Príloha č. 2 Zmluvy o dodaní diela a poskytovaní expertných služieb v oblasti kybernetickej bezpečnosti

ŠPECIFIKÁCIA POŽIADAVIEK

NÁZOV ZÁKAZKY: Rozvoj kybernetickej bezpečnosti v ZZS Bratislava

Bezpečnostný nástroj 1
(Nástroj na procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti)

Nástroj na procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti musí spĺňať najmenej nasledovné:

Požiadavka	Návrh na plnenie / Dôkaz (doplní uchádzač)
1. Centrálna konzola pre používateľov systému prístupná cez webové prehliadače (minimálne Chrome, Firefox, Safari alebo Edge). 2. Centrálna konzola lokalizovaná v Slovenskom jazyku. 3. Centrálna správa musí byť prevádzkovaná ako SaaS. 4. Podpora požiadaviek legislatívy SR. 5. Centrálny dashboard pre rýchle vyhodnotenie aktív (primárne a podporné), rizík podľa kategórie, rizík podľa hrozieb a zraniteľností, aktuálne dosahovaná úroveň súladu s požiadavkami zákona č. 69/2018 Z. z. a vyhlášky č. 227/2025 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. 6. Podpora prihlásenia prostredníctvom multi-faktorovej autentifikácie. 7. Podpora tvorby klasifikácie informácií a kategorizácie sietí a informačných systémov podľa zákona č. 69/2018 Z.z. a doporučení vyhlášky č. 227/2025 Z. z., vytváranie registrov aktív, hrozieb.	
8. Parametrizácia systému: 8.1. Definovanie metódy na výpočet hodnotenie aktív, 8.2. Definovanie metódy na kategorizáciu rizík, 8.3. Definovanie bezpečnostnej štruktúry spoločnosti (osoby, organizačné jednotky, role), 8.4. Definovanie druhov aktív, 8.5. Definovanie vlastných atribútov aktív, 8.6. Definovanie stupnice pre hodnotenie dôvernosti, dostupnosti, integrity, dopadov, hrozieb a zraniteľností, 8.7. Definovanie bezpečnostných opatrení, 8.8. Register dodávateľov, 8.9. Definovanie kritérií na hodnotenie dodávateľov. 9. Register rizík prostredníctvom, ktorého je možné definovať kombinácie hrozba/zraniteľnosť na konkrétne typy aktív.	

10. Evidencia aktív (manuálne alebo prostredníctvom importu z dátového súboru): 10.1. Všeobecné (druh, typ, lokalita, garant, administrátor, dodávateľ, prevádzkovateľ, závislosť aktíva na iných aktívach) 10.2. Hodnotenie aktíva (dôvernosť, dostupnosť a integrita), 10.3. Identifikácia hrozieb/zraniteľnosti manuálne alebo priamo z registra rizík, 10.4. Spôsob používania a manipulácie, 10.5. Vlastné atribúty. 11. Mapa aktív pre grafické zobrazenie závislostí medzi jednotlivými aktívami: 11.1. Zobrazenie priameho vzťahu aktíva a jeho podriadených a nadriadených aktív, 11.2. Komplexné zobrazenie mapy všetkých aktív, 11.3. Filtrácia zobrazených aktív (druh alebo kategória aktíva).	
12. Hodnotenie rizík: 12.1. Možnosť stiahnuť súbor vo formáte pdf s identifikovanými rizikami pre jedno alebo viaceré aktíva, 12.2. Hodnotenie dopadu identifikovaných rizík, 12.3. Návrh bezpečnostných opatrení pre zníženie rizika na úrovni aktíva, 12.4. Výpočet rizika pred a po opatrení bezpečnostného opatrenia, 12.5. Rozhodnutie o akceptovaní alebo neakceptovaní rizika. 13. Hodnotenie opatrení: 13.1. Zoznam rizík, ktoré bezpečnostné opatrenie rieši, 13.2. Aplikovateľnosť bezpečnostného opatrenia, 13.3. Zavedenie bezpečnostného opatrenia a jeho riadenie (ľudské a finančné zdroje, časový harmonogram, evidencia komunikácie riešiteľského tímu) 14. Plán zvládania rizík pre riadenie implementácie bezpečnostných opatrení: 14.1. Evidencia požiadaviek na ľudské a finančné zdroje, 14.2. Dátum začatia a ukončenie implementácie, 14.3. Diskusný priestor pre riešiteľský tím.	
15. Hodnotenie dodávateľov: 15.1. Hodnotenie atribútov dodávateľov aktív, 15.2. Mapovanie dodávateľov na konkrétne aktíva, 15.3. Možnosť evidencie podpornej dokumentácie k dodávateľov (zmluvy, SLA).	
16. Evidencia plnenia požiadaviek legislatívy: 16.1. zákon č. 69/2018 Z. z. a vyhláška NBÚ č. 227/2025 Z. z. 16.2. Jednotlivé požiadavky môžu byť v stave zavedené, v procese zavádzania, neaplikované alebo nezavedené,	

