Splnenie požiadaviek na predmet zákazky

Posilnenie informačnej a kybernetickej bezpečnosti MF SR –
Vestník verejného obstarávania . 234/2025 dňa 20. 11. 2025 pod č. 18386 – MSS

Bezpečnostný nástroj 1
(Nástroj na ochranu perimetra – Next Generation Firewall)

Verejný obstarávateľ požaduje nástroj na ochranu perimetra (NGFW), ktorý spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Počet portov a. GE SFP porty: min. 2 ks. b. GE RJ45 Internal Ports min. 6 ks. c. GE RJ45 FortiLink Ports min. 2 ks. d. USB Port 3.0 min. 1 ks. e. Console Port (RJ45) min. 1 ks.	• FG-80F, FortiGate 80F, HW, HW only (3 ks) • Porty/rozhrania: 8× GE RJ45 + 2× GE RJ45/SFP „shared media“ porty, 1× RJ45 konzola, 1× USB 3.0. • Výkon: Firewall throughput 10/10/7 Gbps (1518/512/64B UDP), IPS 1.4 Gbps, NGFW 1.0 Gbps, Threat Protection 900 Mbps. • VPN: IPsec VPN throughput (512B) 6.5 Gbps, SSL-VPN throughput 950 Mbps. • Kapacity: Concurrent sessions 1.5M, new sessions/s 45k, politiky 5k. • Form factor / rozmery: desktop / wall mount / rack tray; 38.5 × 216 × 160 mm. • Napájanie/spotreba: externé DC adaptéry; priemer/max 12.6W / 15.4W (80F).	✓
Systémové požiadavky a. Firewall priepustnosť (1518/512/64 byte UDP paketov) min. 10/10/7 Gbps. b. Firewall priepustnosť (pakety za sekundu) min. 10,5 Mpps. c. Firewall latencia (64 byte UDP pakety) 3,32 mikro sekúnd. d. Počet súbežných relácií (TCP) min. 1 500 000. e. Nové relácie za sekundu (TCP) min. 45 000. f. IPSec VPN priepustnosť (512 bajtové pakety) min. 6.5 Gbps. g. SSL-VPN priepustnosť min. 950 Mbps. h. Súbežný SSL-VPN používatelia (doporučené max.) 200. i. IPS priepustnosť min. 1.4 Gbps. j. NGFW priepustnosť min. 1 Gbps. k. Threat Protection priepustnosť min. 900 Mbps. l. Virtuálne domény min. 10. m. Konfigurácia vysokej dostupnosti aktívne/aktívne, aktívne/pasívne, klastrovanie. n. Rozmery 1U, forma rack mount. o. Certifikácie ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN.	• https://www.fortinet.com/resources/data-sheets/fortigate-fortiwifi-80f-series • https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf • https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-80f-series.pdf Systémové požiadavky • Firewall priepustnosť (1518/512/64 byte UDP paketov) min. 10/10/7 Gbps. • Firewall priepustnosť (pakety za sekundu) min. 10,5 Mpps. • Firewall latencia (64 byte UDP pakety) 3,32 mikro sekúnd. • Počet súbežných relácií (TCP) min. 1 500 000. • Nové relácie za sekundu (TCP) min. 45 000. • IPSec VPN priepustnosť (512 bajtové pakety) min. 6.5 Gbps. • SSL-VPN priepustnosť min. 950 Mbps. • Súbežný SSL-VPN používatelia (doporučené max.) 200. • IPS priepustnosť min. 1.4 Gbps. • NGFW priepustnosť min. 1 Gbps. • Threat Protection priepustnosť min. 900 Mbps. • Virtuálne domény min. 10. • Konfigurácia vysokej dostupnosti aktívne/aktívne, aktívne/pasívne, klastrovanie. • Rozmery 1U, forma rack mount. • Certifikácie ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN.	

Funkčná špecifikácia a. Pokročilý firewall s možnosťou stavového filtrovania paketov (stateful inspection). b. Funkcionalita IPS (Intrusion Prevention System) s podpisovou a heuristickou detekciou. c. Ochrana proti malvéru, botnetom a škodlivým webovým stránkam (Web Filtering, Anti-Virus). d. Podpora Application Control – identifikácia a riadenie prevádzky na úrovni aplikácií. e. SSL/TLS dešifrovanie a kontrola šifrovanej komunikácie. f. VPN služby: Podpora IPSec VPN a SSL VPN pre vzdialený prístup. g. Možnosť integrácie s autentifikačnými službami (LDAP, RADIUS, SAML). h. Zariadenie musí podporovať Zero Trust Network Access (ZTNA).	Funkčná špecifikácia a. Pokročilý firewall s možnosťou stavového filtrovania paketov (stateful inspection). b. Funkcionalita IPS (Intrusion Prevention System) s podpisovou a heuristickou detekciou. c. Ochrana proti malvéru, botnetom a škodlivým webovým stránkam (Web Filtering, Anti-Virus). d. Podpora Application Control – identifikácia a riadenie prevádzky na úrovni aplikácií. e. SSL/TLS dešifrovanie a kontrola šifrovanej komunikácie. f. VPN služby: Podpora IPSec VPN a SSL VPN pre vzdialený prístup. g. Možnosť integrácie s autentifikačnými službami (LDAP, RADIUS, SAML). h. Zariadenie musí podporovať Zero Trust Network Access (ZTNA).	
Záruka a podpora a. Podpora od výrobcu a riešenie tiketov s dostupnosťou 7/24/365 po dobu 24 mesiacov. b. Hardvérová podpora s dostupnosťou 24 x 7 s garantovanou opravou/výmenou vadného komponentu do 24 hod., po dobu trvania 24 mesiacov. c. Balík služieb zahŕňajúci podporu pre IPS, antivírus, aplikačnú kontrolu, DNS filtering, URL filtering, video filtering, anti-botnet a C2 communications služby.	• FC-10-0080F-950-02-12, FortiGate 80F, RNW, Unified Threat Protection + FortiCare Premium 1YR • Network & File Security: IPS, antimalware/AV (vrátane prvkov typu AMP v rámci portfólia), Application Control, reputácia/botnet ochrany atď • Web & DNS Security: URL filtering, DNS filtering, Video filtering. • Anti-Spam (UTP obsahuje Anti-Spam; v porovnávacej tabuľke je pri UTP zahrnutý) • FortiCare Premium je v balíkoch zahrnutý • https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiguard.pdf • https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-forticare.pdf Záruka a podpora • Podpora od výrobcu a riešenie tiketov s dostupnosťou 7/24/365 po dobu 24 mesiacov. • Hardvérová podpora s dostupnosťou 24 x 7 s garantovanou opravou/výmenou vadného komponentu do 24 hod., po dobu trvania 24 mesiacov. • Balík služieb zahŕňajúci podporu pre IPS, antivírus, aplikačnú kontrolu, DNS filtering, URL filtering, video filtering, anti-botnet a C2 communications služby.	✓ ŽoV č. 2 Vysvetlenie akceptované

Informácia pre uchádzača: Požiadavky spĺňa napríklad riešenie zn. **Fortinet**, typ **FortiGate FG-80F-BDL-950-XX** (XX = dĺžka licencie) vrátane FortiCare Premium a FortiGuard Unified Threat Protection (UTP).

Bezpečnostný nástroj 2
(Nástroj pre centrálne riadenie sieťovej ochrany)

Verejný obstarávateľ požaduje nástroj pre centrálne riadenie sieťovej ochrany, ktorý spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Špecifikácia kapacity a. Počet zariadení: min. 6 a max.10. b. Úložisko (GB): 2500. c. Počet logov (GB/deň): 1.	• FMG-VM-10-UG, FortiManager VM, Licence, 10 Device Add-on (1 ks) • Špecifikácia licencie: „Upgrade license for adding 10 Fortinet devices/Virtual domains; allows for total of 2 GB/Day of Logs." • Technické/VM parametre (FortiManager datasheet – VM špecifikácie): • vCPU (min/max): 4 / unlimited • RAM (min/max): 8 GB / unlimited (64-bit) • vNIC (min/max): 1 / 12 (pozn.: VM podporuje až 12 vNIC, závisí od platformy) • https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	✓
Technická špecifikácia a. Podporované virtualizačné prostredia: minimálne VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, alebo novšie. b. Podpora vCPU: min/max. 2/neobmedzené. c. Podpora sieťových rozhraní: min/max. ¼. d. Podpora úložiska: min/max. 80 GB/16 TB. e. Podpora pamäte RAM: min/max. 1 GB/4 GB (32 bit), 2 GB/neobmedzené (64bit).	Technická špecifikácia a. Podporované virtualizačné prostredia: minimálne VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, alebo novšie. b. Podpora vCPU: min/max. 2/neobmedzené. c. Podpora sieťových rozhraní: min/max. ¼. d. Podpora úložiska: min/max. 80 GB/16 TB. e. Podpora pamäte RAM: min/max. 1 GB/4 GB (32 bit), 2 GB/neobmedzené (64bit).	
Funkčná špecifikácia a. Centralizovaná správa zariadení: • Jednotná správa politiky bezpečnosti súčasne pre firewally zn. FortiGate 200F vo vlastníctve verejného obstarávateľa a bezpečnostným nástrojom 1 (tzn. firewally uvedené v návrhu na plnenie kritérií. • Konfigurácia z jedného miesta - správa pravidiel firewallu, VPN, routing, SD-WAN, IDS/IPS, web filtering. • Možnosť hierarchického riadenia - rôzne úrovne administrátorských oprávnení. b. Správa viacerých sieti – ADOM (administrative domains): • Umožňuje oddelenú správu viacerých prostredí (pobočky, regionálne siete).	Funkčná špecifikácia a. Centralizovaná správa zariadení: • Jednotná správa politiky bezpečnosti súčasne pre firewally zn. FortiGate 200F vo vlastníctve verejného obstarávateľa a bezpečnostným nástrojom 1 (tzn. firewally uvedené v návrhu na plnenie kritérií. • Konfigurácia z jedného miesta - správa pravidiel firewallu, VPN, routing, SD-WAN, IDS/IPS, web filtering. • Možnosť hierarchického riadenia - rôzne úrovne administrátorských oprávnení. b. Správa viacerých sieti – ADOM (administrative domains): • Umožňuje oddelenú správu viacerých prostredí (pobočky, regionálne siete). • Každý ADOM môže mať vlastné politiky a konfigurácie. c. Automatizovaná konfigurácia a šablóny politík: • Konfigurácia Firewallov pomocou šablón (štandardizácia nastavení). • Automatické nasadenie politiky na viacero zariadení súčasne. d. SD-WAN Manažment (riadenie sieťového prenosu): • Centralizované riadenie SD-WAN pre optimalizáciu sieťového prenosu.	

• Každý ADOM môže mať vlastné politiky a konfigurácie. c. Automatizovaná konfigurácia a šablóny politík: • Konfigurácia Firewallov pomocou šablón (štandardizácia nastavení). • Automatické nasadenie politiky na viacero zariadení súčasne. d. SD-WAN Manažment (riadenie sieťového prenosu): • Centralizované riadenie SD-WAN pre optimalizáciu sieťového prenosu. • Monitorovanie kvality linky (latencia, jitter, packet loss). • Dynamický výber najlepšej trasy. e. Logging, monitoring a reporting: • Zhromažďovanie logov z firewallov zn. Fortigate 200F vo vlastníctve verejného obstarávateľa a bezpečnostným nástrojom 1 (tzn. firewally uvedené v návrhu na plnenie kritérií. f. Zálohovanie a verzionovanie konfigurácie: • Automatické zálohovanie konfigurácií spravovaných firewallov. • Možnosť vrátiť sa k predchádzajúcim konfiguráciám (versioning). • Obnova konfigurácie pri havárii alebo nesprávnej zmene. g. Zero-Touch deployment (ZTD): • Automatické nasadenie nových a už spravovaných zariadení bez manuálnej konfigurácie. • Možnosť jednoduchého nasadenia firewallov v pobočkách bez technickej podpory na mieste. h. API a automatizácia (API & scripts): • REST API pre integráciu s externými systémami. • Možnosť automatizovať konfiguráciu firewallov pomocou skriptov (min. Python, Ansible, Terraform).	• Monitorovanie kvality linky (latencia, jitter, packet loss). • Dynamický výber najlepšej trasy. e. Logging, monitoring a reporting: • Zhromažďovanie logov z firewallov zn. Fortigate 200F vo vlastníctve verejného obstarávateľa a bezpečnostným nástrojom 1 (tzn. firewally uvedené v návrhu na plnenie kritérií. f. Zálohovanie a verzionovanie konfigurácie: • Automatické zálohovanie konfigurácií spravovaných firewallov. • Možnosť vrátiť sa k predchádzajúcim konfiguráciám (versioning). • Obnova konfigurácie pri havárii alebo nesprávnej zmene. g. Zero-Touch deployment (ZTD): • Automatické nasadenie nových a už spravovaných zariadení bez manuálnej konfigurácie. • Možnosť jednoduchého nasadenia firewallov v pobočkách bez technickej podpory na mieste. h. API a automatizácia (API & scripts): • REST API pre integráciu s externými systémami. • Možnosť automatizovať konfiguráciu firewallov pomocou skriptov (min. Python, Ansible, Terraform).	
Licencia a podpora a. Podpora od výrobcu a riešenie tiketov, s dostupnosťou 7/24/365 po dobu 24 mesiacov. b. Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou nefunkčného komponentu do 24 hod. po dobu 24 mesiacov.	• FC1-10-M3004-248-02-12, FortiManager VM, SW podpora, FortiCare Premium (1-10) 1YR • https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-forticare.pdf Licencia a podpora • Podpora od výrobcu a riešenie tiketov, s dostupnosťou 7/24/365 po dobu 24 mesiacov. • Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou nefunkčného komponentu do 24 hod. po dobu 24 mesiacov.	✓ ŽoV č. 2 Vysvetlenie akceptované

c. Prístup softvérovým aktualizáciám po dobu 24 mesiacov.	• Prístup softvérovým aktualizáciám po dobu 24 mesiacov.	

