických CPU jadier. Licenčný model je subscription per core.* *Uchádzač zabezpečí nepretržité licenčné a podporné krytie počas 24 mesiacov prostredníctvom dvoch nadväzujúcich jednoročných období.* *Licenčné oprávnenie bude evidované na príslušnom Broadcom Site ID verejného obstarávateľa.*	**SPLNIL**

		https://knowledge.broadcom.com/external/article/313548/counting-cores-for-vmware-cloud-foundati.html https://knowledge.broadcom.com/external/article/319282/vmware-cloud-foundation-and-vsphere-foun.html	
Počet zalicencovaných jadier na prevádzku virtualizačnej platformy	256 ks	***Spĺňa.*** *Ponúkané predplatné VMware vSphere Foundation zahŕňa licenčné oprávnenie na 256 fyzických CPU jadier (256 core) určených na prevádzku virtualizačnej platformy.* *https://knowledge.broadcom.com/external/article/313548/counting-cores-for-vmware-cloud-foundati.html*	**SPLNIL**
Celková požadovaná doba predplatného pre licencie virtualizačnej platformy	2 roky	***Spĺňa.*** *Uchádzač zabezpečí predplatné VMware vSphere Foundation pre 256 jadier na celkové obdobie 24 mesiacov. Keďže ponúkaný SKU VCF-VSP-FND-1Y predstavuje jednoročné predplatné, licenčné a podporné krytie bude zabezpečené dvomi bezprostredne nadväzujúcimi 12-mesačnými obdobiami bez prerušenia.* *https://knowledge.broadcom.com/external/article/207581/* *https://knowledge.broadcom.com/external/article/319282/vmware-cloud-foundation-and-vsphere-foun.html*	**SPLNIL**
Kompatibilita a integrácia	• dodané licencie musia byť kompatibilné s aktuálnou infraštruktúrou verejného obstarávateľa a umožňovať integráciu s existujúcim prostredím. Predplatné musí byť registrované priamo na verejného obstarávateľa ako vlastníka licencie.	***Spĺňa.*** *Licencie VMware vSphere Foundation sú určené aj na integráciu do existujúceho prostredia VMware vSphere (brownfield). Pre vSphere 8.0 Update 2b a novší sa solution license key aplikuje priamo na existujúci vCenter Server a ESXi hosty. Pre staršie podporované verzie výrobca poskytuje príslušné komponentové licenčné kľúče a možnosť downgrade.* *Predplatné bude objednané na verejného obstarávateľa a priradené k jeho Broadcom Site ID. Verejný obstarávateľ bude vedený ako držiteľ licenčného oprávnenia (entitlement) s prístupom k licenciám, softvéru a podpore prostredníctvom Broadcom Support Portal.* *https://knowledge.broadcom.com/external/article/319282/vmware-cloud-foundation-and-vsphere-foun.html* *https://knowledge.broadcom.com/external/article/188869*	**SPLNIL**

Administrácia a reporting	• Súčasťou predplatného musí byť prístup do administrátorského portálu pre správu licencií a monitoring využitia. • Uchádzač je povinný poskytnúť asistenciu pri aktivácii predplatného a overení jeho funkčnosti.	***Spĺňa.*** • *Súčasťou predplatného bude prístup oprávnených administrátorov verejného obstarávateľa do Broadcom Support Portal a pre VVF 9.x aj do VMware Cloud Foundation Business Services Console, ktoré umožňujú správu licenčných oprávnení, licenčných súborov a monitoring využitia licencií prostredníctvom VCF Operations.* • *Uchádzač poskytne asistenciu pri priradení predplatného k Site ID verejného obstarávateľa, aktivácii licencií, nastavení administrátorského prístupu a overení správnej funkčnosti a licenčnej kapacity.* *https://knowledge.broadcom.com/external/article/392124/accessing-vmware-license-folders-and-key.html*	**SPLNIL**
Podpora a údržba	• Predmetom predplatného je aj technická podpora výrobcu/dodávateľa s možnosťou kontaktu 24/7. • Garantovaná doba odozvy na kritické incidenty: max. 4 hodiny. • Zahrnuté musia byť všetky aktualizácie, upgrade verzií a bezpečnostné záplaty počas obdobia platnosti predplatného.	***Spĺňa.*** • *Predplatné VMware vSphere Foundation zahŕňa VMware Production Support s možnosťou nahlasovania požiadaviek 24/7 a nepretržitou podporou kritických incidentov Severity 1.* • *Uchádzač garantuje odozvu na kritický incident najneskôr do 4 hodín; cieľová úvodná odozva výrobcu pre Severity 1 je do 30 minút.* • *Počas celej platnosti predplatného sú zahrnuté všetky výrobcom sprístupnené aktualizácie, nové verzie, upgrady a bezpečnostné záplaty.* *https://docs.broadcom.com/docs/vmware-production-support-datasheet* *https://blogs.vmware.com/cloud-foundation/2024/01/17/embracing-change-with-vmware-vsphere-foundation/* *https://knowledge.broadcom.com/external/article/281797/upgrade-and-downgrade-vmware-license-key.html*	**SPLNIL**

1.18 Rozšírenie licencií existujúceho zálohovacieho riešenia

Rozšírenie licencií existujúceho zálohovacieho riešenia			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Veeam Software – Veeam Data Platform Advanced, SKU P-ADV000-1S-SU2YP-00, aktuálna podporovaná verzia 13.1.* ***Riešenie obsahuje:*** *Veeam Backup & Replication s funkciami edície Enterprise Plus a Veeam ONE.* ***Licenčný model****: 6× CPU socket pre VMware vSphere/Microsoft Hyper-V, dvojročné predplatné s podporou Production 24×7, Public Sector.* *https://www.veeam.com/legal/licensing-policy.html* *https://helpcenter.veeam.com/category/vdp.html*	**SPLNIL**
Požadovaná Licencia	Veeam Data Platform Advanced Socket-Subscription License. - 1 socket. Includes Enterprise Plus Edition features. 2 Years Subscription Upfront Billing & Production (24/7) Support. Public Sector.	***Spĺňa****.* *Ponúkané riešenie obsahuje 6 ks licencií Veeam Data Platform Advanced Socket-Subscription License, SKU P-ADV000-1S-SU2YP-00, každú pre 1 CPU socket. Licencia zahŕňa funkcie Enterprise Plus, dvojročné predplatné s platbou vopred a podporu Production 24×7 pre verejný sektor.* *https://www.veeam.com/legal/licensing-policy.html*	**SPLNIL**
Funkčnosť	• Licencie musia zahŕňať všetky funkcionality dostupné v rámci Enterprise Plus Edition, vrátane pokročilých možností ochrany dát, replikácie a rýchlej obnovy. • Musia podporovať hybridné prostredia (virtuálne, fyzické, cloudové a Kubernetes). • Podpora inkrementálneho zálohovania, dlhodobej	***Spĺňa****.* • *socketová licencia Veeam Data Platform Advanced poskytuje funkcie Enterprise Plus vrátane inkrementálneho zálohovania, replikácie, dlhodobej archivácie a Instant Recovery* • podporuje hybridné prostredia (virtuálne, fyzické, cloudové a Kubernetes). • podpodporuje inkrementálne zálohovanie, dlhodobú archivácia a okamžitú obnovu dát. *https://www.veeam.com/legal/licensing-policy.html* *https://helpcenter.veeam.com/docs/vbr/userguide/forward_incremental_backup_hv.html* *https://helpcenter.veeam.com/docs/vbr/userguide/archive_tier.html* *https://helpcenter.veeam.com/docs/vbr/userguide/instant_recovery.html*	**SPLNIL**

	archivácie a okamžitej obnovy dát.		
Počet licencií	6 ks	***Spĺňa.*** *Ponúkané riešenie obsahuje 6 ks licencií Veeam Data Platform Advanced, SKU P-ADV000-1S-SU2YP-00, pričom každá licencia pokrýva 1 CPU socket; celkový licenčný rozsah je 6 CPU socketov.* *https://www.veeam.com/legal/licensing-policy.html*	**SPLNIL**
Celková požadovaná doba predplatného licencie zálohovacieho riešenia	2 roky	*Ponúkaných 6 ks licencií Veeam Data Platform Advanced, SKU P-ADV000-1S-SU2YP-00, zahŕňa predplatné na požadované obdobie 2 rokov s platbou vopred a podporou Production 24×7.* *https://www.veeam.com/legal/licensing-policy.html*	**SPLNIL**
Podpora a údržba	• Súčasťou dodávky musí byť Production Support (režim 24/7) spolu po dobu 2 rokov. • Podpora musí zahŕňať prístup k aktualizáciám, opravám a novým verziám softvéru vrátane garantovanej reakcie výrobcu na kritické incidenty v maximálnej lehote 4 hodín.	***Spĺňa.*** • *Súčasťou všetkých 6 licencií je Veeam Production Support v režime 24×7×365 počas celej doby predplatného 2 rokov.* • *Podpora zahŕňa produktové aktualizácie, opravy a nové verzie softvéru. Pre kritický incident kategórie Severity 1 stanovuje výrobca reakčnú SLA 1 hodinu, čím je požadovaná maximálna lehota 4 hodín splnená s rezervou.* *https://www.veeam.com/legal/support-policy.html*	**SPLNIL**
Administrácia	• Licencie musia poskytovať prístup do administračného portálu pre správu inštancií, monitoring zálohovacích úloh a reporting. • Dodávateľ musí poskytnúť asistenciu pri aktivácii licencií a overení ich plnej funkčnosti.	***Spĺňa.*** • *Riešenie poskytuje centralizovanú webovú správu a aktiváciu licencií prostredníctvom Veeam Backup Enterprise Manager. Komponent Veeam ONE, zahrnutý v edícii Advanced, zabezpečuje monitoring zálohovacích úloh, alarmy, dashboardy a reporting.* • *Dodávateľ poskytne asistenciu pri registrácii, aktivácii všetkých licencií a overení ich plnej funkčnosti.* *https://helpcenter.veeam.com/docs/vbr/em/managing_licenses.html* *https://helpcenter.veeam.com/docs/one/userguide/about_one.html*	**SPLNIL**

		https://www.veeam.com/legal/licensing-policy.html	
Kompatibilita a integrácia	• Licencie musia byť kompatibilné s existujúcou infraštruktúrou obstarávateľa (virtualizované prostredia, servery, storage). • Musia umožniť jednoduchú integráciu do už využívaného zálohovacieho riešenia.	***Spĺňa.*** • *Ponúkané licencie sú kompatibilné s podporovanými prostrediami VMware vSphere a Microsoft Hyper-V, servermi zálohovacej infraštruktúry a podporovanými diskovými, sieťovými, deduplikačnými a objektovými úložiskami.* • *Do existujúceho riešenia Veeam Backup & Replication sa integrujú inštaláciou alebo aktualizáciou licenčného kľúča bez potreby migrácie konfigurácie. Kompatibilita konkrétnych verzií komponentov bude overená pri aktivácii.* *https://helpcenter.veeam.com/docs/vbr/userguide/system_requirements.html* *https://helpcenter.veeam.com/docs/vbr/userguide/backup_repository_sobr.html* *https://helpcenter.veeam.com/docs/vbr/userguide/install_license_console.html*	**SPLNIL**

2. Monitorovaná lokalita

2.1 NDR (senzor, collector) - monitorovaná lokalita

NDR (senzor, collector) - monitorovaná lokalita			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *GREYCORTEX s.r.o. – GREYCORTEX Mendel 5.0, edícia Sensor + Collector s rozšírením ICS/SCADA Pack.* ***Licenčný model a komponenty:*** *4× perpetuálna licencia MA-SC-4k-SW (4 Gbit/s, 3 000 obojsmerných tokov/s, 6 000 NetFlow/s, 16 000 monitorovaných IP adries, PinA) a 4× perpetuálne rozšírenie ME-ICS-SC-50-SW pre monitorovanie 50 ICS/SCADA zariadení. Súčasťou je podpora a údržba v rozsahu 8 ročných jednotiek pre základné licencie a 8 ročných jednotiek pre ICS/SCADA rozšírenia, t. j. 2 roky na každú licenciu.* *https://www.greycortex.com/mendel* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	**SPLNIL**
Predmet dodávky a počet	dodávka 4 ks virtuálneho NDR (senzor, collector) - monitorovaná lokalita určeného na pasívny zber, analýzu a spracovanie kópie sieťovej prevádzky. Súčasťou dodávky musí byť kompletný softvér, licencie, aktualizácie.	***Spĺňa.*** *Predmetom dodávky sú 4 ks virtuálneho NDR riešenia GREYCORTEX Mendel 5.0, každý v konfigurácii Sensor + Collector, určeného na pasívny zber, analýzu a spracovanie kópie sieťovej prevádzky prostredníctvom TAP/SPAN/RSPAN/ERSPAN. Každá inštancia obsahuje perpetuálnu licenciu MA-SC-4k-SW a rozšírenie ME-ICS-SC-50-SW pre 50 ICS/SCADA zariadení. Dodávka zahŕňa kompletný softvér, licencie a aktualizácie počas 24-mesačnej podpory a údržby.* *https://www.greycortex.com/mendel* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	**SPLNIL**
Účel riešenia	musí zabezpečiť detailnú viditeľnosť sieťovej prevádzky, vizualizáciu komunikácie koncových zariadení, služieb a podsietí, forenznú analýzu sieťových tokov a detekciu	***Spĺňa.*** *Požiadavka je splnená. GREYCORTEX Mendel zabezpečuje detailnú viditeľnosť monitorovanej sieťovej prevádzky a vizualizáciu komunikácie koncových zariadení, služieb, podsietí a komunikačných väzieb. Ukladá a indexuje obohatené metadáta obojsmerných sieťových tokov na účely spätnej forenznej*	**SPLNIL**

	bezpečnostných aj prevádzkových anomálií v monitorovanej sieti.	*analýzy. Pomocou behaviorálnej analýzy, strojového učenia, IDS signatúr a monitorovania výkonu deteguje bezpečnostné hrozby, prevádzkové anomálie a výkonnostné problémy.* *https://www.greycortex.com/mendel* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	
Architektúra riešenia	• musí pozostávať minimálne z jednej virtuálnej sondy/senzora na zber a predspracovanie dát a z konzoly alebo časti platformy na vyhodnocovanie, koreláciu, administráciu a reporting, pričom má ísť o jedno zariadenie, ktoré obsahuje obe funkcionality. • softvérová časť riešenia musí tvoriť jeden ucelený celok od jedného výrobcu.	***Spĺňa.*** • *Každá dodávaná virtuálna inštancia GREYCORTEX Mendel MA-SC-4k-SW predstavuje jedno zariadenie typu All-in-One, ktoré obsahuje funkcie senzora aj kolektora. Senzor zabezpečuje zber a predspracovanie sieťových dát, zatiaľ čo kolektor poskytuje vyhodnocovanie, koreláciu udalostí, administráciu, forenznú analýzu a reporting prostredníctvom webového rozhrania.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf* • *Celú softvérovú časť riešenia vrátane senzora, kolektora, analytických a detekčných funkcií, administrácie, reportingu a rozšírenia ICS/SCADA Pack tvorí jednotná platforma GREYCORTEX Mendel od jedného výrobcu – GREYCORTEX s.r.o.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	**SPLNIL**
Vyhotovenie zariadenia	• musí byť dodaný ako virtuálne zariadenie. • musí obsahovať všetky komponenty potrebné na prevádzku vrátane operačného prostredia, aplikačných komponentov, interného úložiska a manažmentového rozhrania. • riešenie nesmie vyžadovať dodatočné licencovanie	***Spĺňa.*** • *Požiadavka je splnená. GREYCORTEX Mendel MA-SC-4k-SW bude dodaný ako virtuálne zariadenie typu All-in-One, ktoré v jednej inštancii obsahuje senzor aj kolektor. Virtuálne nasadenie je podporované na platformách VMware, KVM a Microsoft Hyper-V.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf* • *Virtuálne zariadenie GREYCORTEX Mendel obsahuje integrované operačné prostredie CentOS, aplikačné komponenty senzora a kolektora, internú databázu a dátové úložisko realizované na pridelených virtuálnych diskoch. Administrácia, konfigurácia, analýza a reporting sa*	**SPLNIL**