16.3. Ku každej požiadavke je možné pripojiť komentár a záznam zo zoznamu bezpečnostných opatrení, 16.4. Hodnotenie je možné exportovať do súboru vo formáte pdf.	
17. Plán kontinuity: 17.1. Všeobecné údaje o pláne kontinuity (názov, popis, dotknuté aktíva), 17.2. Definovanie členov analytického, výkonného a riadiaceho tímu, 17.3. Popis procesu a dokumentácia, 17.4. Export plánu obnovy do súboru.	
18. Auditný log pre zaznamenávanie aktivít v systéme: 18.1. Systém zaznamenáva aktivitu používateľa (pridanie, zmena, vymazanie) pre konkrétne časti systému (aktívum, atribút aktíva, riziko), 18.2. Možnosť pozrieť stav pred vykonanou zmenou a po zmene.	

Bezpečnostný nástroj 2

(Nástroj pre ochranu perimetra – Next Generation Firewall)

Riešenie musí spĺňať minimálne nasledujúce technické a funkčné požiadavky:

Požiadavka	Návrh na plnenie / Dôkaz (doplní uchádzač)
1. HW appliance NGFW/UTM firewallu v režime vysokej dostupnosti (dve fyzické zariadenia rovnakého typu zapojené do funkčného clustra). 2. Platforma postavená na HW akcelerovanej architektúre (t.j. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií. 3. HW appliance do racku s veľkosťou 1RU. 4. Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu. 5. Zariadenie vybavené dvoma zdrojmi energie pre možnosť zabezpečenia redundancie napájania (interné alebo pripojené externe).	
6. Rozhrania na každom firewalle využiteľné pre management min. 1x GE RJ45. 7. Rozhrania na každom firewalle využiteľné pre spracovanie komunikácie min. 16x GE RJ45 Ports, 8x GE SFP Slots, 4x 10 GE SFP+ Slots. 8. Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky. 9. Podpora VLAN, LACP.	
10. Počet FW pravidiel min. 8000. 11. Možnosť definície FW pravidiel v tzv. NGFW režime (t.j. súčasťou základnej definície FW pravidla) min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.	
12. Celková priepustnosť firewallu min. 27/27/11 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B). 13. Latencia firewallu nepresahuje 5 µs (merané na malých UDP paketoch (64B)). 14. Počet nových spojení za sekundu (setup-rate) min. 270000. 15. Celkový počet súčasných TCP spojení firewallu min. 3000000. 16. PPS (počet spracovaných paketov za 1 sekundu) min. 16000000.	
17. Funkcia detekcie aplikácií na L7 (Application Control). 18. Detekcia známych aplikácií na základe signatúr (aplikácií/signatúr). 19. Pre cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa	

požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii). 20. Aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu. 21. Priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response) min. 12 Gbps. 22. Podpora použitia Application control aj formou profilov priradených k pravidlám.	
23. Funkcie detekcie a zamedzenia narušení (IPS/IDS). 24. Počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom min. 11000. 25. Funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám. 26. Možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS. 27. Priepustnosť funkcie IPS vrátane logovania min. 5 Gbps.	
28. Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom. 29. AV kontrola rozšírená o inšpekciu tzv. sandbox technikou: Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky. 30. Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním min. 3 Gbps. 31. Podpora služby výrobcu umožňujúca detegovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hash-ov. 32. Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky.	
33. Podpora SSL dešifrovania/SSL inšpekcie min. 4 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou). 34. Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii. 35. Možnosť definovať vlastný tzv. blacklist domén. 36. Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL. 37. Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos. 38. Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom server. 39. Podpora SSL VPN. 40. Priepustnosť SSL VPN min. 2 Gbps. 41. Podpora IPSEC VPN v režime site-2-site aj client-2-site.	