Informácia pre uchádzača: Požiadavky spĺňa napríklad riešenie zn. **Fortinet**, typ **FortiManager Virtual Appliances FMG-VM-Base** vrátane podpory **FortiCare Premium Support FC1-10-M3004-248-02-XX** (XX = zvolená dĺžka licencie)**.**

Server typ 1
(Serverová infraštruktúra pre lokality pre virtualizáciu)

Verejný obstarávateľ požaduje dodanie serverovej infraštruktúry pre lokality, ktorá spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia a. Procesory: • 1 ks osadeného CPU, s parametrami min. 32 jadier s frekvenciou min. 2,7 GHz (pozn. Verejný obstarávateľ bude akceptovať aj konfiguráciu s osadením 2 socketov, každý so 16-jadrovými CPU). • Server má mať možnosť rozšíriť počet CPU na 2 ks. b. Pamäť (RAM): • 5 ks 32 GB DDR5 pamäťových modulov osadených v serveri. • Podpora až 24 DIMM slotov. • Možnosť rozšírenia až na 6 TB. c. Úložný priestor: • Šasi servera formátu 2U kvôli možnosti v budúcnosti rozšíriť interné diskové pole s kapacitou minimálne 30 ks 2,5" SSD diskov. • RAID radič. • 6 ks 480 GB SSD diskov v RAID6. • Podpora hot-swap diskov. d. Rozhranie a konektivita: • 1 ks sieťová karta s 2 ks 1 Gb. • 1 ks dedikovaný port pre správu (Management Port). e. Napájanie: • 2 ks 1100 W Redundantne napájaných zdrojov prípadne aj viac ako 1100 W pokiaľ to hardvérová konfigurácia bude vyžadovať s tým, že do rezervy kapacity je potrebné zarátať zapojenie druhého rovnakého procesora a zdvojnásobenie počtu RAM pamäte. f. Správa a zabezpečenie: • Podpora technológie AMD Infinity Guard pre zabezpečenie dát, prípadne Intel Software Guard Extensions (SGX) alebo ich ekvivalent v závislosti od výrobcu procesora obsiahnutého v dodávanom serveri.	HPE ProLiant DL385 Gen11 (3 ks) - HPE ProLiant DL385 Gen11 QuickSpecs a. Procesory: • 1x AMD EPYC 9334 2.7GHz 32-core => 1 ks osadeného CPU, s parametrami min. 32 jadier s frekvenciou min. 2,7 GHz • možnosť rozšíriť počet CPU na 2 ks b. Pamäť (RAM): • 6 ks 32GB DDR5-4800 pamäťových modulov osadených v serveri • Podpora 24 DIMM slotov. • Možnosť rozšírenia až na 6 TB použitím 256GB pamäťových modulov. c. Úložný priestor: • Šasi servera formátu 2U s možnosťou v budúcnosti rozšíriť interné diskové pole na 32 ks 2,5" SSD diskov • RAID radič HPE MR416i-o Gen11 8GB Cache • 6 ks 480GB SATA 6G Read Intensive SSD diskov v RAID6 • Podpora hot-swap diskov d. Rozhranie a konektivita: • 1 ks sieťová karta Broadcom BCM5719 Ethernet 1Gb 4-port BASE-T Adapter • 1 ks HPE iLO Advanced - dedikovaný port pre správu (Management Port) e. Napájanie: • 2 ks 1800W Redundantne napájaných zdrojov, ktoré umožňujú zapojenie druhého rovnakého procesora a zdvojnásobenie počtu RAM pamäte f. Správa a zabezpečenie: • Podpora technológie AMD Infinity Guard pre zabezpečenie dát. • Integrovaný systém správy HPE OneView (funkčný ekvivalent Lenovo XClarity Controller v navrhovanom modeli serveru) • Možnosť vzdialenej aktualizácie firmvéru, monitorovania systému a konfigurácie bez fyzického prístupu k serveru prostredníctvom HPE iLO Advanced. • TPM 2.0.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

• Integrovaný systém správy Lenovo XClarity Controller alebo jeho ekvivalent pri inom ako navrhovanom modeli serveru. • Možnosť vzdialenej aktualizácie firmvéru, monitorovania systému a konfigurácie bez fyzického prístupu k serveru. • TPM 2.0 pre zabezpečenie hardvéru. g. Server podporuje: • Podpora virtualizačných riešení (VMware, Hyper-V, KVM). • Kompatibilita s operačnými systémami Windows Server, Linux red hat.	g. Server podporuje: • Podpora virtualizačných riešení (VMware, Hyper-V, KVM,). • Kompatibilita s operačnými systémami Windows Server, Linux Red Hat.	
Podpora • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, pozn. minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov. • Spôsob poskytovania podpory – servis priamo na mieste u obstarávateľa. • Reakčný čas: 8 x 5 v nasledujúci pracovný deň (NBD) počas bežných pracovných hodín (9:00 až 17:00 hod.).	HPE 3Y Tech Care Basic Service: • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov. • Spôsob poskytovania podpory – servis priamo na mieste u obstarávateľa. • Reakčný čas: 8 x 5 v nasledujúci pracovný deň (NBD) počas bežných pracovných hodín (9:00 až 17:00 hod.).	
Ďalšie požiadavky • Server nemôže byť repasovaný. • Daný typ servera nebol uvedený na trh skôr ako v roku 2022. • Daný typ servera nemôže mať uvedený end of support alebo end of sale. • Server musí byť certifikovaný podľa Energy Star. • Server musí mať minimálne certifikáciu EPEAT Silver. • Server musí spĺňať požiadavky EU lot 9. • Server musí mať modulárnu konštrukciu umožňujúcu výmenu komponentov.	• Server nie je repasovaný. • Daný typ servera bol uvedený na trh v roku 2022. • Daný typ servera nemá uvedený end of support a end of sale. • Server je certifikovaný podľa Energy Star – HPE ProLiant DL385 Gen11 QuickSpecs • Server má certifikáciu EPEAT Silver - HPE ProLiant DL385 Gen11 Server | EPEAT Registry • Server spĺňa požiadavky EU lot 9 - HPE ProLiant DL385 Gen11 QuickSpecs Server má modulárnu konštrukciu umožňujúcu výmenu komponentov.	

Informácia pre uchádzača: Požiadavky spĺňa napríklad riešenie zn. **Lenovo**, typ **Lenovo ThinkSystem SR665 V3** vrátane podpory **Lenovo Server Foundation NBD.**

Server typ 2
(Core serverová infraštruktúra pre virtualizáciu)

Verejný obstarávateľ požaduje dodanie serverovej infraštruktúry pre core infraštruktúru, ktorá spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia a. Procesory: • 1 ks osadeného CPU, s parametrami min. 48 jadier s frekvenciou min. 2,7 GHz. • Server má mať možnosť rozšíriť počet CPU na 2 ks. b. Pamäť (RAM): • 8 ks 64 GB DDR5 pamäťových modulov osadených v serveri • Podpora až 24 DIMM slotov. • Možnosť rozšírenia až na 6 TB. c. Úložný priestor: • 2 ks 240 GB SSD diskov v RAID1 pre operačný systém. • Podpora hot-swap diskov. d. Rozhranie a konektivita: • 1 ks sieťová karta s 2 ks 25/10 Gb portami, osadená s 2 ks 10 Gb optickými prevodníkmi. • 1 ks fibre channel karta s 2 ks 32 Gb portami s 2 ks osadenými 32 Gb optickými prevodníkmi. • 1 ks dedikovaný port pre správu (Management Port). e. Napájanie: 2 ks 1100 W Redundantne napájaných zdrojov. f. Správa a zabezpečenie**:** • Podpora technológie AMD Infinity Guard pre zabezpečenie dát, prípadne Intel Software Guard Extensions (SGX) alebo ich ekvivalent v závislosti od výrobcu procesora obsiahnutého v dodávanom serveri. • Integrovaný systém správy Lenovo XClarity Controller alebo jeho ekvivalent pri inom ako navrhovanom modeli serveru. • Možnosť vzdialenej aktualizácie firmvéru, monitorovania systému a konfigurácie bez fyzického prístupu k serveru. • TPM 2.0 pre zabezpečenie hardvéru. g. Server podporuje: • Podpora virtualizačných riešení (VMware, Hyper-V, KVM). • Kompatibilita s operačnými systémami Windows Server, Linux red hat.	HPE ProLiant DL385 Gen11 (3 ks) - HPE ProLiant DL385 Gen11 QuickSpecs a. Procesory: • 1x ks AMD EPYC 9454 2.75GHz 48-core => 1ks osadeného CPU, s parametrami min. 48 jadier s frekvenciou min. 2,7 GHz • možnosť rozšíriť počet CPU na 2 ks b. Pamäť (RAM): • 8 ks 64 GB DDR5-4800 pamäťových modulov osadených v serveri • Podpora 24 DIMM slotov. • Možnosť rozšírenia až na 6 TB použitím 256GB pamäťových modulov. c. Úložný priestor: • 2 ks 480 GB SATA 6G Read Intensive SSD diskov v RAID1 pre operačný systém • Podpora hot-swap diskov d. Rozhranie a konektivita: • 1 ks sieťová karta Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 s 2 ks 25/10 Gb portami, osadená s 2 ks 10 Gb optickými prevodníkmi • 1 ks fibre channel karta HPE SN1610Q 32Gb 2-port Fibre Channel Host Bus Adapter s 2 ks 32 Gb portami s 2 ks osadenými 32 Gb optickými prevodníkmi • 1 ks HPE iLO Advanced - dedikovaný port pre správu (Management Port) e. Napájanie: • 2 ks 1800W Redundantne napájaných zdrojov f. Správa a zabezpečenie: • Podpora technológie AMD Infinity Guard pre zabezpečenie dát. • Integrovaný systém správy HPE OneView (funkčný ekvivalent Lenovo XClarity Controller v navrhovanom modeli serveru) • Možnosť vzdialenej aktualizácie firmvéru, monitorovania systému a konfigurácie bez fyzického prístupu k serveru prostredníctvom HPE iLO Advanced. • TPM 2.0. g. Server podporuje: • Podpora virtualizačných riešení (VMware, Hyper-V, KVM,). • Kompatibilita s operačnými systémami Windows Server, Linux Red Hat.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

Podpora • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, pozn. minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov. • Spôsob poskytovania podpory – servis priamo na mieste u obstarávateľa. • Reakčný čas: 8 x 5 v nasledujúci pracovný deň (NBD) počas bežných pracovných hodín (9:00 až 17:00 hod.).	HPE 3Y Tech Care Basic Service: • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov. • Spôsob poskytovania podpory – servis priamo na mieste u obstarávateľa. • Reakčný čas: 8 x 5 v nasledujúci pracovný deň (NBD) počas bežných pracovných hodín (9:00 až 17:00 hod.).	
Ďalšie požiadavky • Server nemôže byť repasovaný. • Daný typ servera nebol uvedený na trh skôr ako v roku 2022. • Daný typ servera nemôže mať uvedený end of support alebo end of sale. • Server musí byť certifikovaný podľa Energy Star. • Server musí mať minimálne certifikáciu EPEAT Silver. • Server musí spĺňať požiadavky EU lot 9. • Server musí mať modulárnu konštrukciu umožňujúcu výmenu komponentov.	• Server nie je repasovaný. • Daný typ servera bol uvedený na trh v roku 2022. • Daný typ servera nemá uvedený end of support a end of sale. • Server je certifikovaný podľa Energy Star –HPE ProLiant DL385 Gen11 QuickSpecs • Server má certifikáciu EPEAT Silver - HPE ProLiant DL385 Gen11 Server | EPEAT Registry • Server spĺňa požiadavky EU lot 9 – HPE ProLiant DL385 Gen11 QuickSpecs • Server má modulárnu konštrukciu umožňujúcu výmenu komponentov.	

Informácia pre uchádzača: Požiadavky spĺňa napríklad riešenie zn. **Lenovo**, typ **Lenovo ThinkSystem SR665 V3** vrátane podpory **Lenovo Server Foundation NBD.**

Server typ 3
(Core úložisková infraštruktúra)

Verejný obstarávateľ požaduje dodanie core úložiskovej infraštruktúry (diskové pole), ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia a. Vlastnosti: • Diskové pole s dvomi radičmi v režime active-active. • Použitie hardvérovej kompresie dát bez dopadu na výkon. b. Konektivita: • 2 ks - fibre channel kariet so 4 ks 32 GB portov pre pripojenie serverov na priamo, bez nutnosti FC prepínačov (direct attach), s osadenými 4 ks v každej karte 32 GB optických prevodníkov. • 2 ks - sieťová karta s 2 ks 25/10 GB LAN portami s osadenými 2 ks v každej karte 10 GB optickými prevodníkmi. c. Kapacita: • Osadený počet diskov o kapacite minimálne 35 TiB čistej využiteľnej kapacity na NVMe flash diskoch v RAID6 spolu s distribuovaným hot spare priestorom s kapacitou jedného disku. d. Výkon: • Vyrovnávacia pamäť aspoň 256 GB. • Bandwidth aspoň 25 GB/s. • Latencia menej ako 1 milisekunda v bežnej prevádzke, latencia menej ako 50 mikrosekúnd v rámci načítavania z cash pamäte. • Schopnosť spracovávať aspoň 500 000 IOPS. e. Zabezpečenie: • Možnosť šifrovania dát na úrovni úložiska (Data-at-Rest Encryption). • Možnosť vytvárania tzv. immutable snapshotov (nemazateľné, needitovateľné), pre ochranu pri ransomware útokoch. • Detekcia a hlásenie podozrivej prevádzky na diskoch (detekcia ransomware útokov). f. Škálovateľnosť: • Podpora rozšírenia do clustrovanej konfigurácie na zvýšenie výkonu a redundancie.	HPE Alletra MP B10130 (1 ks) - HPE Alletra Storage MP B10000 QuickSpecs a. Vlastnosti: • Diskové pole s dvomi radičmi v režime active-active. • Použitie hardvérovej kompresie dát bez dopadu na výkon. b. Konektivita: • 4 ks - fibre channel kariet so 4 ks 32 GB portov pre pripojenie serverov na priamo, bez nutnosti FC prepínačov (direct attach), s osadenými 4 ks v každej karte 32 GB SW optických prevodníkov. • 2 ks - sieťová karta s 2 ks 25/10 GB LAN portami s osadenými 2 ks v každej karte 10 GB SR optickými prevodníkmi. c. Kapacita: • Osadený počet diskov o kapacite 39.35 TiB čistej využiteľnej kapacity na NVMe flash diskoch v RAID6 spolu s distribuovaným hot spare priestorom s kapacitou jedného disku. d. Výkon: • Vyrovnávacia pamäť 512 GB. • Bandwidth 28 GB/s. • Latencia menej ako 1 milisekunda v bežnej prevádzke, latencia menej ako 50 mikrosekúnd v rámci načítavania z cash pamäte. • Schopnosť spracovávať 550 000 IOPS. e. Zabezpečenie: • Možnosť šifrovania dát na úrovni úložiska (Data-at-Rest Encryption) - Storage Data Encryption. • Možnosť vytvárania tzv. immutable snapshotov (nemazateľné, needitovateľné), pre ochranu pri ransomware útokoch – virtual lock. • Detekcia a hlásenie podozrivej prevádzky na diskoch (detekcia ransomware útokov) - real-time ransomware detection. f. Škálovateľnosť: Podpora rozšírenia do clustrovanej konfigurácie na zvýšenie výkonu a redundancie – peer persistence.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované
Podpora • Hardvérová údržba s rozšírenou reakčnou dobou zabezpečujúca opravy na mieste v ten istý deň, 24 hodín denne, 7 dní v týždni. • Podpora prostredníctvom Support Line formou technickej asistencie pri otázkach týkajúcich sa používania, inštalácie a	HPE 3Y Tech Care Critical Service • Hardvérová údržba s rozšírenou reakčnou dobou zabezpečujúca opravy do 6 hodín od nahlásenia, 24 hodín denne, 7 dní v týždni.	

kompatibility produktov, riešenie problémov súvisiacich s interoperabilitou systémov. • Predíktívna podpora formou automatického generovania upozornení na potenciálne problémy a návrhy na preventívne opatrenia. • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, pozn. minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov.	• Podpora prostredníctvom Support Line formou technickej asistencie pri otázkach týkajúcich sa používania, inštalácie a kompatibility produktov, riešenie problémov súvisiacich s interoperabilitou systémov. • Predíktívna podpora formou automatického generovania upozornení na potenciálne problémy a návrhy na preventívne opatrenia. • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov.	
Ďalšie požiadavky • Diskové pole nemôže byť repasované. • Daný typ diskového poľa nebol uvedený na trh skôr ako v roku 2022. • Daný typ diskového nemôže mať uvedený end of support alebo end of sale. • Server musí byť certifikovaný podľa Energy Star. • Server musí spĺňať požiadavky EU lot 9. • Server musí mať modulárnu konštrukciu umožňujúcu výmenu komponentov.	• Diskové pole nie je repasované. • Daný typ diskového poľa bol uvedený na trh v roku 2023. • Daný typ diskového poľa nemá uvedený end of support alebo end of sale. • Diskové pole je certifikované podľa Energy Star. - HPE Alletra Storage MP B10000 QuickSpecs • Diskové pole spĺňa požiadavky EU lot 9. - HPE Alletra Storage MP B10000 QuickSpecs • Diskové pole má modulárnu konštrukciu umožňujúcu výmenu komponentov.	