	základných systémových komponentov tretích strán na strane obstarávateľa.	*vykonávajú prostredníctvom integrovaného webového manažmentového rozhrania.* *https://www.greycortex.com/blog/greycortex-mendel-44-released* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Operačné prostredie, databázové a aplikačné komponenty sú súčasťou virtuálneho zariadenia a licencie GREYCORTEX Mendel. Na strane verejného obstarávateľa sa nevyžaduje samostatné licencovanie operačného systému, databázy ani aplikačného runtime; verejný obstarávateľ poskytne iba zdroje existujúcej podporovanej virtualizačnej platformy.* *https://www.greycortex.com/blog/greycortex-mendel-44-released* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf*	
Výkonnostná trieda	• riešenie musí byť dimenzované na spracovanie monitorovanej sieťovej prevádzky minimálne v triede 4 Gbit/s alebo ekvivalentnej výkonnostnej triede deklarovanej výrobcom. • navrhnuté riešenie musí zvládnuť spracovať prevádzku privádzanú na monitorovacie rozhrania bez degradácie existujúcej produkčnej siete.	***Spĺňa.*** • *Každá zo štyroch virtuálnych inštancií GREYCORTEX Mendel je licencovaná prostredníctvom MA-SC-4k-SW na trvalé spracovanie monitorovanej sieťovej prevádzky s priepustnosťou 4 Gbit/s. Výrobca pre zariadenia typu All-in-One deklaruje výkonnostné triedy až do 10 Gbit/s.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf* • *GREYCORTEX Mendel pracuje pasívne a mimo dátovej cesty produkčnej komunikácie. Spracúva iba kópiu prevádzky privádzanú prostredníctvom TAP, SPAN, RSPAN alebo ERSPAN na monitorovacie rozhrania. Keďže riešenie nie je zapojené inline, neovplyvňuje priepustnosť, latenciu ani dostupnosť existujúcej produkčnej siete.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	**SPLNIL**
Monitorovacie a sieťové rozhrania	• riešenie musí podporovať pasívny príjem kópie prevádzky zo SPAN/mirror portov, TAP zariadení, RSPAN, ERSPAN	***Spĺňa.*** • *GREYCORTEX Mendel podporuje pasívny príjem a analýzu kópie prevádzky zo sieťových TAP zariadení, SPAN/mirror portov, RSPAN, ERSPAN a ďalších zdrojov zrkadlenej prevádzky.*	**SPLNIL**

	alebo ekvivalentného zdroja monitorovanej prevádzky. • monitorovacie rozhrania musia byť oddelené od manažmentového rozhrania. • nasadenie musí byť out-of-band, bez potreby zaradenia zariadenia inline do produkčnej komunikácie.	https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf • *Virtuálne zariadenie GREYCORTEX Mendel bude nakonfigurované so samostatnými virtuálnymi sieťovými rozhraniami pre pasívny príjem monitorovanej prevádzky a pre manažment. Monitorovacie rozhrania budú oddelené od manažmentovej siete a manažment bude dostupný prostredníctvom samostatného rozhrania s webovým GUI.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf • *GREYCORTEX Mendel sa nasadzuje out-of-band a spracúva iba kópiu sieťovej prevádzky. Zariadenie sa nezaraďuje inline do produkčnej komunikácie, preto nepredstavuje prenosový bod ani bod zlyhania produkčnej siete.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	
Bezpečnosť nasadenia	• implementácia a prevádzka riešenia nesmie obmedziť, prerušiť ani ohroziť existujúcu prevádzku a bezpečnosť počítačovej siete. • riešenie nesmie obsahovať skrytý administrátorský alebo výrobcom nezdokumentovaný prístup. • komunikácia medzi senzorom a centrálnou časťou riešenia musí byť šifrovaná štandardnými kryptografickými protokolmi, minimálne TLS.	***Spĺňa.*** • *GREYCORTEX Mendel je implementovaný pasívne v režime out-of-band a analyzuje iba kópiu prevádzky zo SPAN/RSPAN/ERSPAN alebo TAP. Nie je zaradený do produkčnej dátovej cesty, preto jeho implementácia, prevádzka ani prípadná nedostupnosť neobmedzí a nepreruší produkčnú komunikáciu.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf • *Riešenie neobsahuje skrytý ani výrobcom nezdokumentovaný administrátorský prístup. Administratívny a servisný prístup sa vykonáva výhradne prostredníctvom zdokumentovaných používateľských účtov a rolí s riadeným oprávnením a auditovateľnosťou aktivít.* https://www.greycortex.com/sites/default/files/perm/document/mendel-4.6-features-list-en.pdf • *V dodávanej konfigurácii All-in-One sú senzor a kolektor súčasťou jednej virtuálnej appliance. Komunikácia medzi komponentmi riešenia je zabezpečená štandardným kryptografickým protokolom TLS minimálne vo verzii TLS 1.2.*	**SPLNIL**

		https://www.greycortex.com/blog/validating-internal-network-policies-access-control-and-encryption https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf	
Požiadavky na metódy detekcie a detekčné schopnosti - Metódy detekcie	• musí byť použitá metóda detekcie počítačových útokov na základe rozpoznania anomálií v sieťovej prevádzke. • anomálie musia byť identifikované porovnaním aktuálneho správanie voči správaniu za minulé obdobie. • detekcia minimálne pre jednotlivé zariadenia v sieti, pre jednotlivé služby v sieti a pre jednotlivé podsiete. • detekcia musí byť realizovaná na základe modelovania koncových klientov EPM - End Point Modeling. • detekcia odchýlok od predikovaného správania musí byť realizovaná proti historickému modelu správania všetkých hostov v sieti, všetkých služieb na každom hostovi v sieti a jednotlivých podsietí. • metóda detekcie počítačových útokov musí byť realizovaná na základe sieťovej behaviorálnej analýzy komunikácie, t.j.	***Spĺňa.*** • *GREYCORTEX Mendel využíva behaviorálnu analýzu sieťovej prevádzky, štatistické metódy a strojové učenie na rozpoznávanie anomálií a detekciu známych aj neznámych počítačových útokov.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Mendel vytvára adaptívne modely historického správania siete a porovnáva s nimi aktuálnu prevádzku. Modely správania sa automaticky pravidelne prepočítavajú a prispôsobujú zmenám monitorovaného prostredia.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf • *Behaviorálne modelovanie a detekcia anomálií sa vykonávajú samostatne pre monitorované podsiete, jednotlivé koncové zariadenia a služby prevádzkované na každom zariadení.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf • *GREYCORTEX Mendel realizuje EPM prostredníctvom individuálneho modelovania správania každého monitorovaného koncového zariadenia vrátane jeho služieb, komunikačných partnerov, portov, objemu dát a počtu sieťových tokov.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf • *Aktuálne správanie sa porovnáva s historickými modelmi všetkých monitorovaných hostov, služieb na jednotlivých hostoch a podsietí. Odchýlky od predikovaného správania sú vyhodnocované ako anomálie.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf	**SPLNIL**

	detekcia vzorov správania za pomoci detekčných pravidiel. • detekcia opakujúceho sa správania musí byť realizovaná so spätnou analýzou každého hosta a každej služby minimálne aspoň 6 hodín. • metóda detekcie porušenia interných bezpečnostných politík pomocou sieťovej behaviorálnej analýzy musí byť cielená na dodržiavanie politikou definovaných komunikačných matíc a komunikačných vektorov. • metóda detekcie kybernetických útokov musí byť realizovaná na základe sieťovej behaviorálnej analýzy cielenej na rozpoznanie strojového a ľudského chovania v dlhodobých časových intervaloch. • metóda pre detekciu aplikačných a sieťových výkonnostných problémov a anomálií musí byť realizovaná za pomoci analýzy sieťových výkonnostných metrík (aspoň. RTT, ART). • metoda detekcie kybernetických útokov musí byť realizovaná na základe	• *Mendel využíva sieťovú behaviorálnu a tokovú analýzu na rozpoznávanie nežiaducich vzorov správania. Detekciu dopĺňa systémovými a používateľsky definovanými pravidlami nad tokmi, objemami dát, zariadeniami, službami a komunikačnými vektormi.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Repetitívna analýza vyhodnocuje opakujúce sa správanie každého monitorovaného hosta a jeho služieb nad historickými, indexovanými dátami. Riešenie umožňuje retenciu dát v rozsahu mesiacov až rokov, čím výrazne prekračuje požadované obdobie 6 hodín.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Mendel umožňuje definovať a kontrolovať povolené komunikačné matice a vektory medzi zariadeniami, podsieťami a službami vrátane protokolu, frekvencie komunikácie, prenášaných príkazov a hodnôt. Porušenie definovanej politiky generuje bezpečnostnú udalosť.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf* • *Repetitívna behaviorálna analýza GREYCORTEX Mendel rozlišuje nepredvídateľné vzory ľudského správania od pravidelného strojového správania. Analýza prebieha nad dlhodobými historickými dátami a umožňuje identifikovať RAT, C&C, APT a ďalšiu automatizovanú škodlivú komunikáciu.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf* • *Mendel vykonáva NPM/APM analýzu sieťových a aplikačných výkonnostných metrík vrátane Round-Trip Time (RTT), Application Response Time (ART), User Experience Time, latencie, jitteru a retransmisií. Odchýlky od štandardného výkonu deteguje pomocou pravidiel aj automatických behaviorálnych modelov.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	

	automaticky a pravidelne aktualizovaných detekčných signatúr známych hrozieb typu Snort. Nástroj musí obsahovať ;. • metóda detekcie počítačových útokov musí byť realizovaná na základe sieťovej behaviorálnej analýzy cielenej na rozpoznanie strojového a ľudského správania v dlhodobých časových intervaloch. • analýza plného obsahu komunikácie musí byť realizovaná pomocou DPI (Deep Packet Inspection), pričom sa nejedná o analýzy len zaznamenaných metadát komunikácie.	• *GREYCORTEX Mendel vykonáva signatúrnu IDS detekciu pomocou automaticky a pravidelne aktualizovaných pravidiel typu Snort/Suricata, ktoré zahŕňajú signatúry Proofpoint Emerging Threats a vlastné pravidlá GREYCORTEX. Databáza obsahuje viac ako 85 000 detekčných pravidiel, pričom ponúkaná konfigurácia bude obsahovať minimálne 3 000 aktívnych signatúr.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *GREYCORTEX Mendel analyzuje dlhodobé komunikačné vzory a rozlišuje pravidelné strojové správanie od nepredvídateľného ľudského správania. Týmto spôsobom deteguje automatizovanú komunikáciu malvéru, botov, RAT, C&C a APT.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf* • *GREYCORTEX Mendel vykonáva Deep Packet Inspection nad paketmi monitorovanej komunikácie až po aplikačnú vrstvu. Analyzuje obsah a protokolové polia komunikácie, IDS signatúry a aplikačné dáta; nejde teda iba o analýzu zaznamenaných tokových metadát. Pre podporované ICS/SCADA protokoly umožňuje analýzu úplného protokolového obsahu.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf*	
Prevádzka online/offline	• riešenie musí umožňovať prevádzku s prístupom na Internet aj bez priameho prístupu na Internet. • aktualizácie softvéru, detekčných signatúr, reputačných databáz a ďalších	***Spĺňa.*** • *GREYCORTEX Mendel podporuje plne lokálne on-premise nasadenie a jeho monitorovacie, detekčné, analytické, forenzné a manažmentové funkcie nevyžadujú priamy prístup na Internet. Internetové pripojenie je voliteľné a môže sa využívať na automatizované aktualizácie alebo externé integrácie.*	**SPLNIL**

	dátových zdrojov musia byť možné aj riadeným offline alebo nepriamym spôsobom.	https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf • *GREYCORTEX Mendel umožňuje online aj offline aktualizáciu systému a pripojených senzorov. V izolovanom prostredí je možné aktualizácie softvéru, IDS signatúr, reputačných databáz a súvisiacich dátových zdrojov aplikovať riadeným spôsobom prostredníctvom offline aktualizačných balíkov bez priameho internetového pripojenia monitorovacieho zariadenia.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	
Spracovanie sieťových dát	• riešenie musí vykonávať analýzu kópie dátovej prevádzky prijatej na monitorovacích rozhraniach. • musí vytvárať štatistické a bezpečnostné záznamy o hostoch, službách, podsieťach, tokoch, protokoloch a komunikujúcich entitách v monitorovanej sieti.	***Spĺňa.*** • *GREYCORTEX Mendel pasívne prijíma a analyzuje kópiu dátovej prevádzky privádzanú na monitorovacie rozhrania zo SPAN/mirror portov, TAP zariadení, RSPAN, ERSPAN alebo iného podporovaného zdroja zrkadlenej prevádzky.* • *Mendel vytvára, obohacuje, indexuje a uchováva štatistické a bezpečnostné záznamy o hostoch, službách, podsieťach, obojsmerných tokoch, aplikačných protokoloch a komunikujúcich entitách. Záznamy ASNM obsahujú kontextové a výkonnostné metadáta využiteľné na detekciu, vizualizáciu a forenznú analýzu.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	**SPLNIL**
Sieťové toky a metadáta	• sieťové toky musia byť prezentované ako obojsmerná komunikácia v rámci jedného záznamu. • záznam toku musí obsahovať minimálne zdrojovú a cieľovú IP adresu, MAC adresu, porty, protokol, počet paketov, objem prenesených dát, identifikovaný aplikačný protokol a dostupné aplikačné metadáta.	***Spĺňa.*** • *GREYCORTEX Mendel zaznamenáva sieťový tok obojsmerne, pričom požiadavka aj odpoveď medzi komunikujúcimi entitami sú zlúčené a prezentované v rámci jedného záznamu toku.* • *Záznam toku obsahuje minimálne zdrojovú a cieľovú IP a MAC adresu, zdrojový a cieľový port, transportný protokol, počet paketov, objem prenesených dát a identifikovaný aplikačný protokol. Prostredníctvom DPI je záznam doplnený o dostupné aplikačné metadáta protokolov, napríklad DNS, DHCP, HTTP/S, TLS, SMB, SMTP, FTP, SSH, SNMP, LDAP, NFS, MS SQL a ďalších IT a OT protokolov.*	**SPLNIL**

		https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	
Aplikačné metadáta	• riešenie musí ukladať a analyzovať aplikačné metadáta minimálne pre DNS, HTTP a HTTPS/TLS. • pri HTTP musí byť dostupná minimálne URL požiadavka a návratový kód odpovede, pri DNS plné znenie požiadavky a odpovede a pri TLS informácie o použitých certifikátoch alebo parametroch spojenia. • musí existovať možnosť obmedziť alebo vypnúť ukladanie vybraných metadát.	***Spĺňa.*** • *GREYCORTEX Mendel pomocou DPI extrahuje, ukladá, indexuje a analyzuje aplikačné metadáta protokolov DNS, HTTP a HTTPS/TLS. Metadáta sú prehľadávateľné a priradené ku konkrétnym hostom a sieťovým tokom.* *https://www.greycortex.com/sites/default/files/perm/document/mendel-4.6-features-list-en.pdf* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Pre HTTP Mendel zaznamenáva URL požiadavky, metódu a návratový kód odpovede. Pre DNS uchováva úplné údaje o požiadavke a odpovedi vrátane názvu, typu a vrátenej hodnoty. Pre TLS spracúva parametre spojenia, napríklad verziu TLS, SNI, použitú šifrovaciu sadu a informácie o certifikáte vrátane jeho platnosti.* *https://www.greycortex.com/blog/validating-internal-network-policies-access-control-and-encryption* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Konfigurácia senzora umožňuje obmedziť alebo vypnúť spracovanie a ukladanie vybraných aplikačných metadát, protokolov alebo typov prevádzky. Zároveň je možné nastaviť rozsah hĺbkovej analýzy a pravidlá záznamu dát podľa požiadaviek na ochranu údajov a kapacitu úložiska.* *https://www.greycortex.com/sites/default/files/perm/document/mendel-4.6-features-list-en.pdf*	**SPLNIL**
PCAP a forenzná analýza	• riešenie musí podporovať ukladanie plného záznamu vybranej sieťovej komunikácie vo formáte PCAP podľa používateľom definovaných filtrov alebo pravidiel.	***Spĺňa.*** • *GREYCORTEX Mendel podporuje úplný paketový záznam vybranej sieťovej komunikácie vo formáte PCAP. Používateľ môže definovať podmienky záznamu podľa bezpečnostnej udalosti, zdrojovej alebo cieľovej IP/MAC adresy, podsiete, protokolu, portu a ďalších parametrov.*	**SPLNIL**