42. Priepustnosť IPSEC VPN (AES256-SHA256, UDP packet size 512B) min. 12 Gbps.	
43. Podpora izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod. 44. FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu. 45. Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky.	
46. Podpora SNMP vrátane SMPB MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete. 47. Požaduje sa certifikácia ICSA Labs minimálne pre Firewall. 48. Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať. 49. Možnosť kombinovať akcie pre automatizačné pravidlá min. webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy. 50. Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel min. schopnosť parsovať vstupy z logov a z predchádzajúcich vykonaných akcií. 51. Podpora otvoreného API pre ďalšie možnosti integrácie.	

Bezpečnostný nástroj 3
(Systém ochrany kritických prvkov infraštruktúry)

Požiadavka	Návrh na plnenie / Dôkaz (doplní uchádzač)
A. Systém ochrany kritických prvkov infraštruktúry musí spĺňať nasledovné certifikačné požiadavky alebo ekvivalent: • ISO 27001 • ISO 27014 • ISO 27034-1 • ISO 27017 • SOC 2/SOC 3	
B. Všeobecné požiadavky pre systém ochrany kritických prvkov infraštruktúry 1. Musí byť dodaný formou SaaS, pričom centrálna konzola beží v cloud prostredí a agenti a sieťové kolektory sú inštalovaní na koncových bodoch. 2. Všetky požadované funkcie týkajúce sa koncového bodu, sú vykonávané výhradne jediným agentom bežiacim na koncovom bode. 3. Riešenie používa systém licencií založený na kreditoch, ktorý umožňuje flexibilné prideľovanie bezpečnostných služieb na základe potrieb organizácie. Kredity možno prideliť rôznym funkciám, ako sú napríklad správa kybernetických rizík, senzory XDR, ochrana koncových bodov, zabezpečenie cloudu a nástroje na hodnotenie rizík. Jednotná konzola na správu poskytuje prehľad o využívaní kreditov, čo umožňuje správcom optimalizovať prideľovanie zdrojov a dynamicky škálovať pokrytie zabezpečenia. 4. Riešenie musí poskytovať jednotné správcovské rozhranie pre správu všetkých komponentov platformy. 5. Riešenie musí poskytovať možnosť konfigurácie politík pre všetky technické opatrenia z jedného miesta. 6. Riešenie musí umožňovať pridávať alebo odoberať funkcionality podľa potrieb organizácie. 7. Riešenie musí umožňovať integráciu nových technických opatrení bez potreby komplexných zmien v existujúcej infraštruktúre. 8. Riešenie musí umožňovať správu poskytovateľov identít: 8.1. podporovať SAML 2.0 pre single sign-on (SSO) integráciu s korporátnymi poskytovateľmi identity, 8.2. umožňovať pridanie nového poskytovateľa identity pomocou nahrania XML súboru s metadátami IdP, 8.3. umožňovať synchronizáciu informácií o skupine s IdP pre SAML skupinové účty, 8.4. umožňovať pozývanie individuálnych SAML užívateľov na prihlásenie do konzoly pomocou IdP, 8.5. umožňovať pozývanie viacerých užívateľov z distribučnej skupiny na prihlásenie do konzoly pomocou IdP, 8.6. podporovať synchronizáciu informácií o skupine s IdP a overenie emailových adries užívateľov pred	