Informácia pre uchádzača: Požiadavky spĺňa napríklad riešenie zn. **IBM**, typ **IBM Storage FlashSystem 5300** s supportom označeným ako **IBM Storage Expert Care Advanced, 24hr.**

Server typ 4
(Core serverová infraštruktúra bez virtualizácie)

Verejný obstarávateľ požaduje dodanie serverovej infraštruktúry pre core infraštruktúru, ktorá spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia a. Procesory: • 1 ks osadeného CPU, s parametrami min. 16 jadier s frekvenciou min. 2,7 GHz. • Server má mať možnosť rozšíriť počet CPU na 2 ks. b. Pamäť (RAM): • 3 ks 16 GB DDR5 pamäťových modulov osadených v serveri • Úložný priestor: • Šasi servera vo formáte 1U. • 2 ks 240 GB SSD diskov v RAID1. • Podpora hot-swap diskov. c. Rozhranie a konektivita: • 1 ks sieťová karta s 2 ks 25/10 Gb portami, osadená s 2 ks 10 GB optickými prevodníkmi. • 1 ks dedikovaný port pre správu (Management Port). d. Napájanie: 2 ks Redundantne napájaných zdrojov, z ktorých každý plne pokryje celkovú spotrebu energie všetkých komponentov nachádzajúcich sa v navrhovanom serveri spolu s dostatočnou rezervou pre prípad pripojenia rovnakého CPU do voľného socketu a navýšenie RAM na dvojnásobok vyššie uvedenej kapacity. e. Správa a zabezpečenie: • Podpora technológie AMD Infinity Guard pre zabezpečenie dát, prípadne Intel Software Guard Extensions (SGX) alebo ich ekvivalent v závislosti od výrobcu procesora obsiahnutého v dodávanom serveri. • Integrovaný systém správy Lenovo XClarity Controller alebo jeho ekvivalent pri inom ako navrhovanom modeli serveru. • Možnosť vzdialenej aktualizácie firmvéru, monitorovania systému a konfigurácie bez fyzického prístupu k serveru. • TPM 2.0 pre zabezpečenie hardvéru. f. Server podporuje: • Kompatibilita s operačnými systémami Windows Server, Linux red hat.	HPE ProLiant DL365 Gen11 (2 ks) - HPE ProLiant DL365 Gen11 QuickSpecs a. Procesory: • 1x AMD EPYC 9124 3.0GHz 16-core => 1 ks osadeného CPU, s parametrami min. 16 jadier s frekvenciou min. 2,7 GHz • možnosť rozšíriť počet CPU na 2 ks b. Pamäť (RAM): • 4 ks 16 GB DDR5-4800 pamäťových modulov osadených v serveri • Úložný priestor: • Šasi servera vo formáte 1U • 2 ks 480 GB SATA 6G Read Intensive SSD SSD diskov v RAID1 • Podpora hot-swap diskov c. Rozhranie a konektivita: • 1 ks sieťová karta Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 s 2 ks 25/10 Gb portami, osadená s 2 ks 10 Gb optickými prevodníkmi • 1 ks HPE iLO Advanced - dedikovaný port pre správu (Management Port) d. Napájanie: • 2 ks 1800W Redundantne napájaných zdrojov, ktoré umožňujú zapojenie druhého rovnakého procesora a zdvojnásobenie počtu RAM pamäte e. Správa a zabezpečenie: • Podpora technológie AMD Infinity Guard pre zabezpečenie dát. • Integrovaný systém správy HPE OneView (funkčný ekvivalent Lenovo XClarity Controller v navrhovanom modeli serveru) • Možnosť vzdialenej aktualizácie firmvéru, monitorovania systému a konfigurácie bez fyzického prístupu k serveru prostredníctvom HPE iLO Advanced. • TPM 2.0. f. Server podporuje: • Kompatibilita s operačnými systémami Windows Server, Linux Red Hat.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

Podpora • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, pozn. minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov. • Spôsob poskytovania podpory – servis priamo na mieste u obstarávateľa. • Reakčný čas: 8 x 5 v nasledujúci pracovný deň (NBD) počas bežných pracovných hodín (9:00 až 17:00 hod.).	HPE 3Y Tech Care Basic Service: • Typ služby - Rozšírená servisná podpora zahŕňajúca opravy a výmenu dielov vrátane práce technika. • Dĺžka trvania podpory – 3 roky, minimálna garantovaná dĺžka životného cyklu podpory výrobcu od dodania - 5 rokov. • Spôsob poskytovania podpory – servis priamo na mieste u obstarávateľa. • Reakčný čas: 8 x 5 v nasledujúci pracovný deň (NBD) počas bežných pracovných hodín (9:00 až 17:00 hod.).	
Ďalšie požiadavky • Server nemôže byť repasovaný. • Daný typ servera nebol uvedený na trh skôr ako v roku 2022. • Daný typ servera nemôže mať uvedený end of support alebo end of sale. • Server musí byť certifikovaný podľa Energy Star. • Server musí mať minimálne certifikáciu EPEAT Silver. • Server musí spĺňať požiadavky EU lot 9. • Server musí mať modulárnu konštrukciu umožňujúcu výmenu komponentov.	• Server nie je repasovaný. • Daný typ servera bol uvedený na trh v roku 2022. • Daný typ servera nemá uvedený end of support a end of sale. • Server je certifikovaný podľa Energy Star - HPE ProLiant DL365 Gen11 QuickSpecs • Server má certifikáciu EPEAT Silver - HPE ProLiant DL365 Gen11 Server | EPEAT Registry • Server spĺňa požiadavky EU lot 9 - HPE ProLiant DL365 Gen11 QuickSpecs • Server má modulárnu konštrukciu umožňujúcu výmenu komponentov.	

Informácia pre uchádzača: Požiadavky spĺňa napríklad riešenie zn. **Lenovo**, typ **Lenovo ThinkSystem SR645 V3** vrátane podpory **Lenovo Server Foundation NBD.**

Systém 1

(Virtualizačná platforma)

Verejný obstarávateľ požaduje dodanie virtualizačnej platformy zn. Broadcom (v minulosti VMware), typ VMware vSphere Standard vo verzii 8 alebo novšej, ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:**: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia Súčasťou licencie je vSphere Hypervisor (ESXi), vCenter Standard a podpora 24/7. Kľúčové vlastnosti: a. Administratívne služby a inteligentné riadenie operácií • Služba správy životného cyklu vCenter - Zjednodušuje správu životného cyklu inštancií vCenter jedným kliknutím. Skracuje čas údržby, čo umožňuje ľahšie plánovať aktualizácie a rýchlejší prístup k novým funkciám. b. Zjednodušené operácie • vSphere Lifecycle Manager - Spravujte infraštruktúrne obrazy na záplaty, aktualizácie alebo upgrady klastrov VMware ESX pomocou modelu požadovaného stavu. • vCenter Server Profiles - Funkcie správy konfigurácie požadovaného stavu pre vCenter Server. Pomáha používateľom definovať, overovať a aplikovať konfigurácie na viacero serverov vCenter. • vCenter Server Update Planner - Spravujte kompatibilitu a interoperabilitu pre scenáre aktualizácie vCenter Server. Umožňuje používateľom generovať správy o interoperabilite a kontrolách, ktoré im pomáhajú plánovať aktualizácie. • Content Library - Pridaná administratívna kontrola a podpora verzovania. Poskytuje jednoduchú a efektívnu centralizovanú správu šablón virtuálnych strojov, virtuálnych zariadení, ISO obrazov a skriptov. • Virtual Volumes™ - Virtualizuje externé úložiská (SAN a NAS) a poskytuje správu úložiska orientovanú na virtuálne stroje na základe politík cez vCenter.	Technická špecifikácia Broadcom VMware Cloud Foundation (240 jadier) https://www.vmware.com/docs/datasheet-vmware-cloud-foundation-9-0 Súčasťou licencie je vSphere Hypervisor (ESXi), vCenter Standard a podpora 24/7. Kľúčové vlastnosti: a. Administratívne služby a inteligentné riadenie operácií • Služba správy životného cyklu vCenter - Zjednodušuje správu životného cyklu inštancií vCenter jedným kliknutím. Skracuje čas údržby, čo umožňuje ľahšie plánovať aktualizácie a rýchlejší prístup k novým funkciám. b. Zjednodušené operácie • vSphere Lifecycle Manager - Spravujte infraštruktúrne obrazy na záplaty, aktualizácie alebo upgrady klastrov VMware ESX pomocou modelu požadovaného stavu. • vCenter Server Profiles - Funkcie správy konfigurácie požadovaného stavu pre vCenter Server. Pomáha používateľom definovať, overovať a aplikovať konfigurácie na viacero serverov vCenter. • vCenter Server Update Planner - Spravujte kompatibilitu a interoperabilitu pre scenáre aktualizácie vCenter Server. Umožňuje používateľom generovať správy o interoperabilite a kontrolách, ktoré im pomáhajú plánovať aktualizácie. • Content Library - Pridaná administratívna kontrola a podpora verzovania. Poskytuje jednoduchú a efektívnu centralizovanú správu šablón virtuálnych strojov, virtuálnych zariadení, ISO obrazov a skriptov. • Virtual Volumes™ - Virtualizuje externé úložiská (SAN a NAS) a poskytuje správu úložiska orientovanú na virtuálne stroje na základe politík cez vCenter.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

• Live Patching for ESX - Komponenty ESX, VMware nástroje a bezpečnostné záplaty je možné aplikovať bez reštartu alebo evakuácie VM, čím sa znižuje čas nečinnosti. c. Zabudovaná bezpečnosť • Identity Federation - Pripojenie k Microsoft Active Directory, Microsoft Active Directory Federation Services (AD FS), Microsoft Entra ID, Okta a PingFederate na centralizovanú autentifikáciu a multifaktorovú autentifikáciu. • Trusted Platform Module Support - Podpora TPM 2.0 pridáva hardvérové bezpečnostné ochrany do hypervízora. • Virtual TPM - Pridáva virtuálny TPM 2.0 do virtuálnych strojov, čím umožňuje bezpečnostné funkcie v hosťujúcom systéme. • FIPS 140-2, 140-3 a Common Criteria Certification - Tretia strana overuje kryptografické algoritmy a bezpečnosť vo vnútri hypervízora. • TLS 1.2 a 1.3 - Moderné ochrany kryptografie pre dáta počas prenosu. • Standard Key Provider - Ukladanie kryptografických kľúčov pre vTPM, šifrovanie VM a šifrovanie dát v pokoji v systéme KMS pomocou protokolu KMIP. • Native Key Provider - Umožňuje vTPM a ďalšie ochrany dát v pokoji natívne v rámci vSphere. • Podpora pre Microsoft Virtualization-Based Security (VBS) - Umožňuje ochranu hosťujúcich systémov, ako sú Device Guard a Credential Guard, na operačných systémoch Microsoft Windows. d. Výkon aplikácií • Storage Policy-Based Management - Umožňuje spoločnú správu medzi úložiskovými vrstvami a dynamickú automatizáciu triedy služieb úložiska prostredníctvom kontrolnej roviny na základe politík. • Dynamic DirectPath IO - Podpora pre vGPU a DirectPath I/O pri počiatočnom umiestnení virtuálnych strojov. e. Kontinuita podnikania • vSphere ESX Hypervisor - Poskytuje robustnú, produkčne overenú, vysokovýkonnú virtualizačnú vrstvu. • vSphere vMotion - Umožňuje živú migráciu virtuálnych strojov bez prerušenia používateľov alebo straty služby, čo eliminuje potrebu plánovania prestojov aplikácií pre plánovanú údržbu serverov.	• Live Patching for ESX - Komponenty ESX, VMware nástroje a bezpečnostné záplaty je možné aplikovať bez reštartu alebo evakuácie VM, čím sa znižuje čas nečinnosti. c. Zabudovaná bezpečnosť • Identity Federation - Pripojenie k Microsoft Active Directory, Microsoft Active Directory Federation Services (AD FS), Microsoft Entra ID, Okta a PingFederate na centralizovanú autentifikáciu a multifaktorovú autentifikáciu. • Trusted Platform Module Support - Podpora TPM 2.0 pridáva hardvérové bezpečnostné ochrany do hypervízora. • Virtual TPM - Pridáva virtuálny TPM 2.0 do virtuálnych strojov, čím umožňuje bezpečnostné funkcie v hosťujúcom systéme. • FIPS 140-2, 140-3 a Common Criteria Certification - Tretia strana overuje kryptografické algoritmy a bezpečnosť vo vnútri hypervízora. • TLS 1.2 a 1.3 - Moderné ochrany kryptografie pre dáta počas prenosu. • Standard Key Provider - Ukladanie kryptografických kľúčov pre vTPM, šifrovanie VM a šifrovanie dát v pokoji v systéme KMS pomocou protokolu KMIP. • Native Key Provider - Umožňuje vTPM a ďalšie ochrany dát v pokoji natívne v rámci vSphere. • Podpora pre Microsoft Virtualization-Based Security (VBS) - Umožňuje ochranu hosťujúcich systémov, ako sú Device Guard a Credential Guard, na operačných systémoch Microsoft Windows. d. Výkon aplikácií • Storage Policy-Based Management - Umožňuje spoločnú správu medzi úložiskovými vrstvami a dynamickú automatizáciu triedy služieb úložiska prostredníctvom kontrolnej roviny na základe politík. • Dynamic DirectPath IO - Podpora pre vGPU a DirectPath I/O pri počiatočnom umiestnení virtuálnych strojov. e. Kontinuita podnikania • vSphere ESX Hypervisor - Poskytuje robustnú, produkčne overenú, vysokovýkonnú virtualizačnú vrstvu. • vSphere vMotion - Umožňuje živú migráciu virtuálnych strojov bez prerušenia používateľov alebo straty služby, čo eliminuje potrebu plánovania prestojov aplikácií pre plánovanú údržbu serverov.	