	• musí umožniť spätné dohľadanie sieťových tokov súvisiacich s bezpečnostnou udalosťou a ich použitie na forenznú analýzu.	https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Mendel uchováva a indexuje historické obojsmerné sieťové toky a prepája ich s detegovanými bezpečnostnými udalosťami. Analytik môže z udalosti prejsť na súvisiace toky a paketové záznamy, filtrovať ich, spätne ich prehrať a použiť pri forenznom vyšetrovaní.* https://www.greycortex.com/greycortex-mendel-4-6 https://www.greycortex.com/sites/default/files/perm/document/mendel-4.6-features-list-en.pdf	
Vyhľadávanie a filtrovanie	• riešenie musí poskytovať jednotné vyhľadávanie a filtrovanie naprieč sieťovými dátami, bezpečnostnými udalosťami, incidentmi a prehľadovými pohľadmi. • filtrovanie musí byť možné podľa ľubovoľných dostupných parametrov toku alebo udalosti, vrátane ich kombinácií. • musí byť podporené ukladanie a zdieľanie používateľských filtrov.	***Spĺňa.*** • *GREYCORTEX Mendel poskytuje jednotný hlavný filter a vyhľadávanie naprieč historickými a aktuálnymi sieťovými dátami, bezpečnostnými udalosťami, incidentmi, hostmi, službami a analytickými pohľadmi.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Pokročilý filter umožňuje filtrovanie podľa dostupných atribútov a metrík sieťových tokov alebo udalostí. Podporuje kombinovanie viacerých podmienok pomocou logických operátorov a tvorbu komplexných používateľských dopytov.* https://www.greycortex.com/greycortex-mendel-4-1 • *Používateľské filtre je možné uložiť ako vlastné analytické pohľady, opakovane používať, sprístupniť prostredníctvom zdieľaného odkazu a importovať alebo exportovať medzi jednotlivými inštanciami GREYCORTEX Mendel.* https://www.greycortex.com/greycortex-mendel-3-9 https://www.greycortex.com/sites/default/files/perm/document/mendel-4.5-features-list-en.pdf	**SPLNIL**
Vizualizácia siete	• riešenie musí poskytovať grafickú vizualizáciu komunikácie hostov, služieb a podsietí.	***Spĺňa.*** • *GREYCORTEX Mendel poskytuje grafickú vizualizáciu sieťovej topológie a komunikačných vzťahov medzi hostmi, službami a podsieťami. Pohľady je možné interaktívne filtrovať podľa podsiete, protokolu, smeru toku, zariadenia a časového obdobia.*	**SPLNIL**

	• musí umožniť zobrazenie komunikačných partnerov, objemu dát, počtu paketov, počtu tokov a výkonnostných metrík ako RTT a ART, s možnosťou triedenia podľa vybraných hodnôt.	https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf • *Mendel zobrazuje komunikačných partnerov vrátane objemu prenesených dát, počtu paketov, počtu tokov a výkonnostných metrík RTT a ART. Údaje sú dostupné v interaktívnych grafoch a tabuľkách s možnosťou filtrovania a triedenia podľa vybraných hodnôt.* https://www.greycortex.com/solutions/operational-monitoring https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	
Identifikácia aktív	• riešenie musí automaticky priraďovať IP adresám názvy zariadení na základe dostupných DNS a DHCP informácií. • pre externé IP adresy musí poskytovať geolokačné a reputačné informácie podľa databáz platných v čase zaznamenania komunikácie.	***Spĺňa.*** • *GREYCORTEX Mendel automaticky získava a koreluje názvy zariadení s IP adresami z dostupných DNS a DHCP záznamov. Zmeny názvov priebežne časovo označuje a uchováva v histórii identity zariadenia.* https://www.greycortex.com/sites/default/files/perm/document/mendel-4.6-features-list-en.pdf • *Mendel obohacuje externé IP adresy o geolokačné, reputačné a vlastnícke informácie z databáz IP reputation, doménovej reputácie, GEO IP, WHOIS a ďalších zdrojov Threat Intelligence. Informácie sa priraďujú pri spracovaní komunikácie a uchovávajú sa s historickým záznamom toku, čím zostáva zachovaný kontext platný v čase zaznamenania komunikácie.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	**SPLNIL**
DPI a detekčné signatúry	• detekcia minimálne nasledujúcich typov skenovania portov: TCP, SYN, FIN, NULL • detekcia hádania hesiel pre minimálne nasledujúce protokoly: TELNET, HTTP, SSH,	***Spĺňa.*** • *GREYCORTEX Mendel deteguje skenovanie portov pomocou behaviorálnej analýzy sieťových tokov a IDS signatúr, vrátane TCP Connect, TCP SYN, TCP FIN a TCP NULL skenovania.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	**SPLNIL**

	RDP, FTP, SMTP, IMAP, POP3, SMB, SMB2 • musí obsahovať detekciu známych (vyskytujúcich sa v signatúrach nástroje) hrozieb a škodlivého kódu (malware). • musí obsahovať detekciu DoS útokov. • musí umožňovať meranie výkonnosti všetkých aplikácií vyskytujúcich sa v monitorovanej sieti, ktoré používajú TCP, minimálne podľa RTT (Round Trip Time) a ART (Application Response Time). • musí podporovať grafickú vizualizáciu pre jednotlivé hosty v sieti a všetky služby obsiahnuté v monitorovanej sieti. • riešenie musí vykonávať Deep Packet Inspection nad monitorovanou prevádzkou a používať pravidelne aktualizované detekčné signatúry pre známe hrozby, malware, útoky, porušenia politík a podozrivé aktivity. • musí umožniť použitie alebo tvorbu vlastných detekčných pravidiel ekvivalentných pravidlám typu IDS/Snort/Suricata.	• *Mendel deteguje slovníkové a brute-force útoky pomocou analýzy opakovaných spojení, neúspešných autentizácií a IDS signatúr pre protokoly TELNET, HTTP, SSH, RDP, FTP, SMTP, IMAP, POP3, SMB a SMB2.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf* • *GREYCORTEX Mendel používa IDS signatúry Proofpoint Emerging Threats a vlastné pravidlá GREYCORTEX na detekciu známych útokov, exploitov, škodlivých súborov, malvéru, ransomvéru, trójskych koní, botnetov a C&C komunikácie.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Mendel deteguje DoS a DDoS útoky prostredníctvom volumetrickej behaviorálnej analýzy, vyhodnocovania anomálneho množstva paketov a tokov a signatúrnej detekcie. Súčasťou riešenia je aj ochranný režim pre vysoký počet tokov spôsobený DDoS útokmi a skenovaním.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* *https://www.greycortex.com/greycortex-mendel-4-5* • *GREYCORTEX Mendel zabezpečuje monitorovanie výkonnosti sieťovej a aplikačnej komunikácie používajúcej TCP. Pre jednotlivé spojenia a aplikácie vypočítava minimálne Round-Trip Time (RTT) a Application Response Time (ART), ako aj latenciu, jitter, retransmisie a User Experience Time.* *https://www.greycortex.com/solutions/operational-monitoring* • *Mendel poskytuje grafickú vizualizáciu jednotlivých hostov, ich služieb, komunikačných partnerov, podsietí a vzájomných komunikačných väzieb. Pohľady umožňujú interaktívne filtrovanie a zobrazenie detailov konkrétneho hosta alebo služby.* *https://www.greycortex.com/solutions/operational-monitoring* • *GREYCORTEX Mendel vykonáva Deep Packet Inspection nad paketmi monitorovanej prevádzky a využíva pravidelne aktualizované IDS*	

		signatúry Proofpoint Emerging Threats a GREYCORTEX. Signatúry pokrývajú známe hrozby, malvér, exploity, útoky, porušenia politík a ďalšie podozrivé aktivity. *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Mendel umožňuje importovať, upravovať a vytvárať vlastné IDS pravidlá ekvivalentné pravidlám typu Snort/Suricata. Integrovaný IDS Rule Wizard umožňuje vytvárať pravidlá prostredníctvom grafického sprievodcu vrátane kontroly syntaxe.* *https://www.greycortex.com/greycortex-mendel-4-2* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	
Behaviorálna a anomálna detekcia	• riešenie musí detegovať anomálie porovnaním aktuálneho správania so správaním z historického obdobia. • detekcia musí byť možná minimálne na úrovni hostov, služieb a podsietí. • riešenie musí podporovať modelovanie koncových zariadení, komunikačných vzorov, komunikačných matíc a odchýlok od bežného správania.	***Spĺňa.*** • *GREYCORTEX Mendel vytvára adaptívne behaviorálne modely z historickej sieťovej prevádzky a porovnáva s nimi aktuálne správanie. Odchýlky od predikovaného správania automaticky vyhodnocuje ako anomálie, pričom modely pravidelne aktualizuje podľa zmien v sieti.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf* • *Behaviorálne modelovanie a detekcia anomálií sa vykonávajú samostatne pre jednotlivé monitorované hosty, služby prevádzkované na hostoch a jednotlivé podsiete.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf* • *Mendel modeluje správanie koncových zariadení, ich služby, komunikačných partnerov, porty, objemy dát, frekvenciu a smer komunikácie. Umožňuje definovať komunikačné matice a povolené komunikačné vektory a detegovať nové, zmenené alebo nepovolené komunikačné vzory a ďalšie odchýlky od bežného správania.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf*	**SPLNIL**

Detekčné schopnosti – bezpečnostné udalosti	musí umožňovať detegovať minimálne port scanning, brute-force/hádanie hesiel, malware komunikáciu, komunikáciu s nízkou reputáciou, botnet/C2 komunikáciu, DoS prejavy, P2P/TOR alebo obdobnú anonymizačnú komunikáciu, tunelovanie protokolov, použitie štandardných protokolov na neštandardných portoch a anomálie protokolov DNS, DHCP, HTTP, SMTP a SMB.	**Spĺňa.** *GREYCORTEX Mendel kombináciou DPI, IDS signatúr, behaviorálnej analýzy, tokovej analýzy a Threat Intelligence deteguje:* • *skenovanie portov a brute-force/hádanie hesiel,* • *malvérovú, botnetovú a C2/C&C komunikáciu,* • *komunikáciu s IP adresami alebo doménami s nízkou reputáciou,* • *prejavy DoS a DDoS útokov,* • *P2P, TOR a obdobnú anonymizačnú komunikáciu,* • *tunelovanie komunikácie prostredníctvom DNS, HTTP/S, SSH, ICMP a ďalších protokolov,* • *použitie rozpoznaných aplikačných protokolov na neštandardných portoch,* • *protokolové a behaviorálne anomálie komunikácie DNS, DHCP, HTTP, SMTP, SMB a SMB2.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	**SPLNIL**
Detekčné schopnosti – sieťové udalosti	musí umožňovať detegovať minimálne MAC spoofing, IP spoofing, duplicitu alebo zmenu IP adresy, duplicitu alebo zmenu MAC adresy, neočakávaný objem prenesených dát, neočakávaný počet spojení, vznik nových služieb, zmenu komunikačných vektorov a nedostupnosť vybraných zariadení alebo služieb.	***Spĺňa.*** *GREYCORTEX Mendel kombináciou sledovania L2/L3 komunikácie, behaviorálnych modelov a používateľských politík deteguje:* • *MAC a IP spoofing vrátane nezrovnalostí medzi IP, MAC a ARP údajmi,* • *duplicitu, objavenie, zmiznutie alebo zmenu IP a MAC adresy,* • *neočakávaný objem prenesených dát a počet spojení alebo tokov,* • *vznik novej služby alebo zariadenia,* • *nové, zmenené alebo nepovolené komunikačné vektory,* • *ukončenie komunikácie a nedostupnosť sledovaných zariadení alebo služieb.* *https://www.greycortex.com/blog/validating-internal-network-policies-mendel* *https://www.greycortex.com/solutions/operational-monitoring*	**SPLNIL**

		https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf	
Výkonnostné metriky	• riešenie musí merať výkonnosť aplikácií používajúcich TCP minimálne prostredníctvom metrík RTT (Round Trip Time) a ART (Application Response Time). • výkonnostné metriky musia byť dostupné vo vizualizáciách, filtroch a reportoch.	***Spĺňa.*** • *GREYCORTEX Mendel monitoruje výkonnosť sieťovej a aplikačnej komunikácie používajúcej TCP a vypočítava minimálne metriky Round-Trip Time (RTT) a Application Response Time (ART). Ďalej poskytuje napríklad User Experience Time, latenciu, jitter a retransmisie.* https://www.greycortex.com/solutions/operational-monitoring • *Výkonnostné metriky sú dostupné v interaktívnych grafoch, tabuľkách a používateľských dashboardoch. Možno ich použiť vo filtroch, porovnávať s definovanými hodnotami, vyhodnocovať ich anomálie a zahrnúť ich do generovaných reportov a upozornení.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf https://www.greycortex.com/solutions/operational-monitoring	**SPLNIL**
TLS/SSL inšpekcia	• riešenie musí umožniť dešifrovanie vybranej TLS/SSL komunikácie v prípade, že obstarávateľ poskytne príslušný privátny kľúč alebo certifikát a takýto postup je v súlade s internými bezpečnostnými a právnymi pravidlami. • po dešifrovaní musí byť možné vykonať plnohodnotnú bezpečnostnú analýzu obsahu.	***Spĺňa.*** • *GREYCORTEX Mendel umožňuje dešifrovanie vybranej podporovanej TLS/SSL komunikácie po poskytnutí príslušného privátneho alebo iného dešifrovacieho kľúča, prípadne certifikátu s dostupným privátnym kľúčom. Funkciu možno aplikovať selektívne v súlade s bezpečnostnými a právnymi pravidlami verejného obstarávateľa.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Po dešifrovaní Mendel vykonáva nad obsahom plnohodnotnú DPI a IDS analýzu vrátane identifikácie aplikačného protokolu, extrakcie aplikačných metadát, vyhodnotenia detekčných signatúr a detekcie škodlivého alebo podozrivého obsahu.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	**SPLNIL**
Incidenty a väzba na dôkazy	• pre každú identifikovanú bezpečnostnú udalosť musí riešenie poskytnúť odkaz na konkrétny sieťový tok alebo	***Spĺňa.*** • *Detail každej bezpečnostnej udalosti v GREYCORTEX Mendel obsahuje priamu väzbu na konkrétny sieťový tok alebo skupinu tokov, ktoré udalosť*	**SPLNIL**