prihlásením, 8.7. umožňovať pridanie viacerých užívateľov z priradenej skupiny na prihlásenie pomocou IdP, pričom nie je potrebná synchronizácia skupinových informácií ani overenie emailových adries, 8.8. umožňovať nastavenie a správu prístupových oprávnení pre užívateľov a skupiny definované IdP, 8.9. podporovať dvojfaktorovú autentifikáciu pre miestne účty a špecifikované operácie v konzole, 8.10. podporovať pridanie a správu viacerých poskytovateľov identity pre rôzne časti organizácie alebo pre rôzne aplikácie, 8.11. umožňovať intuitívne pridanie a konfiguráciu poskytovateľov identity cez administratívne rozhranie, 8.12. umožňovať nastavenie politík a pravidiel pre skupiny užívateľov cez poskytovateľov identity, 9. Riešenie musí umožňovať správu účtov: 9.1. vytvorenie nových užívateľských účtov pre autorizovaných užívateľov na prístup ku konzole, 9.2. vytvorenie účtu, 9.3. úpravu detailov existujúcich účtov ako napríklad rola a popis, 9.4. úpravu účtu kliknutím na účet a následnou úpravou detailov, 9.5. výber a zmazanie jedného alebo viacerých účtov, 9.6. povolenie alebo zakázanie účtov pomocou prepínača v stĺpci, 10. Riešenie musí umožňovať správu užívateľských účtov a rolí: 10.1. SAML single sign-on (SSO), 10.2. správa individuálnych užívateľských účtov a ich viditeľnosti aktív, 10.3. vytváranie a úpravu vlastných užívateľských rolí, 10.4. priradenie povolení pre rôzne aplikácie v rámci platformy, 10.5. preddefinované roly, ktoré nemôžu byť upravené ani zmazané, a podporu vlastných rolí, ktoré môžu byť upravované a kopírované, 10.6. zapnutie alebo vypnutie 2FA pre lokálne účty, 10.7. integráciu s externými poskytovateľmi identity, 10.8. mapovanie užívateľských skupín z tretích strán na roly v platforme, 10.9. definovanie rozsahov viditeľnosti aktív pre jednotlivých užívateľov. 11. Riešenie musí umožňovať správu aktív v rôznych bezpečnostných doménach (email, cloud, sieť, mobil, identita a dáta). 12. Riešenie musí poskytovať jednotné rozhranie pre sledovanie bezpečnostných udalostí zo všetkých zdrojov 13. Riešenie musí umožňovať vytvárať a spúšťať automatizované workflow pre bežné bezpečnostné operácie (automatická reakcia na incident, pravidelné spustenie skriptu,..) 14. Riešenie musí poskytovať centralizovaný prehľad všetkých spravovaných zariadení a systémov 15. Riešenie musí poskytovať automatická detekcia a kategorizácia nových zariadení v sieti	

16. Riešenie musí podporovať: 16.1. integráciu s Microsoft Information Protection (MIP) pre dešifrovanie a skenovanie šifrovaných emailov a súborov, 16.2. integráciu s Microsoft Identity Protection (MS Entra ID) pre riadenie prístupu rizikových používateľov, 16.3. integráciu s bežnými SIEM a SOAR produktmi, 16.4. integráciu s riešeniami 3. strán pre Single Sign-On (SSO), 16.5. generovanie API kľúčov s kontrolou prístupu založenou na rolách, 16.6. schopnosť integrácie s ďalšími riešeniami tretích strán cez API. 17. Riešenie musí mať pripravené konektory pre integráciu s podporovanými bezpečnostnými riešeniami tretích strán 18. Riešenie musí mať otvorené API pre prepojenie s inými systémami 19. Riešenie musí byť schopné integrovať sa s aspoň jedným riešením tretej strany v nasledujúcich kategóriách: 19.1. Hodnotenie a simulácia narušenia bezpečnosti (BAS) 19.2. Cloudové služby 19.3. Firewall a sieť 19.4. Správa IT služieb (ITSM) 19.5. Správa identity a prístupu (IAM) 19.6. SIEM 19.7. SOAR 19.8. Threat Intelligence 19.9. Správa zjednotených koncových bodov (UEM) 19.10. Správa zraniteľností 20. Riešenie musí podporovať import dát z externých zdrojov hrozieb 21. Riešenie musí podporovať natívny import dát o zraniteľnostiach zo skenerov zraniteľností (minimálne Tenable, Rapid7 alebo Qualys) 22. Riešenie musí poskytovať rozhranie AI chatbox pre zefektívnenie práce (vysvetlenie skriptu, interpretácia udalosti, vytvorenie vyhľadávacieho dotazu,..) 23. Riešenie musí poskytovať retenciu údajov z agentov nasadených na koncových bodoch, ktoré sú uložené v centrálnom úložisku, po dobu minimálne 30 dní. Údajmi sa rozumejú všetky telemetrické dáta alebo nespracované (tzv. raw) udalosti (spustenie procesu, príkazu alebo inej aktivity na koncovom bode), ktoré riešenie z koncového bodu kontinuálne získava. 24. Riešenie musí poskytovať možnosť dodatočne rozšíriť retenciu údajov (samotné rozšírenie retencie nie je predmetom verejného obstarávania, čiže uvedená aktivita nebude realizovaná úspešným uchádzačom v	