• vCenter Hybrid Linked Mode - Umožňuje jednotnú viditeľnosť a správu naprieč lokálnymi vCenter a vCenter v cloude na báze vSphere, ako je VMware Cloud na AWS. • VSMP - Virtuálny symetrický multiprocessing (SMP) umožňuje virtuálnym strojom mať viacero virtuálnych procesorov. • High Availability (HA) - Automaticky reštartuje vaše virtuálne stroje po zlyhaní fyzického stroja. • Storage vMotion - Vyhýba sa prestojom aplikácií počas plánovanej údržby úložísk migráciou diskových súborov virtuálnych strojov medzi úložiskovými poľami. • Fault Tolerance - Poskytuje nepretržitú dostupnosť akejkoľvek aplikácie v prípade zlyhania hardvéru—bez straty dát alebo prestojov pre pracovné zaťaženia až do 8 vCPU. • vSphere Replication™ - Umožňuje efektívnu, na poli nezávislú replikáciu dát virtuálnych strojov cez LAN alebo WAN a zjednodušuje správu umožnením replikácie na úrovni virtuálneho stroja. • Podpora pre 4K Native Storage - Zvyšuje škálovateľnosť platformy využívaním vysokokapacitných diskov. Znižuje CAPEX. • vSphere Quick Boot™ - Preskakuje kroky inicializácie hardvéru a dramaticky znižuje čas potrebný na záplaty a aktualizácie. • vCenter High Availability (vCenter HA) - Automaticky reštartuje vaše virtuálne stroje po zlyhaní fyzického stroja. • vCenter Backup and Restore - Nativná záloha a obnova servera vCenter. • vCenter Server Appliance™ Migration - Nástroj na migráciu a aktualizáciu existujúcich Windows inštalácií vCenter do vCenter Server Appliance jedným krokom. f. Hybridné cloudové možnosti • Cross vCenter Mixed Version Provisioning - Používajte rôzne verzie vCenter naprieč lokálnymi a verejnými cloudovými prostrediami na báze vSphere, pričom umožňujú pokračovanie v operačných úlohách, ako sú vMotion, Full Clone a Cold Migrate. • Hot and Cold Migration to the Cloud - Podpora pre horúcu aj studenú migráciu pracovných zaťažení naprieč hybridným cloudom.	• vCenter Hybrid Linked Mode - Umožňuje jednotnú viditeľnosť a správu naprieč lokálnymi vCenter a vCenter v cloude na báze vSphere, ako je VMware Cloud na AWS. • VSMP - Virtuálny symetrický multiprocessing (SMP) umožňuje virtuálnym strojom mať viacero virtuálnych procesorov. • High Availability (HA) - Automaticky reštartuje vaše virtuálne stroje po zlyhaní fyzického stroja. • Storage vMotion - Vyhýba sa prestojom aplikácií počas plánovanej údržby úložísk migráciou diskových súborov virtuálnych strojov medzi úložiskovými poľami. • Fault Tolerance - Poskytuje nepretržitú dostupnosť akejkoľvek aplikácie v prípade zlyhania hardvéru—bez straty dát alebo prestojov pre pracovné zaťaženia až do 2 vCPU. • vSphere Replication™ - Umožňuje efektívnu, na poli nezávislú replikáciu dát virtuálnych strojov cez LAN alebo WAN a zjednodušuje správu umožnením replikácie na úrovni virtuálneho stroja. • Podpora pre 4K Native Storage - Zvyšuje škálovateľnosť platformy využívaním vysokokapacitných diskov. Znižuje CAPEX. • vSphere Quick Boot™ - Preskakuje kroky inicializácie hardvéru a dramaticky znižuje čas potrebný na záplaty a aktualizácie. • vCenter High Availability (vCenter HA) - Automaticky reštartuje vaše virtuálne stroje po zlyhaní fyzického stroja. • vCenter Backup and Restore - Nativná záloha a obnova servera vCenter. • vCenter Server Appliance™ Migration - Nástroj na migráciu a aktualizáciu existujúcich Windows inštalácií vCenter do vCenter Server Appliance jedným krokom. f. Hybridné cloudové možnosti • Cross vCenter Mixed Version Provisioning - Používajte rôzne verzie vCenter naprieč lokálnymi a verejnými cloudovými prostrediami na báze vSphere, pričom umožňujú pokračovanie v operačných úlohách, ako sú vMotion, Full Clone a Cold Migrate. • Hot and Cold Migration to the Cloud - Podpora pre horúcu aj studenú migráciu pracovných zaťažení naprieč hybridným cloudom	

Systém 2
(Operačný systém na báze Microsoft)

Verejný obstarávateľ požaduje dodanie operačného systému pre servery na báze Microsoft, typ Microsoft Windows Server standard v najnovšej stabilnej verzii v čase predkladania ponuky (napr. verzia 2022 alebo novšia), ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAĆA č. 1**: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia a. Výkonnosť: 64-bitová architektúra a optimalizácia pre viacjadrové procesory b. Funkcionalita: • Centralizovaná správa identít, autentifikácia a autorizácia užívateľov. • Implementácia a správa Group Policy pre konfiguráciu a správu nastavení operačných systémov a aplikácií. • Replikácia a synchronizácia dát medzi doménovými kontrolérmi pre zabezpečenie vysokej dostupnosti. • Integrácia so službami DNS, DHCP a ďalšími komponentmi potrebnými pre bezproblémový chod domény. • Podpora trust vzťahov pre integráciu s inými doménami a adresárovými službami. c. Bezpečnosť: • Podpora autentifikačných mechanizmov, minimálne služby Microsoft Kerberos. • Implementácia šifrovania komunikácie (TLS) a dodržiavanie bezpečnostných štandardov (napr. FIPS).	Technická špecifikácia Microsoft Windows server 2025 (5 ks) https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/windows-server-2025-data-sheet.pdf a. Výkonnosť: 64-bitová architektúra a optimalizácia pre viacjadrové procesory b. Funkcionalita: • Centralizovaná správa identít, autentifikácia a autorizácia užívateľov. • Implementácia a správa Group Policy pre konfiguráciu a správu nastavení operačných systémov a aplikácií. • Replikácia a synchronizácia dát medzi doménovými kontrolérmi pre zabezpečenie vysokej dostupnosti. • Integrácia so službami DNS, DHCP a ďalšími komponentmi potrebnými pre bezproblémový chod domény. • Podpora trust vzťahov pre integráciu s inými doménami a adresárovými službami. c. Bezpečnosť: • Podpora autentifikačných mechanizmov, minimálne služby Microsoft Kerberos. • Implementácia šifrovania komunikácie (TLS) a dodržiavanie bezpečnostných štandardov (napr. FIPS).	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

Systém 3
(Operačný systém na báze Linux)

Verejný obstarávateľ požaduje dodanie **operačného systému pre servery na báze Linux**, typ **Red Hat Enterprise Linux for Virtual Datacenters (Standard)** v najnovšej stabilnej verzii v čase predkladania ponuky, ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAĆA č. 1**: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia a. Licencia umožňuje nasadenie na neobmedzený počet virtualizovaných prostredí. b. Licencia je podporovaná na hypervízoroch, minimálne Red Hat Virtualization, VMware a MicrosoftHyperV. c. Zahŕňa Red Hat Enterprise Linux Atomic Host. d. Funkčné požiadavky: Kompatibilita s nasledovnými softvérmi/informačnými systémami: MISP (malware information sharing platform), Elastic, Tenable security center, Nessus skener, Cyberark. e. Podpora: neobmedzená webová ako aj telefonická podpora od 9:00 do 17:00 hod. okrem víkendov a štátnych sviatkov.	Technická špecifikácia Red Hat Enterprise Linux for Virtual Datacenters (6 ks) https://www.hpe.com/psnow/doc/PSN6830277PTEN a. Licencia umožňuje nasadenie na neobmedzený počet virtualizovaných prostredí. b. Licencia je podporovaná na hypervízoroch, minimálne Red Hat Virtualization, VMware a MicrosoftHyperV. c. Zahŕňa Red Hat Enterprise Linux Atomic Host. d. Funkčné požiadavky: Kompatibilita s nasledovnými softvérmi/informačnými systémami: MISP (malware information sharing platform), Elastic, Tenable security center, Nessus skener, Cyberark. e. Podpora: neobmedzená webová ako aj telefonická podpora od 9:00 do 17:00 hod. okrem víkendov a štátnych sviatkov.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

Systém 4
(Zálohovací systém)

Verejný obstarávateľ požaduje dodanie **zálohovacieho systému VEEAM**, typ **VEEAM Data Platform Advanced Universal Subscription License** v najnovšej stabilnej verzii v čase predkladania ponuky, ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:**: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	**Poznámka**
Technická špecifikácia a. Centrálna správa záloh umožňujúca jednotné plánovanie, konfiguráciu a monitoring zálohovacích a replikačných úloh, vrátane virtualizovaných a fyzických systémov. b. Rýchla obnova podporená funkciou ako instant virtual machine recovery, granular recovery a replikácia dát. c. Optimalizácia prenosu dát použitím technológie ako deduplikácia, kompresia a WAN acceleration, ktoré znižujú nároky na šírku pásma a úložný priestor pri prenose dát medzi lokalitami a centrálnym úložiskom. d. Šifrovanie dát počas prenosu, ako aj v úložisku, ako aj tzv. immutable repository, ktoré chráni dáta neumožnením ich prepisu počas určeného časového obdobia za účelom ochrany záloh pred ransomvérom. e. Podporované prostredia: • Virtualizácia - podpora minimálne pre VMware vSphere, Microsoft Hyper-V. • Fyzické servery - zálohovanie a replikácia fyzických serverov s operačnými systémami na báze Windows a Linux. • Cloudové prostredia: Možnosť zálohovanie a replikácie dát z cloudových alebo do cloudových služieb. f. Posilnenie zálohovacích dát pomocou detekcie hrozieb v celom životnom cykle, ako je detekcia ransomvéru v reálnom čase, skenovanie indexu súborov, analýza pomocou YARA skenov a hlásenie abnormalít. g. Podpora viacfaktorovej autentifikácie min. prostredníctvom aplikácií Microsoft Authenticator a Google Authenticator. h. Architektúra podporujúca princípy Zero Trust, ako je autorizácia na princípe štyroch očí, viacfaktorová autentifikácia, nemennosť dát. Integrácia s bezpečnostnými nástrojmi a pracovnými postupmi,	Technická špecifikácia Veeam Public Sector Data Platform Advanced Universal 2-year Subscription 24x7 Support (70 ks) https://www.veeam.com/veeam_data_platform_feature_comparison_ds.pdf a. Centrálna správa záloh umožňujúca jednotné plánovanie, konfiguráciu a monitoring zálohovacích a replikačných úloh, vrátane virtualizovaných a fyzických systémov. b. Rýchla obnova podporená funkciou ako instant virtual machine recovery, granular recovery a replikácia dát. c. Optimalizácia prenosu dát použitím technológie ako deduplikácia, kompresia a WAN acceleration, ktoré znižujú nároky na šírku pásma a úložný priestor pri prenose dát medzi lokalitami a centrálnym úložiskom. d. Šifrovanie dát počas prenosu, ako aj v úložisku, ako aj tzv. immutable repository, ktoré chráni dáta neumožnením ich prepisu počas určeného časového obdobia za účelom ochrany záloh pred ransomvérom. e. Podporované prostredia: • Virtualizácia - podpora minimálne pre VMware vSphere, Microsoft Hyper-V. • Fyzické servery - zálohovanie a replikácia fyzických serverov s operačnými systémami na báze Windows a Linux. • Cloudové prostredia: Možnosť zálohovanie a replikácie dát z cloudových alebo do cloudových služieb. f. Posilnenie zálohovacích dát pomocou detekcie hrozieb v celom životnom cykle, ako je detekcia ransomvéru v reálnom čase, skenovanie indexu súborov, analýza pomocou YARA skenov a hlásenie abnormalít. g. Podpora viacfaktorovej autentifikácie min. prostredníctvom aplikácií Microsoft Authenticator a Google Authenticator. h. Architektúra podporujúca princípy Zero Trust, ako je autorizácia na princípe štyroch očí, viacfaktorová autentifikácia, nemennosť dát. Integrácia s bezpečnostnými nástrojmi a pracovnými postupmi, preposielanie udalostí cez Syslog, API pre incidenty zaznamenané zálohovacím systémom.	✓ ŽoV č. 2 Vysvetlením doplnené akceptované

preposielanie udalostí cez Syslog, API pre incidenty zaznamenané zálohovacím systémom. i. Produkčná podpora 24/7.	Produkčná podpora 24/7	

Bezpečnostný nástroj 3
(Nástroj pre správu privilegovaných účtov)