	skupinu tokov, ktoré udalosť vyvolali. • incident musí obsahovať dostatok informácií na validáciu udalosti, triedenie, priradenie stavu a eskaláciu.	*vyvolali. Z udalosti možno prejsť na detail komunikácie, súvisiace aplikačné metadáta a dostupný PCAP záznam.* *https://www.greycortex.com/greycortex-mendel-4-6* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Incident obsahuje popis, závažnosť, kategorizáciu, časový priebeh, súvisiace udalosti a sieťové dôkazy. Podporované je pridávanie komentárov a štítkov, zmena stavu, priradenie sledovateľov, validácia falošne pozitívnych udalostí a export incidentného reportu, čo umožňuje triedenie, riadenie životného cyklu a eskaláciu incidentu.* *https://www.greycortex.com/greycortex-mendel-3-6* *https://www.greycortex.com/blog/greycortex-mendel-361-now-available*	
Zdroje reputácie a threat intelligence	musí obsahovať automaticky aktualizované zdroje reputácie a threat intelligence, minimálne databázy škodlivých domén, IP adries s nízkou reputáciou, botnet/C2 infraštruktúry, malware indikátorov a ďalších relevantných indikátorov kompromitácie.	***Spĺňa.*** *GREYCORTEX Mendel obsahuje automaticky a pravidelne aktualizované viaczdrojové Threat Intelligence a reputačné databázy zahŕňajúce:* • *škodlivé domény a URL,* • *IP adresy s nízkou reputáciou,* • *botnetovú a C2/C&C infraštruktúru,* • *indikátory malvéru a škodlivé súborové hashe,* • *zdroje spamu, TOR uzly, proxy servery a ďalšie indikátory kompromitácie.* *Súčasťou sú zdroje GREYCORTEX, Proofpoint Emerging Threats a ďalšie verejné a komerčné databázy. Riešenie podporuje aj integráciu vlastných Threat Intelligence zdrojov vrátane platformy MISP.* *https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* *https://www.greycortex.com/blog/review-greycortex-mendel*	**SPLNIL**
Administrácia	• musí umožňovať základnú administráciu zariadenia cez zabezpečené riadkové rozhranie s využitím SSHv2 a pokročilú administráciu cez jednotné webové grafické rozhranie.	***Spĺňa.*** • *GREYCORTEX Mendel umožňuje základnú systémovú administráciu virtuálneho zariadenia prostredníctvom zabezpečeného riadkového rozhrania mShell dostupného cez SSHv2. Pokročilá konfigurácia, správa senzorov a kolektora, analýza dát, detekcia a reporting sa vykonávajú cez jednotné zabezpečené webové grafické rozhranie.*	**SPLNIL**

	• musí podporovať správu používateľov, rolí, oprávnení a audit aktivít používateľov.	https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Mendel podporuje lokálnu aj centralizovanú správu používateľov, granulárne riadenie oprávnení podľa rolí, integráciu s externými poskytovateľmi identity, SSO a MFA. Aktivity používateľov a administratívne zmeny sa zaznamenávajú, dajú sa filtrovať a exportovať na účely auditu.* https://www.greycortex.com/greycortex-mendel-4-5 https://www.greycortex.com/greycortex-mendel-4-2	
Autentizácia a oprávnenia	• musí podporovať autentizáciu používateľov voči lokálnej databáze a externému adresáru typu LDAP alebo Microsoft Active Directory. • musí umožniť prideľovanie oprávnení minimálne v úrovniach read-only, read-write a bez prístupu pre vybrané administračné oblasti, detekčné metódy alebo rozsahy IP/MAC adries.	***Spĺňa.*** • *GREYCORTEX Mendel podporuje autentizáciu používateľov voči lokálnej databáze účtov aj externým adresárovým a autentizačným službám vrátane LDAP a Microsoft Active Directory. Podporované sú tiež SSO a MFA prostredníctvom externého poskytovateľa identity.* https://www.greycortex.com/greycortex-mendel-4-5 • *Role-Based Access Control v GREYCORTEX Mendel umožňuje pre jednotlivé administračné a analytické oblasti nastaviť oprávnenia na čítanie, čítanie a zápis alebo úplné odobratie prístupu. Oprávnenia možno obmedziť podľa modulov, detekčných metód a sieťového rozsahu vrátane vybraných podsietí, hostov a rozsahov IP/MAC adries.* https://www.greycortex.com/sites/default/files/perm/document/mendel-4.5-features-list-en.pdf https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf	**SPLNIL**
Reporting a exporty	• musí obsahovať integrovaný reporting ako súčasť produktu. • musí umožňovať tvorbu preddefinovaných aj používateľsky definovaných reportov, export minimálne do PDF a DOCX, rozosielanie reportov elektronickou poštou a použitie slovenského alebo	***Spĺňa.*** • *GREYCORTEX Mendel obsahuje integrovaný reportovací modul ako súčasť produktu. Podporuje bezpečnostné, manažérske, incidentné a podmienkou spúšťané reporty nad údajmi uloženými priamo v riešení.* https://www.greycortex.com/greycortex-mendel-4-2 • *Mendel umožňuje vytvárať preddefinované aj používateľsky prispôsobené reporty, exportovať ich minimálne do formátov PDF a DOCX a automatizovane ich rozosielať elektronickou poštou. Reporty je možné generovať v anglickom jazyku.*	**SPLNIL**

	anglického jazyka reportov.	https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-data-sheet-cz-2022_2.pdf	
Integrácie a logovanie	• musí podporovať odosielanie udalostí minimálne vo formáte syslog s konfigurovateľnou štruktúrou záznamu. • Syslog správa musí vedieť obsahovať odkaz do centrálnej konzoly na príslušnú udalosť alebo incident.	***Spĺňa.*** • *GREYCORTEX Mendel podporuje odosielanie bezpečnostných a prevádzkových udalostí cez Syslog vrátane formátov CEF a LEEF. Štruktúru exportovaného záznamu, prenášané atribúty, filtre udalostí a spôsob odosielania je možné konfigurovať.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Exportovaná Syslog správa môže obsahovať priamy URL odkaz do webovej konzoly GREYCORTEX Mendel na detail príslušnej udalosti alebo incidentu, čo umožňuje okamžitý prechod z externého SIEM systému na súvisiace sieťové dôkazy.* https://www.greycortex.com/sites/default/files/perm/document/greycortex-mendel-in-ot-en_0.pdf	**SPLNIL**
Ukladanie a retencia dát	• musí umožniť konfiguráciu retencie ukladaných dát a automatické mazanie dát po uplynutí nastavenej doby. • musí podporovať zálohovanie alebo export dát na externé úložisko dostupné minimálne cez protokol CIFS/SMB alebo ekvivalentný bezpečný protokol.	***Spĺňa.*** • *GREYCORTEX Mendel umožňuje nastaviť retenciu ukladaných sieťových tokov, udalostí, metadát a PCAP záznamov. Po dosiahnutí nastavenej doby alebo kapacitného limitu sa najstaršie dáta automaticky odstraňujú prostredníctvom riadenej rotácie FIFO.* https://www.greycortex.com/greycortex-mendel-4-3 https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf • *Mendel podporuje zálohovanie dát a konfigurácie na externé sieťové úložisko cez protokol SMB/CIFS. Podporované sú aj alternatívne úložiská, napríklad Hitachi HCP, AWS S3, lokálne pripojené USB úložisko alebo sieťovo pripojené úložisko.* https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf https://www.greycortex.com/blog/greycortex-mendel-36-now-available	**SPLNIL**

Licencie a aktualizácie	• licencie musia pokrývať používanie NDR (senzor, collector) - monitorovaná lokalita pre neobmedzený alebo dostatočne dimenzovaný počet používateľov podľa potrieb verejného obstarávateľa. • súčasťou licencie musia byť aktualizácie softvéru, detekčných signatúr, filtrov, reputačných databáz a ďalších dátových zdrojov minimálne na 24 mesiacov.	***Spĺňa.*** • *Požiadavka je splnená. Licencie pokrývajú 4× virtuálne zariadenie GREYCORTEX Mendel All-in-One Sensor + Collector pre monitorované lokality, koreláciu a jednotný prehľad udalostí. Je kapacitne dimenzovaný na všetky štyri lokality a podporuje požadovaný počet používateľov s granulárnym riadením rolí a oprávnení https://www.greycortex.com/blog/greycortex-mendel-35-now-available https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf* • *Ponúkaná konfigurácia obsahuje pre štyri základné licencie 8 ročných jednotiek podpory MA-SC-4k-MS1Y a pre štyri ICS/SCADA rozšírenia 8 ročných jednotiek podpory ME-ICS-SC-50-MS1Y, čo predstavuje 24 mesiacov podpory a aktualizácií na každú licenciu. Podpora zahŕňa aktualizácie softvéru, detekčných signatúr, filtrov, reputačných databáz a ďalších dátových zdrojov. https://www.greycortex.com/sites/default/files/perm/document/greycortex_datasheet_2025_cz_0.pdf*	**SPLNIL**
Podpora výrobcu/dodávateľa	• súčasťou dodávky musí byť technická podpora minimálne na 24 mesiacov v režime najmenej 8x5xNBD alebo ekvivalentnom. Podpora musí zahŕňať riešenie incidentov produktu, aktualizácie, prístup k dokumentácii a eskaláciu na výrobcu alebo výrobcom autorizovanú podporu.	***Spĺňa.*** *Súčasťou dodávky je technická podpora GREYCORTEX Mendel na obdobie 24 mesiacov v režime minimálne 8×5×NBD alebo ekvivalentnom. Podpora zahŕňa evidenciu, diagnostiku a riešenie incidentov produktu, poskytovanie softvérových a bezpečnostných aktualizácií, prístup k technickej a používateľskej dokumentácii a eskaláciu závažných prípadov na výrobcu GREYCORTEX. https://www.greycortex.com/sites/default/files/perm/document/mendel-4.6-features-list-en.pdf*	**SPLNIL**

2.2 Firewall - monitorovaná lokalita

Firewall - monitorovaná lokalita			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné moduly, ktorými preukazuje splnenie požiadaviek pre Firewall - monitorovaná lokalita.	***Výrobca/model:*** *Check Point Software Technologies Ltd. – 4 ks Check Point Spark Firewall 1900 Base Appliance, SKU CPAP-SG1900-SNBT.* ***Edícia/verzia:*** *Base Appliance, operačný systém Gaia Embedded R81.10.X, centrálne spravovaný.* ***Licenčný model:*** *hardvérová appliance s ročným predplatným SandBlast (SNBT), rozšírením Next Generation Threat Prevention o ďalší 1 rok (CPSB-NGTP-1900-1Y) a licenciou SD-WAN na 2 roky (CPSB-SDWAN-1900-2Y).* ***Relevantné moduly:*** *Next Generation Firewall, IPS, Anti-Virus, Anti-Bot, Application Control, URL Filtering, Site-to-Site a Remote Access VPN, SandBlast Threat Emulation/Threat Extraction, SD-WAN, centrálne monitorovanie, správa politík a záznam bezpečnostných udalostí.* *https://www.checkpoint.com/compare/products/* *https://sc1.checkpoint.com/documents/Appliances/GSG_V4/EN/Content/Topics-V4/Appliance.htm* *konfigurácia pre 4 zariadenia Check Point Quantum Spark 1900:* • *4x PAP-SG1900-SNBT* • *4x CPSB-SDWAN-1900-2Y* • *4x CPSB-NGTP-1900-1Y* • *8x CPAC-TR-1SX-D, teda 2× 1 Gb SX na zariadenie* • *8x CPAC-TR-10SR-D, teda 2× 10 Gb SR na zariadenie* • *4x CPCES-CO-PREMIUM-1900-ADD*	**SPLNIL**
Počet:	4 ks (1ks určený pre monitorovanú lokalitu) Dodané zariadenie musí byť vo forme fyzických zariadení s výnimkou manažmentu riešenia, ktoré musí byť vo forme virtuálneho zariadenia pre virtualizačnú platformu.	***Spĺňa.*** *Dodané budú 4 ks fyzických zariadení Check Point Spark Firewall 1900 Base Appliance (CPAP-SG1900-SNBT), pričom 1 ks je určený pre monitorovanú lokalitu. Centrálny manažment Check Point Security Management Server Premium pre 25 brán (CPSM-NGM25-PREMIUM) bude nasadený ako virtuálne*	**SPLNIL**

			zariadenie na virtualizačnej platforme; samostatná fyzická manažment appliance sa nevyžaduje. *https://sc1.checkpoint.com/documents/Appliances/GSG_V4/EN/Content/Topics-V4/Appliance.htm* *https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/Content/Topics-RN/HW-Requirements-Open-Server-VM.htm*	
Výkon:	Priepustnosť Firewallu podľa RFC 3511, 2544, 2647, 1242	Min. 32 Gb/s	***Spĺňa.*** *Check Point Spark Firewall 1900 dosahuje priepustnosť firewallu 32 Gb/s pri 1518-bajtových UDP paketoch, meranú v laboratórnych podmienkach podľa RFC 3511, RFC 2544, RFC 2647 a RFC 1242.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Priepustnosť IPS	Min. 9 Gb/s	***Spĺňa.*** *Ponúkané zariadenie Check Point Spark Firewall 1900 poskytuje priepustnosť IPS 9 Gb/s.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Priepustnosť so zapnutou ochranou pred hrozbami (threat protection – antimalware, IPS, application control)	Min. 4 Gb/s	***Spĺňa.*** *Check Point Spark Firewall 1900 dosahuje priepustnosť Threat Prevention 4 Gb/s pri súčasne aktivovaných funkciách Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot a SandBlast Zero-Day Protection so zapnutým logovaním.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Priepustnosť IPsec VPN (512 bytes)	Min. 5 Gb/s	***Spĺňa.*** *Check Point Spark Firewall 1900 má deklarovanú priepustnosť IPsec VPN 5 Gb/s.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Počet nových spojení za sekundu (CPS)	Min. 90 000	***Spĺňa.*** *Check Point Spark Firewall 1900 podporuje vytvorenie 90 000 nových spojení za sekundu (CPS).*	**SPLNIL**