rámci tohto verejného obstarávania a nevstupuje do ceny). 25. Riešenie musí zabezpečiť, aby všetky požadované funkcionality pre nástroj definované v tomto dokumente boli zabezpečené na koncovom bode jedným agentom a boli dostupné na všetkých podporovaných operačných systémoch koncových bodov, ak sú relevantné pre daný operačný systém.	
C. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Agentské a bezagentské riešenie 1. Riešenie musí podporovať hybridnú cloudovú stratégiu naprieč on-premise a multi-cloud (AWS, Azure, GCP) prostrediami. 2. Riešenie musí byť schopné podporovať on-prem a cloudové aktíva vrátane fyzických, virtuálnych, cloudových, kontajnerových a serverless aktív. 3. Riešenie bezpečnosti kontajnerov musí podporovať cloudové aj on-prem kontajner platformy. 4. Riešenie podporuje natívnu bezagentskú integráciu na Kubernetes. 5. Workload agent riešenia musí podporovať platformy Windows Endpoint aj Server. 6. Riešenie musí podporovať nasadenie v perzistentných a neperzistentných VDI prostrediach. 7. Riešenie musí podporovať multi-session VDI riešenia bez zmeny alebo obmedzenia funkcionality virtuálnych desktopových operačných systémov verejného obstarávateľa. 8. Riešenie musí podporovať staršie a menej bežné operačné systémy vrátane, ale nielen, Windows XP, Windows 7, Red Hat, Solaris, AIX a ďalších. 9. Agent je možné nainštalovať minimálne na nasledujúce platformy a OS: 9.1. Všetky aktuálne podporované verzie Microsoft Windows 7, 8, 10 a 11, 9.2. Všetky aktuálne podporované verzie Windows Server 2012 R2, 2016 štandard aj core, 2019 štandard aj core, 2022 štandard aj core.	
D. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Bezpečnosť workloadov 1. Riešenie musí ponúkať komplexné schopnosti ochrany serverov a workloadov proti známym aj neznámym hrozbám. 2. Riešenie musí poskytovať hĺbkovú ochranu založenú na: 2.1. Posilňovanie bezpečnosti (Hardening), konfigurácia a skenovanie zraniteľností 2.2. Monitorovanie a správa integrity systému 2.3. Kontrola aplikácií/whitelisting 2.4. Ochrana pamäte 2.5. Server EDR 2.6. Hostiteľský IPS (HIPS) s virtuálnym patchovaním zraniteľností 2.7. Skenovanie antimalvérom 3. Riešenie musí ponúkať kombináciu ochrany proti malvéru založenej na signatúrach, behaviorálnej analýze a analýze na báze umelej inteligencie/strojového učenia.	