Verejný obstarávateľ požaduje dodanie **nástroja pre správu privilegovaných účtov**, ktorý spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1**:: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	**Poznámka**
Technická špecifikácia a. Plne onpremise implementovateľné riešenie. b. Vyhľadávanie a inventarizácia privilegovaných účtov. c. Bezpečná správa hesiel a SSH kľúčov pre privilegované účty. d. Komplexná správa privilegovaných identít – používateľov. e. Centrálny kontrolný bod pre izoláciu, riadenie a sledovanie všetkých aktivít správcov. f. Kontrola štyroch očí (dual control) a oddelenie rolí (segregation of duties). g. Centrálne úložisko hesiel (tzv. Digitálny trezor). h. Webové rozhranie pre správu a prístup k privilegovaným účtom. i. Automatická rotácia hesiel (zmena hesla po každom použití alebo v definovaných časových intervaloch). j. Možnosť sprístupňovania webových rozhraní interných systémov priamo cez cyberark rozhranie bez nutnosti prihlasovania sa do jump serveru. k. Centrálna správa politiky oprávnení a spúšťania aplikácií na endpointoch. l. Podpora automatizácie schvaľovacích procesov.	• PRIV-STANDARD-USER-SUBS, Temp, PAS Privileged User Subscription - Lic: 15, měsíce: 24 (360 ks): https://www.cyberark.com/resources/product-datasheets/cyberark-privilege-on-premises-datasheet • Správa privilegovaných prihlasovacích údajov (credential management) a bezpečné riadenie prístupu naprieč on-prem / cloud / hybrid: https://www.cyberark.com/resources/product-datasheets/cyberark-privilege-on-premises-datasheet • Izolácia a monitoring relácií (session isolation / monitoring) pre privilegovaný prístup: https://www.cyberark.com/resources/product-datasheets/cyberark-privilege-on-premises-datasheet • Detekcia hrozieb a monitoring privilegovanej aktivity (threat detection + privileged access monitoring): https://www.cyberark.com/resources/product-datasheets/cyberark-privilege-on-premises-datasheet • EXT-VENDOR-USER-SUBS. Temp, External Vendor License for PAS - Lic: 10, měsíce: 24 (240 ks): https://www.cyberark.com/resources/product-datasheets/vendor-pam-datasheet • Zero-Trust vendor prístup: just-in-time access, izolované a monitorované relácie, bez potreby VPN/agentov/hesiel (podľa Vendor PAM): https://www.cyberark.com/resources/product-datasheets/vendor-pam-datasheet • Biometrické MFA a kontrola prístupu pre externých dodávateľov (Vendor PAM). • EPM-TARGET-WIN-SVR-SUBS, CyberArk Endpoint Privilege Manager - server Provides granular admin rights, credential theft protection, and application control for Windows and Linux servers - per server per month - Lic: 10, měsíce: 24 (240 ks): https://www.cyberark.com/resources/product-datasheets/cyberark-endpoint-privilege-manager-datasheet • Granulárne prideľovanie admin práv / least privilege pre servery: https://www.cyberark.com/resources/product-datasheets/endpoint-privilege-manager-for-windows-servers • Ochrana proti krádeži prihlasovacích údajov (credential theft protection) • Application control (kontrola aplikácií) na serveroch; cieľom je blokovať/izolovať útoky na “endpoint of entry” • EPM rieši odoberanie lokálnych admin práv a presadzovanie least privilege naprieč endpointami	✓

	• APP-STATIC-SUBS, Secret management for homegrown static applications including C3 Credential Provider integrations - Lic: 10, měsíce: 24 (240 ks): https://www.cyberark.com/resources/product-datasheets/cyberark-secrets-manager • Prevencia hard-coded credentials v statických/legacy aplikáciách a bezpečné získanie credentialov za behu • Credential Provider beží na serveri s aplikáciou a podporuje anti-tampering, vysokú dostupnosť a výkon (vrátane lokálnej cache podľa doc) • Secrets Manager (Self-Hosted) podporuje zabezpečenie, rotáciu, audit a správu secretov/credentialov pre aplikácie a non-human identity: https://www.cyberark.com/resources/product-datasheets/cyberark-secrets-manager-self-hosted	
Bezpečnostné požiadavky a. Riadený prístup prostredníctvom RBAC (role based access control) k uloženým heslám, ako aj do webového rozhrania nástroja na správu a prístup k privilegovaným účtom na základe definovaných politík a rolí. b. Detekcia príkazov a možnosť vytvárania alertov pri ich detekcii, ako aj ich blokovanie počas prístupu cez vzdialenú reláciu. c. Odhaľovanie kybernetických útokov zneužívajúcich privilegované účty. d. Detekcia podozrivých aktivít v správaní používateľov v reálnom čase a automatické vynútenie nápravných opatrení - alerting, zmena prihlasovacích údajov, terminácia/pozastavenie relácii. e. Bezpečný prístup k systémom v infraštruktúre pomocou tzv. Jump serveru prostredníctvom zvoleného komunikačného protokolu (SSH alebo RDP) a príslušného privilegovaného účtu. f. Bezpečný mechanizmus pre vkladanie hesiel a SSH kľúčov do aplikácii, skriptov a služieb bez toho, aby boli užložené v plaintext podobe alebo museli byť manuálne spracovávané. Heslá a SSH kľúče nie sú uložené na koncových serveroch, aplikáciách a skriptoch. Sú bezpečne poskytované cez API, CLI alebo Vault dynamicky bez ich viditeľnosti. g. Možnosť prezerania hesiel len v rámci správnych oprávnení a politiky prístupu. h. Rozšírenie pre webové prehliadače umožňujúce bezpečné automatické vypĺňanie hesiel v rámci zobrazovaných webových sídiel, ako aj uloženie do clipboardu s automatickým premazaním clipboardu po uplynutí stanoveného času. i. Monitoring a nahrávanie vzdialených, ako aj webových relácii a aktivít privilegovaných účtov vo video formáte (nahrávanie pracovnej plochy)	Bezpečnostné požiadavky a. Riadený prístup prostredníctvom RBAC (role based access control) k uloženým heslám, ako aj do webového rozhrania nástroja na správu a prístup k privilegovaným účtom na základe definovaných politík a rolí. b. Detekcia príkazov a možnosť vytvárania alertov pri ich detekcii, ako aj ich blokovanie počas prístupu cez vzdialenú reláciu. c. Odhaľovanie kybernetických útokov zneužívajúcich privilegované účty. d. Detekcia podozrivých aktivít v správaní používateľov v reálnom čase a automatické vynútenie nápravných opatrení - alerting, zmena prihlasovacích údajov, terminácia/pozastavenie relácii. e. Bezpečný prístup k systémom v infraštruktúre pomocou tzv. Jump serveru prostredníctvom zvoleného komunikačného protokolu (SSH alebo RDP) a príslušného privilegovaného účtu. f. Bezpečný mechanizmus pre vkladanie hesiel a SSH kľúčov do aplikácii, skriptov a služieb bez toho, aby boli užložené v plaintext podobe alebo museli byť manuálne spracovávané. Heslá a SSH kľúče nie sú uložené na koncových serveroch, aplikáciách a skriptoch. Sú bezpečne poskytované cez API, CLI alebo Vault dynamicky bez ich viditeľnosti. g. Možnosť prezerania hesiel len v rámci správnych oprávnení a politiky prístupu. h. Rozšírenie pre webové prehliadače umožňujúce bezpečné automatické vypĺňanie hesiel v rámci zobrazovaných webových sídiel, ako aj uloženie do clipboardu s automatickým premazaním clipboardu po uplynutí stanoveného času. i. Monitoring a nahrávanie vzdialených, ako aj webových relácii a aktivít privilegovaných účtov vo video formáte (nahrávanie pracovnej plochy) s možnosťou	✓

s možnosťou kontextového vyhľadávania v zadaných príkazoch, ako aj presun na konkrétne časové stopy v nahrávke pri výbere konkrétneho zadaného príkazu. j. Možnosť pridávanie značiek (tagov) alebo označenie incidentov pre konkrétne aktivity zaznamenané v nahrávkach vzdialených relácii, či už manuálne alebo automatizovane pomocou definovaných pravidiel. k. Detekcia hrozieb v privilegovaných prístupoch PTA (Privileged Threat Analytics): o Detekcia anomálií v správaní používateľov (UEBA). o Real-time monitorovanie a analýza privilegovaných prístupov. o Ochrana pred kompromitovanými účtami a insiderskými hrozbami formou identifikácie laterálnych pohybov, použitie neautorizovaných alebo zakázaných nástrojov. o Integrovaný incident response s možnosťou automatického blokovania prístupov a deaktivácia účtov. o Možnosť ladenia detekcie formou konfigurácie citlivosti detekcie, prípadne whitelisting legitímnych aktivít. l. Auditná stopa a personalizácia využívania zdieľaných účtov. m. Podpora štandardu minimálne FIPS 140-2. n. Možnosť elevácie oprávnení na základe schválenej žiadosti alebo politiky na endpointoch. o. Logovanie a audit činností používateľov a aplikácií na endpointoch. p. Blokovanie a rýchla identifikácia podozrivého spustenia (napr. ransomvér, skripty) na endpointoch. q. Detekcia neoprávnených pokusov o eskaláciu práv na endpointoch.	kontextového vyhľadávania v zadaných príkazoch, ako aj presun na konkrétne časové stopy v nahrávke pri výbere konkrétneho zadaného príkazu. j. Možnosť pridávanie značiek (tagov) alebo označenie incidentov pre konkrétne aktivity zaznamenané v nahrávkach vzdialených relácii, či už manuálne alebo automatizovane pomocou definovaných pravidiel. k. Detekcia hrozieb v privilegovaných prístupoch PTA (Privileged Threat Analytics): o Detekcia anomálií v správaní používateľov (UEBA). o Real-time monitorovanie a analýza privilegovaných prístupov. o Ochrana pred kompromitovanými účtami a insiderskými hrozbami formou identifikácie laterálnych pohybov, použitie neautorizovaných alebo zakázaných nástrojov. o Integrovaný incident response s možnosťou automatického blokovania prístupov a deaktivácia účtov. o Možnosť ladenia detekcie formou konfigurácie citlivosti detekcie, prípadne whitelisting legitímnych aktivít. l. Auditná stopa a personalizácia využívania zdieľaných účtov. m. Podpora štandardu minimálne FIPS 140-2. n. Možnosť elevácie oprávnení na základe schválenej žiadosti alebo politiky na endpointoch. o. Logovanie a audit činností používateľov a aplikácií na endpointoch. p. Blokovanie a rýchla identifikácia podozrivého spustenia (napr. ransomvér, skripty) na endpointoch. q. Detekcia neoprávnených pokusov o eskaláciu práv na endpointoch.	
Podpora: Dodávateľ sa zaväzuje: • Poskytovať aktuálne verzie softvéru počas trvania predplatného (subscription): o **Minor Releases**: opravy chýb, bezpečnostné záplaty, drobné vylepšenia funkcionality. o **Major Releases**: nové verzie softvéru s významnými zmenami alebo novými funkciami. o **Kompatibilita**: zabezpečenie, že softvér zostáva kompatibilný s novými verziami OS, prehliadačov, databáz a pod. (ďalej len „**Podpora softvéru**“). • Poskytovať technickú podporu výrobcu a technickú podporu Dodávateľa pre Nástroj PAM v rozsahu:	• Podpora výrobcu je súčasťou licenčného ujedania a licencií popísaných vyššie: https://www.cyberark.com/maintenance-support-terms.pdf • Podpora od dodávateľa bude zaistená podľa požiadaviek obstarávateľa	✓

o V pracovné dni v čase 8:00 – 18:00 hod. v slovenskom alebo českom jazyku (e-mail, telefón)/SLA 2 hodiny. o Prístup k technickej podpore výrobcu certifikovaným personálom, jeho dokumentácii a znalostnej báze. o Konzultácie výrobcu k slovenskom alebo českom jazyku k rozvoju, bezpečnostným opatreniam a používaniu bezpečnostného nástroja. o Garantovanú podporu výrobcom 24 x 7 x 365 minimálne v anglickom jazyku/SLA 4 hodiny.		

Informácia pre uchádzačov: Požiadavky spĺňa napríklad riešenie zn. **Cyberark**, typ **Cyberark Core PAS** v najnovšej stabilnej verzii v čase predkladania ponuky vrátane CyberArk Endpoint Privilege Manager (EPM).

Bezpečnostný nástroj 4
(Nástroj pre spracovanie bezpečnostných udalostí)

Verejný obstarávateľ požaduje dodanie **nástroja pre spracovanie bezpečnostných udalostí zn. Elastic Stack** v najnovšej stabilnej verzii v čase predkladania ponuky, ktorý spĺňa minimálne nasledujúce technické a funkčné požiadavky:	Vlastný návrh plnenia **UCHADZAČA č. 1:**: (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	**Poznámka**

Technická špecifikácia
• Licencovanie založené na počte uzlov klastra, nie na počte udalostí za sekundu (EPS – events per second).
• Centrálna správa logov (log management).
• Zber logov prostredníctvom prijímania zasielaných logov prostredníctvom logstash serverov alebo priamo zber prostredníctvom nasadených agentov na konkrétnych systémoch a serveroch.
• Automatizované notifikácie a výstrahy (alerting) prostredníctvom zasielania e-mailov, prípadne zobrazovanie v rámci dashboardov.
• Detekcia, vyšetrovanie a reakcia na bezpečnostné incidenty.
• Databáza viac ako 500 detekčných pravidiel v rámci mitre attack framwork-u ihneď implementovateľných v rámci elastic stacku a zároveň neobmedzená možnosť vytvárania vlastných detekčných pravidiel.
• Riadenie detegovaných incidentov prostredníctvom vstavaného case management systému, ktorý umožňuje:
  ○ Vytváranie záznamov o incidentoch.
  ○ Pridávanie komentárov, dôkazov, alertov, časovej línie.
  ○ Sledovanie stavu incidentu (otvorený, v procese, uzavretý).
  ○ Prideľovanie incidentov jednotlivým analytikom.
  ○ Export do externých systémov.
• Integrácia externých Threat Intel platforiem (MISP).
• Vizualizácia spracovávaných dát prostredníctvom dashboardov, ktoré je možné v neobmedzenom počte vytvárať na základe vlastných potrieb zobrazovania informácií o stavoch monitorovaných infraštruktúr.
	• ELSP1Y, ELS, Elastic Platinum License 2y (7ks): https://www.elastic.co/de/pdf/subscriptions-2025-10-01.pdf , https://www.elastic.co/docs
	• Bezpečnosť (advanced security) - Field- a document-level security, vlastné authN/authZ “realms”, podpora encryption at rest, FIPS 140-2 mode, pokročilá bezpečnosť pre remote clusters
	• Machine learning / AI a pokročilé analýzy - Funkcie v sekcii Machine Learning / AI, vrátane artefaktov pre ML nody (napr. ELSER/e5 balíky pre ML nody)
	• Alerting / Operations - Pokročilé alertovanie (napr. “noise reduction”, maintenance windows) a ďalšie položky v “Alerting”
	• Škálovanie a dostupnosť - Capability ako napr. cross-cluster replication/search
	• Licencovanie založené na počte uzlov klastra, nie na počte udalostí za sekundu (EPS – events per second).
	• Centrálna správa logov (log management).
	• Zber logov prostredníctvom prijímania zasielaných logov prostredníctvom logstash serverov alebo priamo zber prostredníctvom nasadených agentov na konkrétnych systémoch a serveroch.
	• Automatizované notifikácie a výstrahy (alerting) prostredníctvom zasielania e-mailov, prípadne zobrazovanie v rámci dashboardov.
	• Detekcia, vyšetrovanie a reakcia na bezpečnostné incidenty.
	• Databáza viac ako 500 detekčných pravidiel v rámci mitre attack framwork-u ihneď implementovateľných v rámci elastic stacku a zároveň neobmedzená možnosť vytvárania vlastných detekčných pravidiel.
	• Riadenie detegovaných incidentov prostredníctvom vstavaného case management systému, ktorý umožňuje:
	  ○ Vytváranie záznamov o incidentoch.
	  ○ Pridávanie komentárov, dôkazov, alertov, časovej línie.
	  ○ Sledovanie stavu incidentu (otvorený, v procese, uzavretý).
	  ○ Prideľovanie incidentov jednotlivým analytikom.
	  ○ Export do externých systémov.
	• Integrácia externých Threat Intel platforiem (MISP).
		✓

• Riadenie prístupu používateľov na základe RBAC (role-based access control) ku konkrétnym dashboardom, dátam, indexom alebo typom vizualizácii na základe pridelených oprávnení. • Riadenie prístupu až na úroveň konkrétnych polí v dokumentoch alebo jednotlivým typom dokumentov. • Auditné logovanie všetkých akcií používateľov ako napr. prihlásenia, zmeny, dotazy, exporty. • Možnosť integrácie s externými autentifikačnými systémami (napr. LDAP, Active Directory) a dvojfaktorové overovanie. • Automatizované riadenie retencie logov prostredníctvom „index lifecycle management". • Centralizovaná správa logstash pipelines. • Možnosť nasadenia machine learning modelov na vyhodnocovanie zaznamenaných logov.	• Vizualizácia spracovávaných dát prostredníctvom dashboardov, ktoré je možné v neobmedzenom počte vytvárať na základe vlastných potrieb zobrazovania informácií o stavoch monitorovaných infraštruktúr. • Riadenie prístupu používateľov na základe RBAC (role-based access control) ku konkrétnym dashboardom, dátam, indexom alebo typom vizualizácii na základe pridelených oprávnení. • Riadenie prístupu až na úroveň konkrétnych polí v dokumentoch alebo jednotlivým typom dokumentov. • Auditné logovanie všetkých akcií používateľov ako napr. prihlásenia, zmeny, dotazy, exporty. • Možnosť integrácie s externými autentifikačnými systémami (napr. LDAP, Active Directory) a dvojfaktorové overovanie. • Automatizované riadenie retencie logov prostredníctvom „index lifecycle management". • Centralizovaná správa logstash pipelines. • Možnosť nasadenia machine learning modelov na vyhodnocovanie zaznamenaných logov.	