			https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf	
	Počet súčasných spojení	Min. 4 000 000	***Spĺňa.*** *Check Point Spark Firewall 1900 podporuje až 4 200 000 súčasných spojení, čím prekračuje požadovanú minimálnu hodnotu 4 000 000 spojení.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Počet fyzických sieťových rozhraní	16x 1 GbE RJ-45 2x 2.5GbE Base-T RJ-45 4x10GbE SFP+ ports vrátane 2x short range tranceiverov	***Spĺňa.*** *Každé zariadenie Check Point Spark Firewall 1900 obsahuje:* • *16× 1GbE Base-T RJ-45,* • *2× 2,5GbE Base-T RJ-45,* • *4× 10GbE SFP+.* *Súčasťou ponúkanej konfigurácie je celkovo 8 ks 10GBASE-SR SFP+ transceiverov CPAC-TR-10SR-D, teda 2 ks short-range transceiverov pre každé zo štyroch zariadení.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Podpora pre lokálne úložisko	min. 512 GB SSD	***Spĺňa.*** *Check Point Spark Firewall 1900 obsahuje interné lokálne úložisko s kapacitou 512 GB SSD a navyše slot na MicroSD kartu.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Podpora vysokej dostupnosti v konfigurácii Active-Passive, alebo Active-Active alebo Clustering		***Spĺňa.*** *Check Point Spark Firewall 1900 podporuje vytvorenie klastra ClusterXL High Availability v režime Active/Passive, ktorý zabezpečuje automatické prevzatie prevádzky záložným členom pri výpadku aktívneho zariadenia.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
Požadovaná funkcionalita	Funcia SDWAN spoke v rámci hub and spoke topológie SDWAN		***Spĺňa.*** *Ponúkané zariadenie Check Point Quantum Spark 1900 s licenciou CPSB-SDWAN-1900-2Y podporuje SD-WAN Overlay VPN. Zariadenie môže byť prevádzkované ako spoke/satellite gateway v Star VPN Community, ktorá*	**SPLNIL**

		predstavuje topológiu hub-and-spoke. Funkcia je podporovaná pri centrálnom manažmente zariadenia. *https://sc1.checkpoint.com/documents/Appliances/Quantum_Spark_FAQ/Content/Topics/SD-WAN.htm* *https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/DAIP.htm*	
	Podpora Site to Site IPSEC tunelov.	***Spĺňa.*** *Check Point Quantum Spark 1900 podporuje vytváranie a prevádzku šifrovaných Site-to-Site IPsec VPN tunelov vrátane zapojenia do Star a Mesh VPN komunít.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Podpora 802.1Q VLAN, podpora 802.3ad pasívnej a aktívnej agregácie liniek.	***Spĺňa.*** *Check Point Quantum Spark 1900 podporuje IEEE 802.1Q tagované VLAN s VLAN ID 1 až 4094 a agregáciu liniek prostredníctvom IEEE 802.3ad/LACP. Aktívno-pasívne zapojenie liniek je podporované režimom High Availability – Active/Backup.* *https://sc1.checkpoint.com/documents/SMB_R81.10.X/CLI/EN/Content/Topics/add-interface-vlan.htm* *https://sc1.checkpoint.com/documents/SMB_R81.10.X/CLI/EN/Content/Topics/add-interface-bond.htm*	**SPLNIL**
	Firewall, IPS, Aplikačná kontrola, AntiMalware a Botnet ochrana.	***Spĺňa.*** *Balík SNBT pre Check Point Quantum Spark 1900 zahŕňa Firewall, IPS, Application Control, URL Filtering, Antivirus/AntiMalware, Anti-Bot a SandBlast Threat Emulation. Anti-Bot zisťuje infikované zariadenia a zabraňuje ich komunikácii s C&C servermi.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
	Možnosť integrácie s externou Sandbox službou (cloud alebo on-premises).	***Spĺňa.*** *Funkcia Threat Emulation umožňuje analyzovať súbory v cloudovej sandbox službe Check Point Public ThreatCloud alebo prostredníctvom externého*	**SPLNIL**

		lokálneho privátneho SandBlast/Threat Emulation zariadenia. Podporované je aj nakonfigurovanie viacerých vzdialených emulátorov. *https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Locally_Managed/EN/Content/Topics/Advanced-Threat-Prevention-Engine-Settings.htm*	
	Musí realizovať filtrovanie tokov na základe doménovej / IP reputácie.	***Spĺňa.*** *Check Point Quantum Spark 1900 podporuje kontrolu a blokovanie komunikácie podľa reputácie domén, IP adries a URL. Reputačné údaje sa overujú voči databáze Check Point ThreatCloud a používajú sa najmä na identifikáciu C&C serverov a škodlivej komunikácie.* *https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Locally_Managed/EN/Content/Topics/Advanced-Threat-Prevention-Engine-Settings.htm*	**SPLNIL**
	Musí podporovať filtrovanie web tokov na základe DNS requestov, url filtrovanie a blokovanie na známe botnet a C&C adresy	***Spĺňa.*** *Ponúkané riešenie podporuje DNS Security na identifikáciu a blokovanie škodlivých DNS požiadaviek, C&C spojení a DNS tunelovania. Súčasťou riešenia je URL Filtering a Anti-Bot ochrana blokujúca komunikáciu so známymi botnet a C&C doménami, IP adresami a URL.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf* *https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Locally_Managed/EN/Content/Topics/Advanced-Threat-Prevention-Engine-Settings.htm*	**SPLNIL**
	Musí podporovať inšpekciu certifikátov počas SSL handshaku, bez potreby dešifrovania.	***Spĺňa.*** *Check Point Quantum Spark 1900 podporuje režim HTTPS Categorization Only, ktorý umožňuje kategorizáciu a URL filtrovanie HTTPS komunikácie na základe certifikátu servera počas TLS/SSL handshaku bez aktivovania SSL inšpekcie a bez dešifrovania obsahu komunikácie.* *https://sc1.checkpoint.com/documents/SMB_R81.10.X/CLI/EN/Content/Topics/195343.htm*	**SPLNIL**
	Musí umožňovať filtrovanie na základe geografickej lokality.	***Spĺňa.*** *Centrálne spravovaný Check Point Quantum Spark 1900 podporuje GEO Updatable Objects pre jednotlivé krajiny a kontinenty. Tieto objekty je možné*	**SPLNIL**

		použiť ako zdroj alebo cieľ pravidla na povolenie alebo zablokovanie komunikácie podľa geografickej lokality IP adresy. GEO databáza sa aktualizuje automaticky. *https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Centrally_Managed/EN/Content/Topics/Configuring-Security-Policy.htm*	
	Okamžite použiteľné preddefinované IPS politiky.	***Spĺňa.*** *Check Point Quantum Spark 1900 obsahuje okamžite použiteľné preddefinované profily Threat Prevention/IPS „Recommended“ a „Strict“. Profil Recommended je predvolený a optimalizuje pomer bezpečnosti a výkonu; profil Strict uprednostňuje maximálnu úroveň ochrany. IPS ochrany je možné automaticky aktualizovať.* *https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Locally_Managed/EN/Content/Topics/Configuring-Threat-Prevention-Blade-Control.htm*	**SPLNIL**
Napájacie zdroje	• redundantné (redundancia 1+1) • vstup: 100-240VAC, 60-50Hz	***Spĺňa.*** • *Check Point Quantum Spark 1900 obsahuje dva redundantné napájacie zdroje s výkonom 150 W v konfigurácii 1+1.* • *Podporovaný vstup je 100 – 240 V AC, 50 – 60 Hz.* *https://www.checkpoint.com/downloads/products/quantum-spark-1900-2000-datasheet.pdf*	**SPLNIL**
Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie pre preukázanie funkčnosti a prevádzkyschopnosti dodaného zariadenia Firewall - monitorovaná lokalita. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného zariadenia Firewall - monitorovaná lokalita.	• *Súčasťou ponuky je inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie pre preukázanie funkčnosti a prevádzkyschopnosti dodaného zariadenia Firewall - monitorovaná lokalita.* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného zariadenia Firewall - monitorovaná lokalita.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Check Point Certified Maestro Expert – R81 vydaný výrobcom Check Point Software Technologies LTD. pre dodávané zariadenia Firewall - monitorovaná lokalita.*	**SPLNIL**

	• uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané zariadenia Firewall - monitorovaná lokalita.		
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • podpora môže byť poskytovaná priamo výrobcom alebo prostredníctvom výrobcom autorizovaného poskytovateľa kolaboratívnej podpory, • autorizovaný poskytovateľ podpory môže byť primárnym kontaktným bodom objednávateľa, vykonávať prvotnú diagnostiku, riadiť servisný prípad a zabezpečovať jeho eskaláciu na technické centrum výrobcu, • servisný prípad musí byť možné otvoriť na základe opisu prejavov problému bez povinnosti objednávateľa vopred vykonať úplnú diagnostiku alebo určiť príčinu problému, • verejný obstarávateľ poskytne primeranú súčinnosť, najmä dostupné logy, diagnostické údaje, ak je potrebný na vyriešenie servisného prípadu, • podpora musí pokrývať dodané hardvérové a softvérové produkty	***Spĺňa***. • *Pre ponúkané riešenie je zabezpečená podpora Check Point Collaborative Enterprise Support – Standard na obdobie 2 rokov https://www.checkpoint.com/downloads/support-services/checkpoint-support-datasheet.pdf* • *Podpora je poskytovaná prostredníctvom výrobcom autorizovaného Check Point Collaborative Support Provider v súlade s programom Collaborative Enterprise Support. https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf* • *Autorizovaný poskytovateľ je primárnym kontaktným bodom objednávateľa, vykonáva prvotnú a rozšírenú diagnostiku, riadi servisný prípad a v prípade potreby ho eskaluje na technické centrum Check Point TAC. https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf* • *Servisný prípad možno otvoriť na základe opisu prejavov problému. Úplnú prvotnú diagnostiku, identifikáciu problému a základné riešenie zabezpečuje autorizovaný poskytovateľ podpory. https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf* • *Objednávateľ poskytne dostupné logy, diagnostické súbory, opis prostredia a ďalšie primerane požadované informácie potrebné na diagnostiku a riešenie servisného prípadu. https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf*	**SPLNIL**

	výrobcu, pre ktoré je zakúpený platný servisný kontrakt,
	• reakčný čas pre incident závažnosti 1 musí byť najviac 30 minút a pre incidenty závažnosti 2, 3 a 4 najviac 4 hodiny v rámci servisného času príslušného programu podpory,
	• pri poruche hardvéru musí byť zabezpečená služba Advance Hardware Replacement, pri ktorej bude náhradné zariadenie po schválení RMA odoslané v rovnaký pracovný deň s využitím komerčne primeraného úsilia výrobcu; z prevádzkových dôvodov môže byť odoslané nasledujúci pracovný deň,
	• pri podozrení na problém interoperability s produktmi VMware alebo Veeam zabezpečí poskytovateľ podpory primeranú súčinnosť pri izolácii problému a výmene diagnostických informácií; servisný prípad produktu tretej strany bude riešený podľa platného servisného kontraktu verejného obstarávateľa s príslušným výrobcom
	• koordináciu medzi autorizovaným poskytovateľom podpory a technickým centrom výrobcu zabezpečuje poskytovateľ podpory.
		• *Podpora pokrýva dodané hardvérové a softvérové produkty Check Point, ku ktorým je zakúpený a aktívny príslušný servisný kontrakt.* https://www.checkpoint.com/downloads/support-services/checkpoint-support-datasheet.pdf
		• *V rámci servisného času programu Collaborative Standard, t. j. 5 dní × 9 hodín počas pracovných dní, sú zabezpečené nasledujúce reakčné časy:*
		  ○ *závažnosť 1 – najviac 30 minút,*
		  ○ *závažnosti 2, 3 a 4 – najviac 4 hodiny.*
		https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf
		• *Požiadavka je splnená pre hardvérové produkty pokryté servisným kontraktom. Po diagnostike poruchy a schválení RMA výrobca vynaloží komerčne primerané úsilie na odoslanie náhradného hardvéru v rovnaký pracovný deň; z prevádzkových dôvodov môže byť odoslaný nasledujúci pracovný deň.*
		https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf
		• *Autorizovaný poskytovateľ zabezpečí primeranú súčinnosť pri izolácii problému a výmene diagnostických informácií. Podpora Check Point rieši časti týkajúce sa produktov Check Point; servisný prípad VMware alebo Veeam sa rieši podľa samostatného kontraktu objednávateľa s príslušným výrobcom.*
		https://www.checkpoint.com/support-services/hcl/
		https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf
		• *Autorizovaný poskytovateľ podpory zabezpečuje komunikáciu, odovzdanie diagnostických údajov, eskaláciu a koordináciu riešenia servisného prípadu s technickým centrom Check Point TAC.*
		https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf	

2.3 Server Typ 2

Server Typ 2			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Cisco Systems, Inc. – Cisco UCS C245 M8 SFF Rack Server, model UCSC-C245-M8SX, generácia M8, 4 ks.* ***Edícia/verzia a licenčný model:*** *2U vyhotovenie s 24 pozíciami SFF, prevádzka v samostatnom režime, Cisco IMC v aktuálnej odporúčanej verzii.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html* *Technická špecifikácia:* • *4x UCSC-C245-M8SX - UCS C245 M8 2U rack server with 24× SFF HDD/SSD backplane* • *4x CON-L1NBD-UCSCM8SX - CX Level 1 8x5xNBD support for UCS C245 M8* • *8x UCS-CPU-A9335 - AMD EPYC 9335 3.0GHz, 32-core, 210W processor* • *16x UCS-MRX64G2RE5 - 64GB DDR5-6400 RDIMM memory* • *20x UCS-SD16TKA3XEP-D - 1.6TB 2.5-inch enterprise performance 24G SAS SSD* • *8x UCS-M24800A1V - 480GB M.2 SATA boot SSD* • *4x UCS-M2-HWRAID-D - Cisco boot-optimized M.2 RAID controller* • *4x UCSC-RAID-MP1L32 - 24G Tri-Mode RAID controller with 4GB cache* • *4x UCSC-O-N6CD25GFO - NVIDIA ConnectX-6 Lx dual-port 25G SFP28 OCP NIC* • *4x UCSC-P-I01GC - Intel I710-T4L quad-port 1GBASE-T network adapter* • *4x UCS-TPM2-002D-D - TPM 2.0 module, FIPS 140-2 and Windows Server 2022 compliant* • *8x UCSC-PSU1-1200W-D - 1200W AC Titanium power supply*	**SPLNIL**