4. Strojové učenie musí zahŕňať ako pred-spúšťaciu inteligenciu (extrahovanie vlastností súborov), tak aj analýzu správania súborov/procesov v reálnom čase na identifikáciu hrozieb. 5. Riešenie musí obsahovať modul na monitorovanie správania, ktorý neustále sleduje workloady na neobvyklé modifikácie operačného systému alebo nainštalovaného softvéru, aby poskytol dodatočnú ochranu pred programami vykazujúcimi škodlivé správanie. 6. Riešenie musí mať anti-exploit funkcionalitu na ukončenie programu, ktorý vykazuje abnormálne správanie spojené s exploit útokmi. Musí byť schopné detegovať viaceré techniky exploitov pomocou mechanizmov ako Data Execution Prevention (DEP), Structured Exception Handling Overwrite Protection (SEHOP) a prevencia heap spray útokov. 7. Riešenie musí poskytovať ochranný mechanizmus proti ransomvéru. V prípade kompromitácie stroja musí riešenie chrániť dokumenty pred neoprávneným šifrovaním alebo modifikáciou. 8. Riešenie musí byť schopné vytvárať kópie súborov šifrovaných ransomvérom na koncovom bode a musí byť schopné obnoviť postihnuté súbory do pôvodného stavu. 9. Riešenie musí byť schopné identifikovať komunikáciu cez HTTP/HTTPS protokoly a bežne používané HTTP porty, detegovať/predchádzať komunikácii s globálnymi C&C servermi a umožniť administrátorom vytvárať vlastné zoznamy povolených/blokovaných adries. 10. Riešenie musí mať integrovanú schopnosť virtuálneho patchovania (Vulnerability Shielding) na poskytovanie včasnej ochrany pred zraniteľnosťami naprieč rôznymi koncovými bodmi a servermi. 11. Riešenie musí podporovať host-based firewall so stavovou inšpekciou a možnosťou vytvárať pravidlá na základe zdroja/cieľa/portu/protokolu/aplikácie pre stavovú inšpekciu a vysoko výkonné skenovanie sieťového prenosu na prítomnosť vírusov. 12. Riešenie musí mať integrovaný modul na kontrolu aplikácií (Application Control) na posilnenie obrany proti malvéru a cieleným útokom tým, že zabráni spúšťaniu neznámych a nechcených aplikácií na firemných koncových bodoch. 13. Riešenie musí mať schopnosť kontroly zariadení (Device Control) a musí byť schopné obmedziť prístup k zariadeniam na koncových bodoch/serveroch priradením práv na plný prístup, iba na čítanie a blokovanie. Musia byť kontrolovateľné minimálne tieto typy zariadení: 13.1. USB Mass Storage 13.2. Funkcia USB Autorun 13.3. Mobilné zariadenia (MTP/PTP) 14. Riešenie musí mať služby na čistenie škôd (damage cleanup) na automatizované odstránenie zmien vykonaných malvérom, vrátane sieťových a súborových škodlivých aplikácií a zvyškov vírusov a červov (Trojany, záznamy v registroch, vírusové súbory). 15. Riešenie musí mať vstavaný modul na monitorovanie integrity (Integrity Monitoring) na skenovanie neočakávaných zmien v hodnotách a kľúčoch registrov, službách, procesoch, nainštalovanom softvéri,	

portoch a súboroch na agentoch. 16. Riešenie musí mať vstavaný modul na inšpekciu logov (Log Inspection) na identifikáciu dôležitých udalostí, ktoré by mohli byť skryté v logoch operačného systému a aplikácií. Riešenie musí byť schopné posielať tieto udalosti do SIEM systému alebo centralizovaného logovacieho servera na koreláciu, reportovanie a archiváciu. 17. Riešenie musí podporovať host-based ochranu pre hostiteľov kontajnerov s real-time antimalvérovým skenovaním a službami prevencie prienikov na ochranu bežiacich kontajnerov pred vzdialenými exploitmi softvérových zraniteľností. 18. Riešenie musí byť schopné aplikovať nastavenia firewallu na sieť kontajnerov a poskytovať optimálnu inšpekciu sieťového prenosu kontajnerov, vrátane east-west komunikácie medzi kontajnermi. 19. Riešenie musí mať schopnosti skenovania kontajnerov pred spustením (pre-runtime) aj počas behu (runtime). 20. Riešenie musí byť schopné chrániť kontajnery počas celého ich životného cyklu (pri nasadení, po nasadení, počas behu). 21. Riešenie musí pomáhať riešiť zraniteľnosti a iné bezpečnostné problémy v obrazoch kontajnerov predtým, ako môžu byť zneužité v produkcii. 22. Riešenie musí byť schopné integrovať bezpečnosť do CI/CD pipeline bez narušenia vývojových cyklov. 23. Riešenie musí byť schopné generovať Softvérový zoznam (Software Bill of Materials - SBOM) a vrátiť report o zraniteľnostiach po vykonaní skenovania výsledkov SBOM.	
<u>E. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Bezpečnosť kontajnerov</u> 1. Riešenie musí byť schopné skenovať obrazy kontajnerov ako súčasť vývojovej pipeline a vykonávať priebežné skenovanie obrazov v registroch verejného obstarávateľa. 2. Riešenie musí podporovať funkcionalitu Admission Controller založenú na politikách. 3. Riešenie musí mať možnosť vytvárať vlastné politiky, ktoré povoľujú alebo blokujú nasadenia na základe definovaného súboru pravidiel kontroly prístupu. 4. Riešenie musí byť schopné integrovať výsledky skenovania artefaktov do politík kontroly prístupu pre bezpečnosť kontajnerov. 5. Riešenie musí podporovať skenovanie malvéru/hrozieb v kontajneroch. 6. Riešenie musí mať bezpečnostné schopnosti pre behové prostredie (runtime security) a poskytovať upozornenia a indikátory útokov (IoA) naprieč bežiacimi kontajnerizovanými aplikáciami. 7. Riešenie musí mať skenovanie zraniteľností kontajnerov počas behu (runtime). 8. Riešenie musí podporovať eBPF runtime security. 9. Riešenie musí podporovať skenovanie malvéru/hrozieb, skenovanie tajomstiev (secret scan) a skenovanie zraniteľností pred spustením (pre-runtime). 10. Riešenie musí poskytovať viditeľnosť do kontajnerov/clusterov.	