Podpora:
• Podpora od výrobcu dostupná 24 x 7 x 365 s možnosťou nahlasovania prostredníctvom e-mailového prípadne telefonického alebo support portálu
• Nelimitované množstvo nahlasovaných incidentov.
• Odozva na nahlásené incidenty:
  ○ Kritická závažnosť - 1 hodina
  ○ Vysoká závažnosť - 4 hodiny
  ○ Závažnosť nižšia ako vysoká - 1 business day
• Možnosť pridelenia vyhradeného inžiniera v rámci výrobcu (tzv. Designated support enginner) s nasledovnými podmienkami:
  ○ Možnosť využitia až 25 hodín práce mesačne.
  ○ Dostupnosť od 9:00 do 17:00 hod. v časovom pásme podporovanom výrobcom.
  ○ Podpora na diaľku.
  ○ Možnosť mesačných kontrolných stretnutí.
  ○ Možnosť mesačných správ o prípadoch nahlásených výrobcovi.
	• Popdora výrobcu podľa požiadaviek obstarávateľa: https://www.elastic.co/support/welcome
	• Podpora od výrobcu dostupná 24 x 7 x 365 s možnosťou nahlasovania prostredníctvom e-mailového prípadne telefonického alebo support portálu
	• Nelimitované množstvo nahlasovaných incidentov.
	• Odozva na nahlásené incidenty:
	  ○ Kritická závažnosť - 1 hodina
	  ○ Vysoká závažnosť - 4 hodiny
	  ○ Závažnosť nižšia ako vysoká - 1 business day
	• Možnosť pridelenia vyhradeného inžiniera v rámci výrobcu (tzv. Designated support engineer) s nasledovnými podmienkami:
	  ○ Možnosť využitia až 25 hodín práce mesačne.
	  ○ Dostupnosť od 9:00 do 17:00 hod. v časovom pásme podporovanom výrobcom.
	  ○ Podpora na diaľku.
	  ○ Možnosť mesačných kontrolných stretnutí.
	  ○ Možnosť mesačných správ o prípadoch nahlásených výrobcovi.
	  ○ Možnosť pracovať na viacerých prípadoch použitia či projektoch v rámci aktívnych licencií.
		✓
		ŽoV č. 1
		Vysvetlením
		doplnené - akceptované

○ Možnosť pracovať na viacerých prípadoch použitia či projektoch v rámci aktívnych licencií.		

Verejný obstarávateľ požaduje dodanie **nástroja pre spracovanie bezpečnostných udalostí zn. Elastic Stack** v najnovšej stabilnej verzii v čase predkladania ponuky, ktorý spĺňa minimálne nasledujúce technické a funkčné požiadavky:

Bezpečnostný nástroj 5
(Nástroj pre sieťový bezpečnostný monitoring)

Verejný obstarávateľ požaduje dodanie nástroja pre bezpečnostný monitoring sieťovej komunikácie, detekciu anomálií a analýzu dát v reálnom čase, ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	**Vlastný návrh plnenia UCHADZAČA č. 1::** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka
Technická špecifikácia:		

1. Požiadavky na zber dát
 	
Prevedenie:
• Fyzické zariadenie (appliance) montovateľné do racku.
• Počet a typ monitorovacích portov - 2 ks 1 GB/s monitorovací port pre metalický prepoj.
• Výkon:
  ○ Výkon per Port: 1,48 Mpps.
  ○ Výkon podľa zariadenia: 2,96 Mpps.
  ○ Vyrovnávacia pamäť pre počet flowov pre monitorovaci port: 0,5 M.
Vlastnosti zariadenia:
• Min. 1 ks manažment port pre zabezpečenú vzdialenú správu a konfiguráciu appliance, manažment a export flowov.
• Vizualizácia štatistických dát podľa objemu (min. počet prenesených bytov, tokov, paketov), IP prevádzky (min. TCP, UDP, ICMP, ostatné) alebo protokolu (min. HTTP, IMAP, SSH), vrátane plnej konfigurácie grafov a pohľadov užívateľom.
• Podpora autentizácie voči LDAP (Active Directory).
• Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.
• Použitie DNS cache na zariadení pre rýchlejší preklad IP adries na doménové mená.
• Monitorovanie rozšírených L2, L3/L4 informácií: Podpora pre monitorovanie rozšírených L3/L4 informácií - TTL (Time to live), TCP Window size, TCP SYN.
• Monitorovanie a reportovanie MAC adries vo flow štatistikách. Možnosť použiť MAC adresu ako položku kľúča flow záznamu.
• Spracovanie dátovej prevádzky min. IPv4 a IPv6, VLAN, MPLS, AS, HTTP, HTTPS (SNI) VoIP, DNS, DHCP, SMB/CIFS a e-mailovej prevádzky.
	• FM-PRB-HW-STD-2000-CU, Progress Flowmon Probe 2000 (6 ks): https://www.progress.com/docs/default-source/flowmon-resources/2025-11-flowmon_probe_specification.pdf?sfvrsn=b7d1fab4_113
	• Výkon: 1.48 Mpps na port, 2.96 Mpps na zariadenie
	• Monitoring porty: 2 × 10/100/1000 Mbps Ethernet (copper)
	• Flow cache: 0.5 M
	• HW parametre: CPU 8, RAM 32 GB, disk 1× SATA
	• Podpora NetFlow/IPFIX + Flowmon IPFIX Extensions (RTT, SRT, jitter a L7 protokoly ako HTTP, DNS, DHCP, SMB, SQL, SMTP atď.)
	• Podpora L2/tunelovania (napr. VLAN, MPLS, GRE, VxLAN…) a možnosť použitia monitorovacích rozhraní ako ciele pre ERSPAN/GRE alebo VxLAN sessions
	• FM-PRB-HW-STD-2000-CU-SS, 1Y Progress Flowmon Probe 2000 Standard Support: https://www.progress.com/docs/default-source/eula/2024-04-19-flowmon-technical-support-rev_for_fy25.pdf?sfvrsn=fb02388e_9 (https://www.progress.com/docs/default-source/flowmon-resources/flowmon-support-services-flyer.pdf)
	• 8×5 technická podpora + software updates & upgrades
	• Pri nasadení ADS: prístup k Flowmon Threat Intelligence (v rámci Standard Support).
	Prevedenie:
	• Fyzické zariadenie (appliance) montovateľné do racku.
	• Počet a typ monitorovacích portov - 2 ks 1 GB/s monitorovací port pre metalický prepoj.
	• Výkon:
	  ○ Výkon per Port: 1,48 Mpps.
	  ○ Výkon podľa zariadenia: 2,96 Mpps.
	  ○ Vyrovnávacia pamäť pre počet flowov pre monitorovaci port: 0,5 M.
	Vlastnosti zariadenia:
	• Min. 1 ks manažment port pre zabezpečenú vzdialenú správu a konfiguráciu appliance, manažment a export flowov.
	• Vizualizácia štatistických dát podľa objemu (min. počet prenesených bytov, tokov, paketov), IP prevádzky (min. TCP, UDP, ICMP, ostatné) alebo protokolu (min. HTTP, IMAP, SSH), vrátane plnej konfigurácie grafov a pohľadov užívateľom.
	• Podpora autentizácie voči LDAP (Active Directory).
	• Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.
	• Použitie DNS cache na zariadení pre rýchlejší preklad IP adries na doménové mená.
		✓

• Analýza oneskorenia na sieti min. RTT, SRT, delay, jitter, retransmisiu, out-of-order pakety ako súčasť flow štatistík a podpora pre analýzu CISCO AVC. • Monitoring aktívnych zariadení na sieti a viditeľnosť do šifrovanej komunikácie SSL/TLS. • Monitoring využívaných externých cloudových služieb (MS Azure, AWS, GPC) s podporou end-to-end visibility dátovej komunikácie. • Systém musí umožňovať vizualizáciu monitorovaných liniek a prepojov a sieťovej topológie. • Generovanie štatistík a podrobných výpisov nad voliteľnými časovými intervalmi s voliteľnými filtrami. Rôzne formáty výstupov, minimálne PDF, CSV. • Monitorovanie zariadení pripojených k dátovej sieti, dlhodobá história aktívnych zariadení, identifikácia na základe IP adresy, MAC adresy, sledovanie VLAN, operačného systému, prihláseného používateľa na danom zariadení. <u>Integrácia:</u> • So systémami SIEM/NPM/APM, prípadne možnosť prenosu tokových dát do iných nástrojov pre správu IT a kybernetickej bezpečnosti. <u>Podpora:</u> • Podpora po dobu 2 rokov obsahujúca: o Prístup k aktualizáciám a upgrade. o Odborná technická podpora 8 x 5, dostupná cez telefonické spojenie alebo e-mailovú komunikáciu. o Rozšírená hardvérová záruka (NBD – Next Business Day). o Flowmon Threat Intelligence pre Flowmon ADS.	• Monitorovanie rozšírených L2, L3/L4 informácií: Podpora pre monitorovanie rozšírených L3/L4 informácií - TTL (Time to live), TCP Window size, TCP SYN. • Monitorovanie a reportovanie MAC adries vo flow štatistikách. Možnosť použiť MAC adresu ako položku kľúča flow záznamu. • Spracovanie dátovej prevádzky min. IPv4 a IPv6, VLAN, MPLS, AS, HTTP, HTTPS (SNI) VoIP, DNS, DHCP, SMB/CIFS a e-mailovej prevádzky. • Analýza oneskorenia na sieti min. RTT, SRT, delay, jitter, retransmisiu, out-of-order pakety ako súčasť flow štatistík a podpora pre analýzu CISCO AVC. • Monitoring aktívnych zariadení na sieti a viditeľnosť do šifrovanej komunikácie SSL/TLS. • Monitoring využívaných externých cloudových služieb (MS Azure, AWS, GPC) s podporou end-to-end visibility dátovej komunikácie. • Systém musí umožňovať vizualizáciu monitorovaných liniek a prepojov a sieťovej topológie. • Generovanie štatistík a podrobných výpisov nad voliteľnými časovými intervalmi s voliteľnými filtrami. Rôzne formáty výstupov, minimálne PDF, CSV. • Monitorovanie zariadení pripojených k dátovej sieti, dlhodobá história aktívnych zariadení, identifikácia na základe IP adresy, MAC adresy, sledovanie VLAN, operačného systému, prihláseného používateľa na danom zariadení. <u>Integrácia:</u> • So systémami SIEM/NPM/APM, prípadne možnosť prenosu tokových dát do iných nástrojov pre správu IT a kybernetickej bezpečnosti. <u>Podpora:</u> • Podpora po dobu 2 rokov obsahujúca: o Prístup k aktualizáciám a upgrade. Odborná technická podpora 8 x 5, dostupná cez telefonické spojenie alebo e-mailovú komunikáciu o Rozšírená hardvérová záruka (NBD – Next Business Day). Flowmon Threat Intelligence pre Flowmon ADS.	
2. Požiadavky na centralizáciu dát <u>Prevedenie:</u> • Virtuálne zariadenie (appliance). • Šablóny pre nasadenie virtuálneho stroja (VmWare, KVM, Hyper-V). <u>Výkon kolektora:</u> • 75000 fps (dátových tokov/s). <u>Vlastnosti zariadenia:</u> • Spracovanie dátových tokov / paketov a vizualizácia v 5-minútových, 1-minútových alebo 30-sekundových intervaloch.	• FM-COL-VA-500, Progress Flowmon Collector 500 VA (3 ks): https://www.progress.com/docs/default-source/flowmon-resources/2025-11-flowmon_collector_specification.pdf?sfvrsn=f8ed35b5_3 • Výkon: do 75,000 fps (flows per second) • Úložisko: 0.5 TB • Podporované platformy (min.): VMware ESXi 5.5+, Hyper-V 2012 R2+, KVM 3.10+ (s uvedenými min. QEMU/libvirt) • Minimálna konfigurácia VA: 4 CPU cores, 8 GB RAM, 500 IOPS • FM-COL-VA-500-SS, 1Y Flowmon Collector 500 VA Standard Support: https://www.progress.com/docs/default-source/eula/2024-04-19-flowmon-technical-support-rev_for_fy25.pdf?sfvrsn=fb02388e_9 (https://www.progress.com/docs/default-source/flowmon-resources/flowmon-support-services-flyer.pdf)	✓