		• *8x CAB-C13-C14-2M - Power cord jumper with C13–C14 connectors, 2 m length* • *4x UCSC-RAIL-D - Ball-bearing rail kit for UCS C240 M8* • *4x UCSC-CMA-C240-D - Reversible cable-management arm for UCS C240* • *4x CIMC-LATEST-D - Latest Cisco IMC software for C-Series servers*	
Procesor (CPU)	• model CPU pri osadení dvomi procesormi typu x86 musí byť schopný dosiahnuť výkon minimálne 852 bodov podľa testu SPECrate®2017_int_base result a musí byť poslednej generácie daného výrobcu • celkový počet jadier jedného procesora nesmie presiahnuť 32 z dôvodu licenčných obmedzení.	***Spĺňa***. *V súlade s Vysvetlením informácií potrebných na vypracovanie ponuky zo dňa 24. 8. 2026, Odpoveďou č. 20, je každý zo 4 ponúkaných serverov Cisco UCS C245 M8 osadený dvomi procesormi x86-64:* • *výrobca a model: AMD EPYC 9335,* • *generácia: 5. generácia AMD EPYC, séria 9005,* • *Cisco PID: UCS-CPU-A9335,* • *počet procesorov v jednom serveri: 2,* • *počet fyzických jadier jedného procesora: 32,* • *celkový počet procesorov v ponúkanej konfigurácii: 8.* *Procesor AMD EPYC 9335 predstavuje najnovšiu generáciu procesorov AMD EPYC, ktorá je ku dňu uplynutia lehoty na predkladanie ponúk oficiálne podporovaná, certifikovaná a objednateľná výrobcom Cisco pre ponúkanú aktuálnu serverovú platformu Cisco UCS C245 M8. Procesor UCS-CPU-A9335 je uvedený v aktuálnom zozname procesorov podporovaných spoločnosťou Cisco pre server UCS C245 M8 a je súčasťou predloženej objednateľnej konfigurácie Cisco.* *Oficiálny výsledok SPEC pre server Cisco UCS C245 M8 osadený dvomi procesormi AMD EPYC 9335 uvádza:* • *SPECrate®2017_int_base = 852 bodov,* • *2 osadené procesory,* • *spolu 64 aktívnych fyzických jadier, teda 32 jadier na jeden procesor.*	**SPLNIL**

		Konfigurácia preto kumulatívne spĺňa požadovaný minimálny výkon 852 bodov, požiadavku dvoch procesorov x86-64, limit maximálne 32 jadier na jeden procesor a podmienku generácie procesora podľa Odpovede č. 20. *https://www.spec.org/cpu2017/results/res2025q2/cpu2017-20250408-47540.html* *https://www.amd.com/en/products/processors/server/epyc/9005-series/amd-epyc-9335.html* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_release-notes-ucsm-4_3.html* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html*	
Počet/max. počet CPU	2/2	***Spĺňa***. *Ponúkaný server Cisco UCS C245 M8 je osadený 2 procesormi AMD EPYC 9335 a podporuje maximálne 2 procesory. Požadovaný údaj: 2/2 CPU.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html*	**SPLNIL**
Pamäť	• požadovaná kapacita 256 GB (4x 64GB), DDR5 Registered min. 6400MHz, • rozšíriteľnosť pamäte pri zachovaní rovnakých modulov je rozšíriteľná na maximálnu veľkosť 1536 GB.	***Spĺňa***. • *V súlade s Vysvetlením informácií potrebných na vypracovanie ponuky zo dňa 24. 8. 2026, Odpoveďou č. 19, je každý zo 4 ponúkaných serverov Cisco UCS C245 M8 osadený:* ○ *4× pamäťový modul UCS-MRX64G2RE5,* ○ *kapacita jedného modulu 64 GB,* ○ *celková kapacita jedného servera 256 GB,* ○ *typ DDR5 Registered DIMM (RDIMM), 2Rx4,* ○ *menovitá, výrobcom deklarovaná rýchlosť DDR5-6400, t. j. 6400 MT/s.* *Ponúkané moduly spĺňajú požiadavku na menovitú rýchlosť najmenej 6400 MT/s. Prípadná nižšia efektívna prevádzková rýchlosť vyplývajúca z architektúry procesora, serverovej platformy alebo podporovaného spôsobu osadenia pamäte je v súlade s Odpoveďou č. 19 a nepovažuje sa za nesplnenie požiadavky.*	**SPLNIL**

		Konfigurácia obsahuje celkovo 16 pamäťových modulov, teda 4 moduly pre každý zo 4 serverov. • *Server obsahuje 24 pamäťových slotov, preto je pri zachovaní existujúcich modulov rozšíriteľný doplnením rovnakých modulov až na 1 536 GB (24× 64 GB).* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_release-notes-ucsm-4_3.html* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/select-ucs-ucsx-hci-accessories-eol15910.html* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html*	
Škálovateľnosť pamäte	do 6144 GB pri využití 256GB modulov	***Spĺňa***. *Server Cisco UCS C245 M8 disponuje 24 slotmi pre pamäťové moduly DDR5 a podporuje moduly s kapacitou 256 GB. Maximálna podporovaná kapacita pamäte jedného servera je preto 6144 GB (24 × 256 GB).* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html*	**SPLNIL**
Ethernet adaptér	• minimálne 1x 1Gb/s port na nezávislé pripojenie od operačného systému. • minimálne 1× duálne portový 10/25Gb/s Ethernet sieťový adaptér vo formáte OCP 3.0 alebo ekvivalentnom serverovom formáte, určený na vysokovýkonné pripojenie servera do dátovej siete. ○ vlastnosti adaptéra: ▪ minimálne 2× sieťový port SFP28 s podporou 10GbE a 25GbE, ▪ hostiteľské rozhranie minimálne PCIe x8,	***Spĺňa***. • *Server obsahuje 1× dedikovaný 10/100/1000BASE-T RJ-45 port pre Cisco IMC/BMC, ktorý zabezpečuje nezávislý out-of-band manažment bez závislosti od operačného systému.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-overview.html* • *Server obsahuje 1× NVIDIA ConnectX-6 Lx MCX631432AC-ADAB, Cisco PID UCSC-O-N6CD25GFO, vo formáte OCP 3.0, určený na vysokovýkonné pripojenie servera.* *https://www.cisco.com/c/en/us/products/servers-unified-computing/third-party-adapters-listing.html* *https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction*	**SPLNIL**

	▪ podpora virtualizačných technológií sieťového adaptéra, SR-IOV alebo ekvivalent, ▪ podpora akcelerácie softvérovo definovaných sietí a offloadu sieťovej prevádzky, ▪ podpora overlay enkapsulácií, napríklad VXLAN a GENEVE alebo ekvivalent, ▪ podpora RDMA/RoCE alebo ekvivalentnej nízkolatenčnej technológie pre dátové centrá, ▪ podpora bezpečnostných mechanizmov adaptéra, minimálne hardvérový root of trust, secure firmware update alebo secure boot firmvéru, ▪ podpora vzdialeného zavádzania systému cez sieť, napríklad PXE, UEFI alebo iSCSI boot, ▪ určené na použitie v serveroch pre virtualizované, kontajnerové alebo dátovo náročné prostredia • minimálne 1× štvorportový 1Gb/s Ethernet adaptér s metalickými portami RJ45, o vlastnosti adaptéra: ▪ minimálne 4× port RJ45 s podporou 1000BASE-T, ▪ spätná podpora 100BASE-TX, ▪ podpora štandardnej kabeláže kategórie CAT5e/CAT6/CAT6A,	o *Adaptér obsahuje 2× SFP28 port s podporou prenosových rýchlostí 10 a 25 Gb/s.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction o *Adaptér využíva hostiteľské rozhranie PCIe 4.0 x8.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction o *NVIDIA ConnectX-6 Lx podporuje hardvérovú virtualizáciu I/O a technológiu SR-IOV s izolovanými prostriedkami pre virtuálne stroje.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction o *Adaptér podporuje hardvérový CPU offload, Open vSwitch offload a technológiu NVIDIA ASAP² vrátane akcelerácie spracovania a tunelovania sieťovej prevádzky.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction o *Adaptér podporuje hardvérový offload overlay protokolov VXLAN a NVGRE a prostredníctvom firmvéru aj GENEVE.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction https://networking-docs.nvidia.com/connectx6lxfwrn/26352000lts/changes-and-new-feature-history o *NVIDIA ConnectX-6 Lx podporuje RDMA a RoCE pre nízkolatenčný prenos dát v sieťach dátových centier.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction o *Ponúkaný variant MCX631432AC-ADAB podporuje hardvérový Root of Trust, Secure Boot a zabezpečenú aktualizáciu firmvéru pomocou RSA kryptografie a unikátneho kľúča zariadenia.*	

	▪ hostiteľské rozhranie minimálne PCIe 3.0 x8 alebo ekvivalent, ▪ podpora Energy Efficient Ethernet podľa IEEE 802.3az, ▪ podpora hardvérových offload mechanizmov na zníženie záťaže CPU, ▪ podpora virtualizačných a overlay funkcií, napríklad VXLAN, GENEVE, NVGRE alebo ekvivalent, ▪ podpora optimalizácie paketového spracovania pre serverové a virtualizované prostredia, ▪ vhodný na manažment, doplnkové dátové siete, oddelené prevádzkové siete alebo nezávislé sieťové pripojenie servera	https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction ○ *Adaptér podporuje sieťové zavádzanie systému prostredníctvom UEFI ovládača vrátane UEFI Secure Boot.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction ○ *NVIDIA ConnectX-6 Lx je serverový adaptér určený pre virtualizované podnikové dátové centrá, vysokovýkonné výpočty, softvérovo definované siete a dátovo náročné pracovné záťaže.* https://networking-docs.nvidia.com/connectx6lxocp3hw/introduction • *Server obsahuje 1× Intel Ethernet Network Adapter I710-T4L, Cisco PID UCSC-P-IQ1GC, so štyrmi metalickými portmi RJ-45.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Adaptér poskytuje 4× RJ-45 port s podporou 1000BASE-T.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Porty podporujú automatické vyjednávanie medzi 1000BASE-T a 100BASE-TX.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Adaptér podporuje štandardnú metalickú kabeláž kategórií CAT5e, CAT6 a CAT6A.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Adaptér využíva hostiteľské rozhranie PCIe 3.0 x8.*	

		https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Intel I710-T4L podporuje Energy Efficient Ethernet podľa IEEE 802.3az.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Adaptér podporuje hardvérové offloady vrátane checksum offload, TCP Segmentation Offload, Receive Side Scaling a Intel Ethernet Flow Director.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Adaptér podporuje Intel Virtualization Technology, SR-IOV a hardvérové offloady overlay protokolov VXLAN, GENEVE a NVGRE.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Adaptér podporuje Intel Ethernet Flow Director, RSS, DPDK a optimalizované spracovanie malých paketov pre virtualizáciu a Network Functions Virtualization.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf ○ *Štvorportový serverový adaptér Intel I710-T4L poskytuje štyri samostatné 1GbE rozhrania vhodné na manažment, doplnkové dátové siete a oddelenie prevádzkových segmentov.* https://cdrdv2-public.intel.com/741849/Cisco%20Product%20Brief%20for%20Intel%20Ethernet%20Network%20Adapter%20I710-T4L.pdf	

Diskový radič	• minimálne 2x hardvérový diskový radič:
	  ○ radič s podporou min. RAID 1 s rozhraním M.2
	  ○ radič s podporou pripojenia minimálne 28 diskov typu SAS/SATA/U.3 NvVMe, 4 GB Cahce, s minimálnou podporou RAID 0,1,5,10,50,60, JBOD a možnosťou mixovaného módu RAID a JBOD
		Spĺňa.
		• *Každý server obsahuje dva samostatné hardvérové diskové radiče:*
		  ○ *Cisco Boot Optimized M.2 RAID Controller – UCS-M2-HWRAID-D*
		  ○ *Cisco 24G Tri-Mode MP1 RAID Controller – UCSC-RAID-MP1L32*
		https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-overview.html
		Cisco UCS-M2-HWRAID-D je hardvérový radič pre dvojicu M.2 SATA diskov s podporou RAID 1 a JBOD. V serveri sú k radiču osadené 2× 480 GB M.2 SATA SSD, ktoré umožňujú konfiguráciu zrkadleného RAID 1.
		https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/ucs-c-series-rack-servers/223121-configure-ucs-c-series-optimized-m-2.html
		• *Cisco UCSC-RAID-MP1L32 je 24 Gb/s Tri-Mode hardvérový RAID radič so 4 GB Flash-Backed Write Cache, ktorý podporuje až 32 diskov typu SAS, SATA alebo U.3 NVMe. Podporuje RAID 0, 1, 5, 6, 10, 50 a 60, režim JBOD a súčasnú kombinovanú prevádzku RAID a JBOD.*
		https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/4-3/b_ucsm_gui_storage_management_guide_4_3/m_gui_m-series_storage_profiles.html
		https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-overview.html
			SPLNIL

Subsystém pevných diskov	• minimálne 2x 480GB typu SSD s rozhraním M.2 • minimálne 5x 1.6TB typu SSD s rozhraním SAS a minimálnou rýchlosťou 24 Gbps, podpora vysokej výdrže minimálne 3x DWPD (úplný prepis celého disku za deň)	***Spĺňa.*** • *Každý server obsahuje 2× 480 GB M.2 SATA SSD Solidigm S4520, Cisco PID UCS-M2480OA1V. Disky sú pripojené k Cisco Boot Optimized M.2 RAID radiču a umožňujú konfiguráciu RAID 1.* *https://www.cisco.com/c/en/us/support/docs/field-notices/742/fn74253.html* • *Každý server obsahuje 5× 1,6 TB 2,5-palcový Enterprise Performance SSD KIOXIA PM7-V, Cisco PID UCS-SD16TKA3XEP-D, s rozhraním 24G SAS (SAS-4) a vysokou výdržou 3 DWPD.*	**SPLNIL**

		https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/x210cm7-specsheet.pdf https://americas.kioxia.com/en-us/business/ssd/enterprise-ssd/pm7-v.html	
Škálovateľnosť diskovej kapacity pre vybranú typovú radu serverov	minimálne 28 diskov SFF pre jeden server	***Spĺňa***. *Server Cisco UCS C245 M8 podporuje škálovanie diskovej kapacity až na 28 diskov formátu SFF, z toho 24 predných a až 4 prídavné zadné pozície pre SAS, SATA alebo NVMe SSD.* https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html	**SPLNIL**
Konektor	minimálne jeden KVM konektor, ktorý poskytuje pripojenie 2x USB zariadenia, jedného VGA a jedného sériového zariadenia.	***Spĺňa***. *Server Cisco UCS C245 M8 obsahuje jeden predný KVM konektor, ktorý prostredníctvom KVM kábla poskytuje pripojenie 2× USB 2.0, 1× VGA a 1× sériové rozhranie DB-9.* https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-overview.html	**SPLNIL**
PCI sloty	minimálne 3x voľný rozširujúci slot PCI-Express Gen4 (x8; x16; x8)	***Spĺňa***. *Server Cisco UCS C245 M8 má osadený Riser 1A s tromi slotmi PCIe Gen4 (x8, x16, x8).* https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-overview.html	**SPLNIL**
Integrovaný grafický adaptér	integrovaný grafický adaptér na základnej doske	***Spĺňa***. *Každý zo 4 serverov Cisco UCS C245 M8 (UCSC-C245-M8SX) disponuje integrovaným grafickým adaptérom VGA na základnej doske a zadným obrazovým konektorom VGA typu DB-15.* https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-overview.html	**SPLNIL**
Napájacie zdroje	• redundancia: N+1 • minimálny výkon jedného zdroja 1200W pri 230V	***Spĺňa***. *Každý zo 4 serverov Cisco UCS C245 M8 je osadený 2× 1200 W AC Titanium zdrojom UCSC-PSU1-1200W-D v redundantnom režime 1+1 (N+1). Každý zdroj poskytuje výkon 1200 W pri vstupnom napätí 208 – 230 V AC.* https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-server-specifications.html	**SPLNIL**

Bezpečnosť	Požiadavky navrhnuté tak, aby poskytovali vysoký stupeň bezpečnosti s nasledovnými vlastnosťami: • Modul TPM 2.0, • Podpora SPDM (Security Protocol and Data Model), • Podpora MCTP (Management Component Transport Protocol) over PCIe Vendor Defined Messaging, • Podpora BIOS Scrub Policies, • Trust anchor module (TAM).	***Spĺňa***. • *Každý server obsahuje modul UCS-TPM2-002D-D, kompatibilný s TPM 2.0 a FIPS 140-2.* *https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-sff-rack-server.pdf* • *Cisco CIMC/BMC podporuje SPDM autentifikáciu hardvéru a firmvéru diskového radiča.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/4-3/b_ucsm_gui_storage_management_guide_4_3/m_gui_m-series-storage-profiles.html* • *Platforma podporuje komunikáciu MCTP prenášanú prostredníctvom PCIe Vendor Defined Messaging vrátane prenosu správ SPDM.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/mctp-mgmt-ucs-m6-gen-wp.html* • *Server podporuje konfigurovateľné scrub politiky vrátane nastavenia čistenia a kontroly pamäte.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Server-Mgmt/4-3/b_cisco_ucs_manager_server_mgmt_cli_guide_4_3/m-cli-server-new-and-changed-information-4-3.html* • *Hardvérový TAm zabezpečuje koreň dôvery, overenie bootloadera a spúšťanie iba autentického, digitálne podpísaného firmvéru.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_release-notes-ucsm-4_3.html*	**SPLNIL**
Správa a manažment	• hardvérový komponent nezávislý od operačného systému formou vzdialenej grafickej KVM konzoly, • možnosť pripojenia vzdialených médií, napr. CD ROM, DVD ROM, ISO image, USB kľúč, FDD, vzdialený adresár,	***Spĺňa***. • *Integrovaný hardvérový radič Cisco IMC/BMC pracuje nezávisle od procesorov a operačného systému a poskytuje vzdialenú vKVM konzolu.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/6_0/b-cisco-ucs-c-series-imc-gui-configuration-guide-m7-and-later-rack-servers-release-6-0/m_gui_overview.html*	**SPLNIL**

	• možnosť štartu, reštartu a vypnutia servera cez sieť LAN, nezávisle od OS, • možnosť centrálne manažovať firmware, • možnosť centrálne manažovať ovládače OS, • možnosť automaticky registrovať servisné incidenty priamo u výrobcu, • automatická obnova poškodeného / neautentického firmware servera, • server plne integrovaný so softvérovým nástrojom pre centrálnu správu serverovej infraštruktúry.	• *Cisco IMC podporuje mapovanie CD/DVD, FDD, USB, ISO/IMG súborov a vzdialených úložísk prostredníctvom NFS, CIFS a HTTP/HTTPS.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/6_0/b_cisco_ucs_c-series_gui_configuration_guide_6-0/m_gui_managing_remote_presence.pdf* • *Cisco IMC umožňuje cez manažmentovú LAN vykonávať power-on, power-off, reset a power-cycle nezávisle od OS.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/6_0/b-cisco-ucs-c-series-imc-gui-configuration-guide-m7-and-later-rack-servers-release-6-0/m_gui_overview.html* • *Ponúkaný Cisco Intersight Infrastructure Services Private Virtual Appliance – Advantage umožňuje centrálne riadenie firmvérových politík, kompatibility a aktualizácií serverov.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html* • *Cisco Intersight centrálne zhromažďuje verzie OS a ovládačov, vyhodnocuje ich zhodu s Cisco HCL a poskytuje odporúčania.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/cdip_pvc_ucs_m6.html* • *Každý zo štyroch ponúkaných serverov Cisco UCS C245 M8 bude pripojený a registrovaný v Cisco Intersight SaaS alebo prostredníctvom Cisco Intersight Connected Virtual Appliance s aktivovanou službou Proactive RMA a platným servisným kontraktom. Pri podporovaných hardvérových poruchách služba automaticky, bez zásahu obsluhy, vytvorí servisnú požiadavku (SR) a RMA priamo u výrobcu Cisco.* *https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/intersight/215172-proactive-rma-for-intersight-connected-d.html* • *Cisco Secure Boot zabraňuje spusteniu neautentického firmvéru a server podporuje automatickú obnovu BIOS a alternatívny obraz Cisco IMC.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-maintain-the-server.html*	

		• *Server je prostredníctvom integrovaného Device Connectora plne podporovaný v Cisco Intersight; konfigurácia obsahuje režim ISM a licenciu Intersight Advantage pre každý server.* *https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html*	
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • výmena zariadenia v prípade poruchy v režime 8x5xNBD, • centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: ○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora, ○ prístup k softvérovým aktualizáciám, opravným verziám, bezpečnostným opravám, odporúčaným postupom a technickej dokumentácii výrobcu počas celej doby trvania podpory ○ výrobca poskytne podporu na úrovni riešení, ktorá zahŕňa centralizovanú expertízu a správu problémov v rámci riešenia produktov výrobcu a tretích strán schválených výrobcom ○ podpora na úrovni riešení sa vzťahuje na riešenia pozostávajúce z produktov výrobcu a schválených partnerov výrobcu (minimálne VMware a Veeam, ktorými už aktuálne disponuje verejný obstarávateľ), kde je zabezpečený prístup k tímu expertov na riešenia, ktorí	***Spĺňa***. *Pre každý zo 4 ponúkaných serverov Cisco UCS C245 M8, model UCSC-C245-M8SX, je ponúknutá samostatná servisná podpora:* • *výrobca: Cisco Systems,* • *služba: Cisco Support – Standard / CX Level 1,* • *servisný PID: CON-L1NBD-UCSCM8SX,* • *servisná úroveň hardvéru: 8x5xNBD,* • *doba poskytovania podpory: 24 mesiacov,* • *počet: 4 ks.* *Cisco Support – Standard je aktuálnou náhradou ukončenej služby Cisco Solution Support.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/eos-eol-announcement-legacy-offers.pdf* • *Pre každý zo 4 serverov je nakonfigurovaná podpora CON-L1NBD-UCSCM8SX na obdobie 24 mesiacov.* *Služba zahŕňa rozšírenú výmenu chybného hardvéru v režime 8x5xNBD. Náhradný hardvér, nový alebo funkčne ekvivalentný novému, je dodaný nasledujúci pracovný deň v súlade s podmienkami a miestnou dostupnosťou služby Cisco.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Cisco Support – Standard poskytuje prístup k Cisco TAC, podporu hardvéru, aktualizácie podporovaného softvéru a podporu na úrovni riešenia. Podpora pokrýva ponúkané servery Cisco UCS vrátane ich firmvéru, Cisco IMC a podporovaných nástrojov správy.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf*	**SPLNIL**

	pôsobia ako primárny kontaktný bod a ktorí buď ▪ aktívne riadia problém až do jeho vyriešenia expertmi na produkty, ▪ alebo v rozsahu povolenom partnermi Solution Alliance koordinujú vaše kroky na podporu riešenia problému ○ poskytovateľ podpory musí byť primárny bod kontaktu pre incidenty v riešení, ○ v prípade, ak riešenie pozostáva z produktov výrobcu a produktov jeho aliančných partnerov na podporu riešení, musia byť riešenia vytvorené z približne 50 % alebo viac produktami výrobcu, aby boli oprávnené na takto popisovaný typ podpory, ○ dostupnosť podporného centra v požadovanom režime 24x7 formou telefónu, mailu, alebo cez web prístup k riešeniam pri používaní, konfigurácii, alebo pri riešení problémov: ▪ pre závažnosť hovorov 1 a 2 musí byť odpoveď Centra výrobcu do 30min, ▪ pre závažnosť hovorov 3 a 4 musí byť odpoveď Centra výrobcu do 60min počas pracovných hodín, resp. nasledujúci pracovný deň pri hovoroch mimo pracovných hodín, ○ v prípade komunikácie s výrobcom iných súčasti riešenia je nevyhnutné preukázať existenciu supportných kontraktov u týchto výrobcov.	• *Počas 24-mesačnej podpory má zákazník prístup k príslušným softvérovým a firmvérovým vydaniam, dostupným opravám a náhradným riešeniam, bezpečnostným upozorneniam PSIRT, Field Notices, znalostnej databáze, technickej dokumentácii a odporúčaným konfiguračným postupom Cisco.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Cisco Support – Standard obsahuje Solution Level Support, ktorý poskytuje centralizovanú expertízu a správu incidentov naprieč riešením pozostávajúcim z produktov Cisco a produktov schválených Solution Alliance partnerov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *VMware a Veeam sú spoločnosťou Cisco uvedené medzi globálnymi a strategickými partnermi. Podpora sa vzťahuje na ich produkty a verzie zahrnuté do registrovaného a spoločnosťou Cisco podporovaného rozsahu riešenia, za podmienky existencie príslušných platných servisných kontraktov.* *Tím expertov Cisco pôsobí ako primárny kontaktný bod a:* *a) aktívne riadi incident až do jeho vyriešenia príslušnými produktovými expertmi,* *b) alebo v rozsahu povolenom Solution Alliance partnerom koordinuje kroky zákazníka smerujúce k vyriešeniu incidentu.* *https://www.cisco.com/site/us/en/solutions/global-partners/index.html* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Zákazník má prístup k tímu solution expertov Cisco, ktorí pôsobia ako primárny kontaktný bod, preberajú správu incidentu a koordinujú zapojenie produktových tímov Cisco a príslušných Solution Alliance partnerov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf*	

		• *Jadro podporovaného riešenia tvoria 4 servery Cisco UCS C245 M8 a súvisiace komponenty a nástroje správy Cisco. Rozsah riešenia bude registrovaný tak, aby produkty Cisco predstavovali najmenej približne 50 % podporovaného riešenia.* *Cisco uvádza, že riešenia obsahujúce produkty Solution Support Alliance partnerov majú byť vytvorené približne z 50 % alebo viac produktmi Cisco.* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf* • *Cisco Technical Assistance Center je dostupné 24 hodín denne, 7 dní v týždni prostredníctvom telefónu a webového systému správy servisných prípadov na podporu používania, konfigurácie a riešenia problémov.* *a) Pre incidenty závažnosti 1 a 2 je počiatočný reakčný čas Cisco Support – Standard maximálne 30 minút.* *b) Pre incidenty závažnosti 3 a 4 je reakčný čas maximálne 60 minút počas pracovných hodín. Na incidenty prijaté mimo pracovných hodín Cisco reaguje nasledujúci pracovný deň.* *Režim TAC 24x7 je nezávislý od režimu hardvérovej výmeny 8x5xNBD.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* • *Pre produkty VMware a Veeam zahrnuté do podporovaného riešenia budú počas celej doby podpory zabezpečené a v prípade komunikácie s výrobcom iných súčasti riešenia budú predložené servisné kontrakty príslušných výrobcov. Tieto kontrakty umožnia Cisco koordinovať riešenie incidentov s produktovými tímami aliančných partnerov.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Support.pdf* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf*	
Prevedenie	• 19“ serverová skriňa, • výška 2U, • súčasťou servera musia byť aj koľajnice na montáž do serverovej skrine spolu s ramenom	***Spĺňa***. • *Ponúkaný server Cisco UCS C245 M8 (UCSC-C245-M8SX) je rackový server určený na montáž do štandardného 19" racku.* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-install-the-server.html*	**SPLNIL**

	na vedenie kabeláže, ktoré umožňuje servisovanie počas prevádzky	• *Cisco UCS C245 M8 má vyhotovenie 2RU, teda zaberá dve rackové jednotky.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html* • *Pre každý zo 4 serverov konfigurácia obsahuje:* *1× UCSC-RAIL-D – súprava guľôčkových výsuvných koľajníc,* *1× UCSC-CMA-C240-D – reverzibilné rameno na vedenie kabeláže.* *Koľajnice umožňujú vysunutie servera z racku a rameno CMA zachováva vedenie a pripojenie kabeláže počas vysunutia. Tým je umožnený servis servera v racku počas prevádzky, najmä pri komponentoch podporujúcich výmenu za chodu, v súlade so servisnými postupmi Cisco.* *https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c245-m8-rack-server-ds.html* *https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c245m8/install/b-cisco-ucs-c245-m8/m-install-the-server.html*	

Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca dopravu, montáž, inštaláciu a nastavenie dodaných zariadení prípadne softvérov pre preukázanie funkčnosti a prevádzkyschopnosti dodaného zariadenia Server Typ 2. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného zariadenia Server Typ 2. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávané zariadenia Server Typ 2	***Spĺňa***. • *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného* zariadenia Server Typ 2. • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného* zariadenia Server Typ 2. • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Cisco Black Belt Academy – Unified Computing System (UCS) Deployment Stage 3 vydaný výrobcom Black Belt Academy Cisco Systems, Inc. pre dodávané zariadenia Server Typ 2.*	**SPLNIL**
Počet serverov	4 ks	*Ponúkané riešenie obsahuje 4 ks serverov Cisco UCS C245 M8, model UCSC-C245-M8SX*	**SPLNIL**

2.4 LAN prepínač typ 1

LAN prepínač typ 1			Hodnotenie (SPLNIL / NESPLNIL)
Parameter	**Minimálne požadované parametre**	**Plnenie uchádzača – uviesť parameter alebo vlastnosť ponúkaného tovaru**	
Výrobca/ model:	Uchádzač uvedie výrobcu, produkt, edíciu/verziu, licenčný model a relevantné komponenty, ktorými preukazuje splnenie požiadaviek.	***Výrobca/model:*** *Cisco Systems, Inc. – Cisco Catalyst C9300-24T-A s uplinkovým modulom C9300-NM-8X, 4 ks.* ***Produkt a edícia:*** *24-portový dátový prepínač Cisco Catalyst 9300 s edíciou Network Advantage a modulom 8× 1/10GE SFP/SFP+.* ***Verzia a licenčný model:*** *Cisco IOS XE 17.18; trvalá licencia Network Advantage a časovo obmedzená licencia Cisco DNA Advantage na 3 roky pre každý prepínač.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html* *Technická špecifikácia:* • *4x C9300-24T-A - Catalyst 9300 with 24 data ports and Network Advantage* • *4x C9300-NM-8X - Catalyst 9300 network module with 8× 10GE ports* • *4x C9300-NW-A-24 - Network Advantage license for 24 ports* • *4x C9300-DNA-A-24-3Y - DNA Advantage license for 24 ports, 3-year term* • *4x D-DNAS-EXT-S-3Y - Cisco DNA Spaces Extend license for Catalyst switches, 3-year term* • *4x TE-EMBEDDED-T-3Y - Cisco ThousandEyes Enterprise Agent license, 3-year term* • *4x TE-C9K-SW - ThousandEyes agent software for IOS XE on Catalyst 9000* • *4x SC9300UK9-1718 - Universal software for Catalyst 9300*	**SPLNIL**