• Možnosť dohľadania ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty, databázy aktívnych zariadení na sieti vrátane identifikácie zariadení. • Zabezpečená vzdialená správa, dohľad a konfigurácia - SSH, HTTPS. • Prijímanie a preposielanie IPFIX dát pomocou spoľahlivého TCP spojenia s možnosťou šifrovania (TCP/TLS) podľa štandardu RFC 7011. • Kolektor poskytuje dokumentované API pre získavanie a spracovanie dát. Prostredníctvom API je možné kolektor tiež konfigurovať (napr. definovať vlastné prehľady, reporty, a pod.). Podporované štandardy dátových tokov: • Min. NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite a ich zber z desiatok zdrojov v sieti. Integrácia: • Do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov technológií SNMP. • Integrácia na Arcsight SIEM. Podpora: • Podpora po dobu 2 rokov obsahujúca: o Prístup k aktualizáciám a upgrade. o Odborná technická podpora 8 x 5, dostupná cez telefonické spojenie alebo e-mailovú komunikáciu. o Rozšírená hardvérová záruka (NBD – Next Business Day). o Flowmon Threat Intelligence pre Flowmon ADS.	• 8×5 technická podpora + software updates & upgrades • Pri nasadení ADS: prístup k Flowmon Threat Intelligence (v rámci Standard Support). **Požiadavky na centralizáciu dát** Prevedenie: • Virtuálne zariadenie (appliance). • Šablóny pre nasadenie virtuálneho stroja (VmWare, KVM, Hyper-V). Výkon kolektora: • 75000 fps (dátových tokov/s). Vlastnosti zariadenia: • Spracovanie dátových tokov / paketov a vizualizácia v 5-minútových, 1-minútových alebo 30-sekundových intervaloch. • Možnosť dohľadania ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty, databázy aktívnych zariadení na sieti vrátane identifikácie zariadení. • Zabezpečená vzdialená správa, dohľad a konfigurácia - SSH, HTTPS. • Prijímanie a preposielanie IPFIX dát pomocou spoľahlivého TCP spojenia s možnosťou šifrovania (TCP/TLS) podľa štandardu RFC 7011. • Kolektor poskytuje dokumentované API pre získavanie a spracovanie dát. Prostredníctvom API je možné kolektor tiež konfigurovať (napr. definovať vlastné prehľady, reporty, a pod.). Podporované štandardy dátových tokov: • Min. NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite a ich zber z desiatok zdrojov v sieti. Integrácia: • Do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov technológií SNMP. • Integrácia na Arcsight SIEM. Podpora: • Podpora po dobu 2 rokov obsahujúca: o Prístup k aktualizáciám a upgrade. o Odborná technická podpora 8 x 5, dostupná cez telefonické spojenie alebo e-mailovú komunikáciu. o Rozšírená hardvérová záruka (NBD – Next Business Day). Flowmon Threat Intelligence pre Flowmon ADS	
3. Požiadavky na vyhodnocovanie zbieraných dát Požadovaný výkon: • Sada detekčných metód a algoritmov pre analýzu flow štatistík, detekciu bezpečnostných incidentov, prevádzkových problémov a	• FM-ADS-SW-S, Progress Flowmon ADS Standard (3ks, na každý FM-COL-VA-500): https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_ads_specification.pdf?sfvrsn=5c9c19c4_52 • ADS je riešenie na detekciu anomálií s použitím AI/ML na odhalenie hrozieb skrytých v sieťovej prevádzke • Dátové zdroje: NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd. Progress.com	✓

sieťových anomálií pre min. 1000 fps (dátových tokov/s)/min. 3 rozdielnych dátových zdrojov (subnet, sieťový segment a pod.). Vlastnosti produktu: • Automatické vyhodnocovanie NetFlow dát a detekcia anomálií na sieti s podporou deduplikácie, vzorkovania na úrovni tokov, identity používateľov, persistencii doménových mien. • Automatické rozpoznanie odchýlky od normálneho správania siete, ktoré môžu naznačovať hrozby. • Architektúra systému umožňuje streamové spracovávanie flow dát pre rýchlu detekciu bezpečnostných alebo prevádzkových anomálií. • Systém umožňuje spravovať zdroje sieťových tokov, umožňuje dočasne pozastaviť príjem tokov a indikovať poruchu zdroja sieťových tokov. Detekčné mechanizmy: • Detekcia skenovanie portov, slovníkové útoky, útoky odopretia služieb (DoS), útoky na sieťové protokoly SSH, RDP, Telnet. Detekcia anomálií v DNS, DHCP, SMTP, multicast prevádzky a neštandardnej komunikácie. Detekcia P2P sietí, VPN služieb a anonymizačných služieb (napr. TOR). Detekcia nadmernej záťaže siete, nových a cudzích zariadení pripojených k sieti, výpadkov služieb, chýbajúcich reverzných DNS záznamov, nových a cudzích zariadení pripojených k sieti. Detekcia NAT. Detekcia ťažby kryptomien, únikov dát, supply chain útokov a ransomware. • Systém umožňuje Threat Inteligence napojenie - identifikácia bezpečnostných udalostí (napr. komunikáciu s botnet command & control centrom, prístup na phishingové servery, ransomware, cryptojacking a pod.) využívaním zdrojov IP a host reputačných databáz poskytovaných výrobcom a aktualizovaných najmenej každých 24 hodín. Systém umožňuje zapojiť ďalšie zdroje IP a host reputačných dát pre automatickú detekciu cez CSV alebo MISP. • Detekcia sieťových anomálií na základe predikcie budúceho správania siete s využívaním znalosti histórie komunikácie. • Vstavaná funkcionalita detekcie narušenia (Intrusion Detection System). • Systém musí mapovat a vizualizovať kontextuálne MITTRE ATT&CK taktiky a techniky voči jednotlivým udalostiam pre výskyt anomálií a bezpečnostných hrozieb na sieti.	• Detekcie: machine learning, adaptive baselining, behavior analysis, heuristics + integrácia so Suricata IDS na Flowmon Probes • Reporting/alerting: e-mail, PDF/CSV, syslog, SNMP, packet capture trigger, script trigger; SIEM cez CEF (syslog) a SNMP trap • Sizing/performance pre “Standard (FM-ADS-SW-S)”: • stream processing 1,000 flows/s, behavior patterns 1,000 flows/s • data feeds: 3 • RAM: 8 GB, CPU: 2 cores Progress.com • FM-ADS-SW-S-SS — 1Y Flowmon ADS Standard Standard Support: https://www.progress.com/docs/default-source/eula/2024-04-19-flowmon-technical-support-rev_for_fy25.pdf?sfvrsn=fb02388e_9 (https://www.progress.com/docs/default-source/flowmon-resources/flowmon-support-services-flyer.pdf) • prístup k Flowmon Threat Intelligence **Požiadavky na vyhodnocovanie zbieraných dát** Požadovaný výkon: • Sada detekčných metód a algoritmov pre analýzu flow štatistík, detekciu bezpečnostných incidentov, prevádzkových problémov a sieťových anomálií pre min. 1000 fps (dátových tokov/s)/min. 3 rozdielnych dátových zdrojov (subnet, sieťový segment a pod.). Vlastnosti produktu: • Automatické vyhodnocovanie NetFlow dát a detekcia anomálií na sieti s podporou deduplikácie, vzorkovania na úrovni tokov, identity používateľov, persistencii doménových mien. • Automatické rozpoznanie odchýlky od normálneho správania siete, ktoré môžu naznačovať hrozby. • Architektúra systému umožňuje streamové spracovávanie flow dát pre rýchlu detekciu bezpečnostných alebo prevádzkových anomálií. • Systém umožňuje spravovať zdroje sieťových tokov, umožňuje dočasne pozastaviť príjem tokov a indikovať poruchu zdroja sieťových tokov. Detekčné mechanizmy: • Detekcia skenovanie portov, slovníkové útoky, útoky odopretia služieb (DoS), útoky na sieťové protokoly SSH, RDP, Telnet. Detekcia anomálií v DNS, DHCP, SMTP, multicast prevádzky a neštandardnej komunikácie. Detekcia P2P sietí, VPN služieb a anonymizačných služieb (napr. TOR). Detekcia nadmernej záťaže siete, nových a cudzích zariadení pripojených k sieti, výpadkov služieb, chýbajúcich reverzných DNS záznamov, nových a cudzích zariadení pripojených k sieti. Detekcia NAT. Detekcia ťažby kryptomien, únikov dát, supply chain útokov a ransomware.	

• Prípadné udalosti, ktoré predstavujú falošné poplachy (false positives) je možné odstrániť prostredníctvom jednoduchej konfigurácie pravidiel vylúčenia falošných poplachov dostupné v používateľskom rozhraní. • Systém umožňuje vytvárať správcovi vlastné aplikovateľné detekčné metódy na základe vzorcov chovania siete napr. na báze jednoduchého SQL syntaxu. <u>Reporting a alerting:</u> • Udalosti je možné automaticky exportovať vo formáte CEF prostredníctvom Syslogu. • Udalosti je možné reportovať do dohľadových systémov prostredníctvom funkcionality SNMP trap. • Notifikácia o detekovaných udalostiach prostredníctvom e-mailu s podporou rôznych formátov (HTML, incident handling systém, úsporný textový formát). Možnosť pripojiť vzorku flow dát, na základe ktorých bola udalosť detekovaná k e-mailovému reportu. • Vizualizácia priebehu prevádzky s vyznačením detekovaných udalostí v závislosti od nastavenej závažnosti udalostí. • Systém integruje informácie zo služieb DNS, WHOIS, geolokačné služby. Užívateľsky definované externé služby fungujúce na protokole HTTP. • Na výskyt udalosti je možné automaticky reagovať spustením užívateľsky definovaných skriptov. • Automatizovaná analýza sieťovej prevádzky a výsledky analýzy sú prezentované v zrozumiteľnej podobe v rámci udalostí, ktoré popisujú, ako jednotlivé komunikácie v zázname prevádzky prebiehali. Udalosti sú rozdeľované podľa závažnosti do niekoľkých úrovní a indikujú problémy vzniknuté v sieťovej prevádzke na podporovaných protokoloch. • Systém musí umožňovať blokovanie/mitigáciu udalostí plne automatizovanou a poloautomatizovanou formou. • Systém musí byť ako platforma pripravený na doplnenie, doprogramovanie a nasadenie custom zdrojov dát vo formáte Syslog, PlainText, Json a pod., parserov a automatizáciu v rámci činností IT bezpečnostných operácií, či preddefinovanie tvorby bezpečnostných pravidiel pre SOC operátorov a analytikov, doprogramovanie integrácií v rámci inštalovanej bázy pre potreby CTI a ich nasadenie v prostredí infraštruktúry zadávateľa.	• Systém umožňuje Threat Inteligence napojenie - identifikácia bezpečnostných udalostí (napr. komunikáciu s botnet command & control centrom, prístup na phishingové servery, ransomware, cryptojacking a pod.) využívaním zdrojov IP a host reputačných databáz poskytovaných výrobcom a aktualizovaných najmenej každých 24 hodín. Systém umožňuje zapojiť ďalšie zdroje IP a host reputačných dát pre automatickú detekciu cez CSV alebo MISP. • Detekcia sieťových anomálií na základe predikcie budúceho správania siete s využívaním znalosti histórie komunikácie. • Vstavaná funkcionalita detekcie narušenia (Intrusion Detection System). • Systém musí mapovat a vizualizovať kontextuálne MITTRE ATT&CK taktiky a techniky voči jednotlivým udalostiam pre výskyt anomálií a bezpečnostných hrozieb na sieti. • Prípadné udalosti, ktoré predstavujú falošné poplachy (false positives) je možné odstrániť prostredníctvom jednoduchej konfigurácie pravidiel vylúčenia falošných poplachov dostupné v používateľskom rozhraní. • Systém umožňuje vytvárať správcovi vlastné aplikovateľné detekčné metódy na základe vzorcov chovania siete napr. na báze jednoduchého SQL syntaxu. <u>Reporting a alerting:</u> • Udalosti je možné automaticky exportovať vo formáte CEF prostredníctvom Syslogu. • Udalosti je možné reportovať do dohľadových systémov prostredníctvom funkcionality SNMP trap. • Notifikácia o detekovaných udalostiach prostredníctvom e-mailu s podporou rôznych formátov (HTML, incident handling systém, úsporný textový formát). Možnosť pripojiť vzorku flow dát, na základe ktorých bola udalosť detekovaná k e-mailovému reportu. • Vizualizácia priebehu prevádzky s vyznačením detekovaných udalostí v závislosti od nastavenej závažnosti udalostí. • Systém integruje informácie zo služieb DNS, WHOIS, geolokačné služby. Užívateľsky definované externé služby fungujúce na protokole HTTP. • Na výskyt udalosti je možné automaticky reagovať spustením užívateľsky definovaných skriptov. • Automatizovaná analýza sieťovej prevádzky a výsledky analýzy sú prezentované v zrozumiteľnej podobe v rámci udalostí, ktoré popisujú, ako jednotlivé komunikácie v zázname prevádzky prebiehali. Udalosti sú rozdeľované podľa závažnosti do niekoľkých úrovní a indikujú problémy vzniknuté v sieťovej prevádzke na podporovaných protokoloch. • Systém musí umožňovať blokovanie/mitigáciu udalostí plne automatizovanou a poloautomatizovanou formou. • Systém musí byť ako platforma pripravený na doplnenie, doprogramovanie a nasadenie custom zdrojov dát vo formáte Syslog, PlainText, Json a pod., parserov a automatizáciu v rámci činností IT bezpečnostných operácií, či preddefinovanie tvorby bezpečnostných	