		• *4x CON-L1NBD-C93002TA - CX Level 1 8x5xNBD support for Catalyst 9300* • *4x CON-L1SWT-C93A24 - CX Level 1 software subscription support for DNA Advantage* • *4x PWR-C1-350WAC-P - 350W AC 80+ Platinum power supply* • *4x CAB-TA-EU - European AC power cable*	
Priepustnosť	minimálne 205 Gigabits per second (Gbps)	***Spĺňa***. *Každý zo 4 ponúkaných prepínačov Cisco C9300-24T-A dosahuje prepínaciu kapacitu 208 Gbps.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Rýchlosť smerovania	minimálne 152 Mpps	***Spĺňa***. *Ponúkaný prepínač Cisco C9300-24T-A s modulom C9300-NM-8X poskytuje prepínaciu kapacitu 208 Gbps.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Požadované osadenie portami	• minimálne 24 portov 1000BASE-T RJ-45 pre koncové zariadenia, bez PoE, • minimálne 8 porty 1/10Gig SPF+	***Spĺňa***. *Každý ponúkaný prepínač Cisco C9300-24T-A s modulom C9300-NM-8X je vybavený:* • *24× 10/100/1000BASE-T RJ-45 dátovým portom bez PoE,* • *8× uplinkovým portom SFP/SFP+ s podporou rýchlostí 1/10 Gbps.* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Product-overview.html*	**SPLNIL**
Napájacie zdroje	• možnosť redundantné napajánia N+1, • požadovaný 1 zdroj s minimálnym výkonom 350W pri 230V	***Spĺňa***. • *Každý prepínač Cisco C9300-24T-A podporuje dva redundantné, za prevádzky vymeniteľné napájacie zdroje – možnosť redundancie N+1 (1+1).* • *Ponúkaná konfigurácia obsahuje jeden zdroj PWR-C1-350WAC-P s výkonom 350 W a rozsahom vstupného napätia 100 až 240 V AC, teda podporuje aj prevádzku pri 230 V. Druhý zdroj je možné doplniť.*	**SPLNIL**

		https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	
Dedikované rozhranie pre OOB	sériová konzola RJ45 a USB-mini aj samostatný OOB Ethernet port	***Spĺňa***. *Každý prepínač Cisco C9300-24T-A obsahuje:* • *sériový konzolový port RJ-45 (EIA/TIA-232),* • *konzolový port USB mini-Type B,* • *samostatný OOB Ethernet management port MGMT RJ-45 10/100/1000BASE-T vo vyhradenej VRF.* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Product-overview.html*	**SPLNIL**
Počet IPv4 route záznamov	minimálne 30 000	***Spĺňa***. *Cisco C9300-24T-A podporuje celkovo 32 000 IPv4 smerovacích záznamov (24 000 priamych a 8 000 nepriamych trás.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet IPv6 route záznamov	minimálne 15 000	***Spĺňa***. *Cisco C9300-24T-A podporuje 16 000 IPv6 smerovacích záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Požadovaný počet VLAN	minimálne 4090	***Spĺňa***. *Cisco C9300-24T-A podporuje 4 094 VLAN ID.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet MAC address záznamov	minimálne 30 000	***Spĺňa***. *Cisco C9300-24T-A podporuje 32 000 MAC adries.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet podporovaných Switched Virtual Interfaces (SVI)	minimálne 1000	***Spĺňa***. *Cisco C9300-24T-A podporuje celkovo 1 000 Switched Virtual Interfaces (SVI).* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**

Počet PVST inštancií	minimálne 300	***Spĺňa***. *Cisco C9300-24T-A podporuje 300 PVST inštancií.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Počet Flexible NetFlow (FNF) záznamov	minimálne 60000	***Spĺňa***. *Cisco C9300-24T-A podporuje 64 000 Flexible NetFlow (FNF) záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Celkový počet ACL záznamov	minimálne 5000	***Spĺňa***. *Cisco C9300-24T-A podporuje celkovo 5 120 ACL záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Celkový počet QoS záznamov	minimálne 5000	***Spĺňa***. *Cisco C9300-24T-A podporuje celkovo 5 120 QoS záznamov.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Požadovaný Mean Time Between Failure (MTBF)	minimálne 314 000 hodín	***Spĺňa***. *Výrobcom deklarovaná hodnota MTBF pre Cisco C9300-24T-A je 314 790 hodín.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	**SPLNIL**
Technické vlastnosti:	Prepínač musí funkčne a licenčne spĺňať nasledovné technické požiadavky a funkcionality: • samostatný manažovateľný prepínač pracujúci na 2. a 3. vrstve OSI, • podpora Jumbo Frame min. 9198 bytov, • podpora RFID TAG pre potreby inventarizácie, • podpora statického smerovania,	***Spĺňa***. • *Cisco C9300-24T-A je samostatne prevádzkovateľný manažovateľný prepínač podporujúci funkcie 2. a 3. vrstvy OSI vrátane pokročilého IP smerovania.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Prepínač podporuje Jumbo Frame s veľkosťou až 9 198 bytov.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Šasi obsahuje integrovaný pasívny RFID tag podporujúci automatickú identifikáciu, evidenciu a sledovanie zariadenia.*	**SPLNIL**

	• podpora dynamického smerovania (RIP, OSPF), • podpora BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM-BIDIR,* IP SLA, OSPF • podpora IP multicast (PIM SSM, PIM SM), • podpora MACsec-256, • podpora stohu cez dedikované stohovacie rozhranie do veľkosti 8 prepínačov, • podpora 802.1x, • podpora 802.1p CoS a DSCP klasifikácie, • podpora 802.1Q VLAN, • podpora IEEE 802.1w, IEEE 802.1d, IEEE 802.1s, • podpora SNMPv1/v2c/v3, • podpora SPAN a RSPAN, ERSPAN • podpora redundantých ventilátorov – 3ks, • podpora automatizácie prostredníctvom protokolov RESTCONF, NETCONF, gRPC, YANG, PnP Agent, ZTP/Open PnP, GuestShell (On-Box Python) • možnosti správy a manažmentu – prostredníctvom centrálneho manažmentu, web rozhrania, príkazového riadku, • podpora ochrany proti nahraniu modifikovaného software do zariadenia prostredníctvom image signing a funkcie secure boot, ktorá overuje autenticitu a integritu bootloadera a operačného systému zariadenia pomocou interných HW prostriedkov - tzv. trusted modulov, • podpora Full Flexible Netflow a PnP,	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Product-overview.html • *Cisco C9300-24T-A podporuje statické smerovanie IPv4 a IPv6.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje dynamické smerovacie protokoly RIPv1, RIPv2, RIPng a plnohodnotný OSPF/OSPFv3.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Všetky požadované funkcie sú podporované a licenčne pokryté dodanou licenciou Network Advantage.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje IP multicast vrátane PIM Sparse Mode (PIM-SM) a Source-Specific Multicast (PIM-SSM).* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Cisco C9300-24T-A s licenciou Network Advantage podporuje IEEE 802.1AE MACsec so šifrovaním AES-256.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač obsahuje dedikované rozhrania StackWise-480 a podporuje vytvorenie stohu s maximálne 8 prepínačmi.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje riadenie prístupu a autentifikáciu podľa IEEE 802.1X.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html • *Prepínač podporuje klasifikáciu a prioritizáciu prevádzky podľa IEEE 802.1p CoS a DSCP.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html	

	• podpora stackovania s priepustnosťou až 480 Gbps	• *Prepínač podporuje VLAN a označovanie rámcov podľa IEEE 802.1Q.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Prepínač podporuje Rapid Spanning Tree IEEE 802.1w, Spanning Tree IEEE 802.1D a Multiple Spanning Tree IEEE 802.1s.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Prepínač podporuje protokoly SNMPv1, SNMPv2c a SNMPv3.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Prepínač podporuje SPAN a RSPAN; funkcia ERSPAN je licenčne pokrytá dodanou licenciou Cisco DNA Advantage.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Prepínač obsahuje 3 za prevádzky vymeniteľné ventilátorové moduly FAN-T2 a podporuje redundanciu ventilátorov N+1.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Licencia Network Advantage podporuje automatizáciu prostredníctvom NETCONF, RESTCONF, gRPC, YANG, PnP Agent, ZTP/Open PnP a GuestShell s On-Box Python.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Prepínač je možné spravovať centrálne prostredníctvom Cisco Catalyst Center, lokálnym webovým rozhraním WebUI a príkazovým riadkom CLI.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Cisco C9300-24T-A používa kryptografické podpisovanie obrazov systému, Secure Boot a hardvérový Cisco Trust Anchor modul na*	

		overenie autenticity a integrity firmvéru, bootovacieho procesu a operačného systému. *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *Dodaná licencia Cisco DNA Advantage podporuje Full Flexible NetFlow; Network Advantage a položka NETWORK-PNP-LIC zabezpečujú podporu Cisco Plug and Play.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html* • *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-18/configuration_guide/nmgmt/b_1718_nmgmt_9300_cg/configuring_flexible_netflow.html* • *Cisco C9300-24T-A podporuje technológiu StackWise-480 s obojsmernou stohovacou priepustnosťou 480 Gbps.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*	
Servisná podpora	minimálne 2 roky od zakúpenia s nasledujúcimi parametrami: • výmena zariadenia v prípade poruchy v režime 8x5xNBD, • centralizovaná podpora dodávaného riešenia, ktorého je produkt súčasťou s nasledujúcimi charakteristikami: ○ podpora celkového riešenia nasadených hardvérových aj softvérových produktov výrobcu, na ktoré je poskytovaná podpora, ○ prístup k softvérovým aktualizáciám, opravným verziám, bezpečnostným opravám, odporúčaným postupom a	***Spĺňa***. • *Podpora je poskytovaná počas 24 mesiacov. Zahŕňa výmenu chybného zariadenia v režime 8×5×NBD, teda dodanie náhradného hardvéru nasledujúci pracovný deň počas štandardných pracovných hodín, v závislosti od miestnej dostupnosti služby.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html* *https://www.cisco.com/E-Learning/pa/bulk/csep_update/m06/m06_t02_p02.shtml* • *Cisco CX Level 1 poskytuje podporu hardvéru, Cisco IOS XE, softvérových licencií a súvisiacich produktov Cisco zahrnutých do podporovaného riešenia.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html*	**SPLNIL**

	technickej dokumentácii výrobcu počas celej doby trvania podpory ○ výrobca poskytne podporu na úrovni riešení, ktorá zahŕňa centralizovanú expertízu a správu problémov v rámci riešenia produktov výrobcu a tretích strán schválených výrobcom ○ podpora na úrovni riešení sa vzťahuje na riešenia pozostávajúce z produktov výrobcu a schválených partnerov výrobcu (minimálne VMware a Veeam, ktorými už aktuálne disponuje verejný obstarávateľ), kde je zabezpečený prístup k tímu expertov na riešenia, ktorí pôsobia ako primárny kontaktný bod a ktorí buď ○ aktívne riadia problém až do jeho vyriešenia expertmi na produkty, ○ alebo v rozsahu povolenom partnermi Solution Alliance koordinujú vaše kroky na podporu riešenia problému ○ poskytovateľ podpory musí byť primárny bod kontaktu pre incidenty v riešení, ○ v prípade, ak riešenie pozostáva z produktov výrobcu a produktov jeho aliančných partnerov na podporu riešení, musia byť riešenia vytvorené z približne 50 % alebo viac produktami výrobcu, aby boli oprávnené na takto popisovaný typ podpory,	• *Podpora zahŕňa prístup k aktualizáciám Cisco IOS XE, opravným a bezpečnostným verziám, bezpečnostným upozorneniam, prioritným chybám, odporúčaným postupom, znalostnej databáze a technickej dokumentácii Cisco počas celej doby podpory.* *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html* *https://www.cisco.com/c/en/us/support/web/tac/technical-services-resource-guide.html* • *Cisco Solution Support poskytuje centralizovanú expertízu a správu incidentov pre riešenia pozostávajúce z produktov Cisco a podporovaných produktov tretích strán. Cisco koordinuje príslušné produktové tímy počas riešenia incidentu.* *https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf* • *Podpora umožňuje koordináciu riešenia incidentov s aliančnými partnermi Cisco. Tím expertov Cisco vystupuje ako primárny kontaktný bod, aktívne riadi incident do vyriešenia alebo koordinuje postup s podporou príslušného aliančného partnera. VMware a Veeam sú súčasťou partnerského ekosystému Cisco; rozsah konkrétnych produktov sa overuje v Cisco Solution Alliance Partner Product Directory.* *https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf* *https://www.cisco.com/c/m/en_us/customer-experience/support/product-directory.html* *https://www.cisco.com/site/us/en/solutions/global-partners/index.html* • *Cisco Solution Support poskytuje jeden primárny kontaktný bod pre incidenty v celom podporovanom riešení bez potreby, aby zákazník vopred určil konkrétny chybný produkt alebo výrobcu.*	

	○ dostupnosť podporného centra v požadovanom režime 24x7 formou telefónu, mailu, alebo cez web prístup k riešeniam pri používaní, konfigurácii, alebo pri riešení problémov: ▪ pre závažnosť hovorov 1 a 2 musí byť odpoveď Centra výrobcu do 30min, ▪ pre závažnosť hovorov 3 a 4 musí byť odpoveď Centra výrobcu do 60min počas pracovných hodín, resp. nasledujúci pracovný deň pri hovoroch mimo pracovných hodín, ○ v prípade komunikácie s výrobcom iných súčasti riešenia je nevyhnutné preukázať existenciu supportných kontraktov u týchto výrobcov.	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Ponúkané riešenie je tvorené prevažne produktmi Cisco. Podľa podmienok Cisco majú riešenia obsahujúce produkty aliančných partnerov pozostávať približne z 50 % alebo viac produktov Cisco.* https://www.cisco.com/c/dam/en_us/services/portfolio/documents/cisco-solution-support.pdf • Cisco TAC je dostupné 24×7 telefonicky alebo online pre otázky používania, konfigurácie a riešenia problémov. Garantované reakčné časy sú: ○ závažnosť 1 a 2: do 30 minút, ○ závažnosť 3 a 4 počas pracovných hodín: do 60 minút, ○ závažnosť 3 a 4 mimo pracovných hodín: nasledujúci pracovný deň. https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf • *Podmienka je akceptovaná. Pri eskalácii incidentu na výrobcu produktu tretej strany musí byť pre príslušný produkt zabezpečený a preukázaný platný supportný kontrakt. Cisco vyžaduje aktívnu podporu všetkých produktov aliančných partnerov zapojených do podporovaného riešenia.* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf	
Prevedenie	• 19“ serverová skriňa, • výška 1U	***Spĺňa***. • *Cisco C9300-24T-A je určený na montáž do štandardného 19-palcového serverového racku pomocou dodaných montážnych konzol.* • *Zariadenie má výšku 1U (4,4 cm).* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/Installing-a-switch.html https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/technical-specs.html	**SPLNIL**

Inštalácia	• súčasťou ponuky musí byť inštalačná služba zahrňujúca montáž, inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného LAN prepínač typ 1. • inštalačnú službu musí zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného LAN prepínač typ 1. • uchádzač musí preukázať, že disponuje aktuálne platným certifikátom vydaný výrobcom alebo producentom, resp. osobou, ktorá je oprávnená tento certifikát vydávať pre dodávaný LAN prepínač typ 1.	• *Súčasťou ponuky je inštalačná služba zahrňujúca inštaláciu a nastavenie dodaného zariadenia pre preukázanie funkčnosti a prevádzkyschopnosti dodaného LAN prepínač typ 1.* • *Inštalačnú službu bude zabezpečovať certifikovaná osoba oprávnená zabezpečovať montáž, inštaláciu a nastavenie dodávaného LAN prepínač typ 1.* • *Ako uchádzač preukazujeme, že disponujeme aktuálne platným certifikátom Cisco Certified Specialist - Enterprise Advanced Infrastructure Implementation vydaný výrobcom Cisco Systems, Inc. pre dodávaný LAN prepínač typ 1.*	
Počet zariadení	4 ks	*Ponúkané riešenie obsahuje 4 ks prepínačov Cisco C9300-24T-A, každý osadený modulom C9300-NM-8X.*	**SPLNIL**