• Systém musí umožniť zvoliť rozsahy siete, na ktoré sa má alebo nemá aplikovať pravidlo pre automatickú mitigáciu kybernetických hrozieb. • Vstavaný tester udalostí a výstrah, ktorý simuluje workflow, keď sa incident stane v sieti. Tester musí byť schopný generovať skutočný incident. • Systém musí umožniť custom prepojenie externých zdrojov informácií pre potreby CTI a CDN cez vstavané API rozhranie vrátane existencie preddefinovaných zdrojov pre look up typu NIST CVE, Shodan, Virustotal, Bitcoin, Maclookup, Cmd, Hostio, RIPE. • Systém musí mať preddefinované zdroje dát min typu Office365, Phistank a umožňovať automatizovanú formu tvorby adresných IP listov, URL a DNS pre využitie EDL (externých dynamických listov). • Webové centrálne užívateľské rozhranie, používateľsky definované (konfigurácia per používateľ). • Systém loguje všetky zmeny konfigurácie s cieľom zaistiť auditovateľnosť činnosti používateľov a vykonané zmeny s dopadom na detekcie a blokovanie udalostí. Zmeny konfigurácie je možné tiež odosielať protokolom syslog pre auditovanie formou externého systému typu SIEM alebo log management. • Reporting min. vo formáte PDF alebo CSV, e-mail, Json a Syslog a možnosť nastavovania rôznych alertovacích mechanizmov per udalosť. <u>Podpora:</u> • Podpora po dobu 2 rokov obsahujúca: o Prístup k aktualizáciám a upgrade o Odborná technická podpora 8 x 5, dostupná cez telefonické spojenie alebo e-mailovú komunikáciu o Rozšírená hardvérová záruka (NBD – Next Business Day) o Flowmon Threat Intelligence pre Flowmon ADS Požadovaná úroveň dostupnosti a spoľahlivosti prevádzky: 99 % v režime 24/7.	pravidiel pre SOC operátorov a analytikov, doprogramovanie integrácií v rámci inštalovanej bázy pre potreby CTI a ich nasadenie v prostredí infraštruktúry zadávateľa. • Systém musí umožniť zvoliť rozsahy siete, na ktoré sa má alebo nemá aplikovať pravidlo pre automatickú mitigáciu kybernetických hrozieb. • Vstavaný tester udalostí a výstrah, ktorý simuluje workflow, keď sa incident stane v sieti. Tester musí byť schopný generovať skutočný incident. • Systém musí umožniť custom prepojenie externých zdrojov informácií pre potreby CTI a CDN cez vstavané API rozhranie vrátane existencie preddefinovaných zdrojov pre look up typu NIST CVE, Shodan, Virustotal, Bitcoin, Maclookup, Cmd, Hostio, RIPE. • Systém musí mať preddefinované zdroje dát min typu Office365, Phistank a umožňovať automatizovanú formu tvorby adresných IP listov, URL a DNS pre využitie EDL (externých dynamických listov). • Webové centrálne užívateľské rozhranie, používateľsky definované (konfigurácia per používateľ). • Systém loguje všetky zmeny konfigurácie s cieľom zaistiť auditovateľnosť činnosti používateľov a vykonané zmeny s dopadom na detekcie a blokovanie udalostí. Zmeny konfigurácie je možné tiež odosielať protokolom syslog pre auditovanie formou externého systému typu SIEM alebo log management. • Reporting min. vo formáte PDF alebo CSV, e-mail, Json a Syslog a možnosť nastavovania rôznych alertovacích mechanizmov per udalosť. <u>Podpora:</u> • Podpora po dobu 2 rokov obsahujúca: o Prístup k aktualizáciám a upgrade o Odborná technická podpora 8 x 5, dostupná cez telefonické spojenie alebo e-mailovú komunikáciu o Rozšírená hardvérová záruka (NBD – Next Business Day) o Flowmon Threat Intelligence pre Flowmon ADS • Požadovaná úroveň dostupnosti a spoľahlivosti prevádzky: 99 % v režime 24/7	

Informácia pre uchádzačov: Požiadavky spĺňa napríklad riešenie zn. **Progress Flowmon, typ Progress Flowmon Probe 2000, Progress Flowmon Collector 500 VA a Progress Flowmon ADS Standard** v najnovšej stabilnej verzii v čase predkladania ponuky vrátane podpory **Progress Flowmon Probe 2000 Standard Support, Progress Flowmon IFC-500-VA Standard Support a Progress Flowmon ADS Standard Standard Support.**

Bezpečnostný nástroj 6
(Nástroj pre správu zraniteľností)

Verejný obstarávateľ požaduje dodanie nástroja pre správu zraniteľností, ktoré spĺňa minimálne nasledujúce technické a funkčné požiadavky:	**Vlastný návrh plnenia UCHADZAČA č. 1:** (uchádzač uvedie konkrétnu technickú špecifikáciu predmetu plnenia vrátane predloženia technického listu, resp. odkazu na technický list od výrobcu)	Poznámka

Technická špecifikácia
 	
Skenovacie možnosti:
• Systém podporuje nasadenie agentov na jednotlivé hostiteľské systémy (lokálne skenovanie) aj vzdialené sieťové skenovanie prostredníctvom centrálnych skenovacích uzlov.
• Agentové skenovanie:
  ○ Agenti musia byť inštalovateľní na zariadenia s operačnými systémami Windows, Windows server 2016 a novšie, Linux, linux Red Hat 8 a novšie a macOS.
  ○ Skenovanie pomocou agentov musí byť schopné identifikovať lokálne zraniteľnosti aj bez trvalého pripojenia zariadenia k sieti.
  ○ Agenti musia umožňovať plánované a pravidelné skeny lokálnych zraniteľností s výsledkami synchronizovanými do centrálneho manažmentu.
• Bezagentové skenovanie:
  ○ Možnosť realizácie vzdialeného skenovania na sieťovej úrovni.
  ○ Možnosť sieťového monitoringu použitím tzv. „discovery mode“.
• Systém musí umožňovať použiť neobmedzený počet skenerov (agentov).
• Systém musí podporovať sieťový monitoring aj v tzv. „dicsovery mode“.
• Systém musí okrem iných podporovať najmä tieto typy skenov: „Credentialed Scans“, „Uncredentialed Scans“, „Policy Compliance Scans (podporujúce CIS Benchmarks)“, „Web Application Scans“, „Custom Scan Policies“.
• Systém podporuje infraštruktúrne skeny aj webové aplikácie.
	• TSC — Tenable Security Center (Tenable.sc), 24m, 800 assets (1 ks): https://docs.tenable.com/security-center.htm , https://dam.tenable.com/1fa9804a-4b0b-4db0-b971-b22d016efc2b/data-sheet-tenable-security-center.pdf , https://docs.tenable.com/quick-reference/licensing-guide/Content/tenable-security-center-licensing.htm
	• On-prem VM/console na centrálne riadenie skenov, reportov, používateľov a analýz; dáta ostávajú „managed on-prem“
	• Architektúra (v praxi):
	• 1× Tenable Security Center console (centrálne riadenie)
	• 1+ scanners (napr. Nessus) ktoré zbierajú dáta a posielajú výsledky do konzoly
	• Licenčný model (assets): licencia je na max. počet aktívnych assetov (IP/UUID) a typicky sa nezapočítava asset, kým nebol posúdený na zraniteľnosť = limit licencie 800 aktívnych posúdených assetov (podľa pravidiel Tenable).
	• Senzory a zdroje dát - kombinácia aktívnych skenerov, agentov, pasívneho monitoringu a integrácií (napr. CMDB) – pre lepšie pokrytie
	Skenovacie možnosti:
	• Systém podporuje nasadenie agentov na jednotlivé hostiteľské systémy (lokálne skenovanie) aj vzdialené sieťové skenovanie prostredníctvom centrálnych skenovacích uzlov.
	• Agentové skenovanie:
	  ○ Agenti musia byť inštalovateľní na zariadenia s operačnými systémami Windows, Windows server 2016 a novšie, Linux, linux Red Hat 8 a novšie a macOS.
	  ○ Skenovanie pomocou agentov musí byť schopné identifikovať lokálne zraniteľnosti aj bez trvalého pripojenia zariadenia k sieti.
	  ○ Agenti musia umožňovať plánované a pravidelné skeny lokálnych zraniteľností s výsledkami synchronizovanými do centrálneho manažmentu.
	• Bezagentové skenovanie:
	  ○ Možnosť realizácie vzdialeného skenovania na sieťovej úrovni.
	  ○ Možnosť sieťového monitoringu použitím tzv. „discovery mode“.
	• Systém musí umožňovať použiť neobmedzený počet skenerov (agentov).
	• Systém musí podporovať sieťový monitoring aj v tzv. „dicsovery mode“.
		✓

	• Systém musí okrem iných podporovať najmä tieto typy skenov: „Credentialed Scans“, „Uncredentialed Scans“, „Policy Compliance Scans (podporujúce CIS Benchmarks)“, „Web Application Scans“, „Custom Scan Policies“. Systém podporuje infraštruktúrne skeny aj webové aplikácie.	
Centrálny manažment zraniteľností: • Centrálna manažment konzola prístupná cez webové rozhranie. • Umožnenie správy skenov a ich výsledkov z jedného centrálneho rozhrania. • Správa skenovacích politík, plánovanie spúšťania skenov a vyhodnocovanie výsledkov skenov v centrálnom rozhraní. • Sledovanie stavu zraniteľností (aj historicky odstránené zraniteľnosti), kde jednotlivé zraniteľnosti budú mať zaevidovaný ich stav, najmenej v týchto typoch stavov: Nová (novo objavená zraniteľnosť, ktorá nebola zistená v predchádzajúcich skenoch), aktívna (zraniteľnosť sa vyskytla vo viacerých skenoch), Fixnutá (odstránená zraniteľnosť) a obnovená (v systéme bola už označená ako fixnutá, avšak objavila sa opätovne). • Možnosť vzdialenej konfigurácie skenovacích agentov a definovania skenovacích oblastí podľa priorít. • Podpora tzv. „Vulnerability Probability Rating“ (VPR) a tzv. „CVSS scoring system“.	Centrálny manažment zraniteľností: • Centrálna manažment konzola prístupná cez webové rozhranie. • Umožnenie správy skenov a ich výsledkov z jedného centrálneho rozhrania. • Správa skenovacích politík, plánovanie spúšťania skenov a vyhodnocovanie výsledkov skenov v centrálnom rozhraní. • Sledovanie stavu zraniteľností (aj historicky odstránené zraniteľnosti), kde jednotlivé zraniteľnosti budú mať zaevidovaný ich stav, najmenej v týchto typoch stavov: Nová (novo objavená zraniteľnosť, ktorá nebola zistená v predchádzajúcich skenoch), aktívna (zraniteľnosť sa vyskytla vo viacerých skenoch), Fixnutá (odstránená zraniteľnosť) a obnovená (v systéme bola už označená ako fixnutá, avšak objavila sa opätovne). • Možnosť vzdialenej konfigurácie skenovacích agentov a definovania skenovacích oblastí podľa priorít. • Podpora tzv. „Vulnerability Probability Rating“ (VPR) a tzv. „CVSS scoring system“.	✓
Užívateľské možnosti: • Neobmedzený počet užívateľských účtov v rámci centrálnej manažment konzoly. • Viaceré typy užívateľských rolí s rôznymi rozsahmi oprávnení ako administrátor, užívateľské roly, read only role, custom roly (nastaviteľné oprávnenia či už v rovine oprávnení vykonávať jednotlivé aktivity v rámci centrálnej manažment konzoly, ale aj definovania oprávnení pre konkrétny rozsah aktív v rámci sledovaných IP adries).	Užívateľské možnosti: • Neobmedzený počet užívateľských účtov v rámci centrálnej manažment konzoly. • Viaceré typy užívateľských rolí s rôznymi rozsahmi oprávnení ako administrátor, užívateľské roly, read only role, custom roly (nastaviteľné oprávnenia či už v rovine oprávnení vykonávať jednotlivé aktivity v rámci centrálnej manažment konzoly, ale aj definovania oprávnení pre konkrétny rozsah aktív v rámci sledovaných IP adries).	✓
Hlavné funkcie a schopnosti systému: • Dynamická aktualizácia - Automatická synchronizácia s najnovšími databázami zraniteľností a rizík, čím sa zabezpečuje aktuálnosť analýz. • Komunikácia centrálnej konzoly na jednotlivé skenery dokáže fungovať v režime pull, čo znamená, že skener komunikuje smerom na centrálnu konzolu, len ak centrálna konzola iniciuje komunikáciu. Skener sám o sebe neiniciuje komunikáciu. Táto funkcionalita je zo strany verejného obstarateľa vyžadovaná ako dôležitá súčasť. • Reporty a analýzy - Automatizované a prispôsobiteľné reportovanie, ktoré zahŕňa klasifikáciu zraniteľností podľa rizikovosti a možných dopadov. Systém musí podporovať aj tzv. „Vulnerability Probability Rating“ (VPR) a tzv. „CVSS scoring system“.	Hlavné funkcie a schopnosti systému: • Dynamická aktualizácia - Automatická synchronizácia s najnovšími databázami zraniteľností a rizík, čím sa zabezpečuje aktuálnosť analýz. • Komunikácia centrálnej konzoly na jednotlivé skenery dokáže fungovať v režime pull, čo znamená, že skener komunikuje smerom na centrálnu konzolu, len ak centrálna konzola iniciuje komunikáciu. Skener sám o sebe neiniciuje komunikáciu. Táto funkcionalita je zo strany verejného obstarateľa vyžadovaná ako dôležitá súčasť. • Reporty a analýzy - Automatizované a prispôsobiteľné reportovanie, ktoré zahŕňa klasifikáciu zraniteľností podľa rizikovosti a možných dopadov. Systém musí podporovať aj tzv. „Vulnerability Probability Rating“ (VPR) a tzv. „CVSS scoring system“.	✓

• Podpora politiky škálovania - Možnosť dynamického pridania IP adries v rámci kapacity 800 adries bez nutnosti rekonfigurácie. • Integrovateľnosť - Schopnosť integrácie s ďalšími bezpečnostnými riešeniami na automatizáciu reakcií na bezpečnostné incidenty, prípadne kontrolu pripojených zariadení do siete (discovery mode). Systém musí byť integrovateľný na Arcsight SIEM. • Zabezpečenie: o Šifrovaná databáza obsahujúca zoznam zraniteľností, ktorú dokáže interpretovať len samotný systém na správu zraniteľností. o Podpora šifrovaného prenosu dát medzi agentmi a centrálnym systémom. o Možnosť viacfaktorovej autentifikácie pre správu systému. • Flexibilita nasadenia - Systém musí podporovať lokálnu inštaláciu (on premise) na dedikovaný server.	• Podpora politiky škálovania - Možnosť dynamického pridania IP adries v rámci kapacity 800 adries bez nutnosti rekonfigurácie. • Integrovateľnosť - Schopnosť integrácie s ďalšími bezpečnostnými riešeniami na automatizáciu reakcií na bezpečnostné incidenty, prípadne kontrolu pripojených zariadení do siete (discovery mode). Systém musí byť integrovateľný na Arcsight SIEM. • Zabezpečenie: o Šifrovaná databáza obsahujúca zoznam zraniteľností, ktorú dokáže interpretovať len samotný systém na správu zraniteľností. o Podpora šifrovaného prenosu dát medzi agentmi a centrálnym systémom. o Možnosť viacfaktorovej autentifikácie pre správu systému. • Flexibilita nasadenia - Systém musí podporovať lokálnu inštaláciu (on premise) na dedikovaný server.	
Uchádzač č. 1 splnil požiadavky na predmet zákazky ✓		

Informácia pre uchádzačov: Požiadavky spĺňa napríklad riešenie zn. **Tenable**, typ **Tenable Security Center** v najnovšej stabilnej verzii v čase predkladania ponuky.

Vysvetlivky : ✓ - splnil, **X – nesplnil** (uvedie sa dôvod), **ŽoV – Žiadosť o vysvetlenie ponuky**

Členovia komisie s právom vyhodnocovať ponuky:

Mgr. Jozef Zajíček .....

Mgr. Stanislav Schubert .....

Ing. Ferdinand Vavrík, PhD. .....

Ing. Branislav Brjančin .....

Členovia komisie bez práva vyhodnocovať ponuky:

Mgr. Janka Miltáková, predseda komisie …….....

Mgr. Natália Kozárová …….....

JUDr. Miriam Johanesová …….....

Ing. Silvia Uhnáková …….....