11. Riešenie musí poskytovať funkcie správy kontajnerov/clusterov s kontrolou rozsahu na základe rolí (RBAC). 12. Riešenie musí poskytovať kontrolu a reportovanie zhody pre k8s (napr. CIS EKS a K8s scan report).	
F. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Detekcia a reakcia 1. Riešenie musí byť schopné zbierať dáta o aktivitách v reálnom čase z objavených cloudových aktív na účely korelácie a obohatenia XDR a automaticky synchronizovať dáta späť do cloudovej manažment konzoly. 2. Riešenie musí mať preddefinované detekčné modely špecifické pre workloady a kontajnery, ktoré kombinujú viaceré pravidlá a filtre udalostí s použitím techník ako strojové učenie a data stacking. 3. Riešenie musí mať schopnosť povoliť alebo zakázať detekčné modely a pridávať/konfigurovať výnimky detekčných modelov v závislosti od potrieb prostredia. 4. Riešenie musí umožňovať vytváranie vlastných detekčných modelov a vlastných filtrov udalostí, ktoré definujú udalosti, ktoré model používa na spustenie upozornení. 5. Riešenie musí mapovať všetky Indikátory útokov (IOA), do rámca MITRE ATT&CK, ktoré môže SOC analytik použiť ako východiskový bod pre ďalšie vyšetrovanie. 6. Konzola musí poskytovať rôzne metódy vyhľadávania, filtre a ľahko použiteľný dopytovací jazyk podobný Kibane na identifikáciu, kategorizáciu a získavanie výsledkov vyhľadávania. 7. Riešenie musí mať schopnosť vyhľadávať v dátach o aktivite workloadov alebo kontajnerov, písať vlastné vyhľadávacie dopyty, pridávať uložené dopyty do watchlistu a automaticky ich spúšťať proti najnovším telemetrickým dátam v pravidelných intervaloch. 8. Riešenie musí byť schopné generovať konsolidovanxý alert a prezentovať analýzu príčin (root cause analysis) – vrátane asociovaných MITRE ATT&CK TTPs – a identifikovať rozsah dopadu naprieč cloudovými aktívami. 9. Riešenie musí umožňovať vykonávanie reakčných akcií priamo z kontextového menu v rámci okna vyšetrovania. 10. Riešenie musí byť schopné vykonávať reakčné akcie na obmedzenie incidentov v cloudovom účte verejného obstarávateľa, ako napríklad odobratie prístupu podozrivým IAM používateľom. 11. Riešenie musí podporovať ďalšie reakčné akcie využívajúce integráciu s tretími stranami, ako sú ticketingové systémy. 12. Riešenie musí podporovať Playbooks na prechod od manuálnej reakcie k automatizovaným workflow, čo pomáha znižovať záťaž a zrýchľovať bezpečnostné úlohy a vyšetrovania. 13. Riešenie musí zahŕňať schopnosť vytvárať playbooks proti hrozbám a rizikám, ako je ukončenie procesu, vypnutie koncového bodu, odpojenie koncového bodu od internetu, presun súborov do karantény, mazanie škodlivých súborov atď. 14. Riešenie musí mať schopnosť vytvárať playbooks od nuly alebo používať vstavané šablóny v závislosti od	

potrieb prostredia. 15. Riešenie musí podporovať XDR monitoring vášho cloudového účtu (napr. AWS CloudTrail) na získanie akčných prehľadov o aktivite používateľov, služieb a zdrojov s detekčnými modelmi identifikujúcimi aktivity ako eskalácia privilégií, modifikácia hesiel a iné útočné techniky. 16. Riešenie musí byť schopné integrovať sa s kybernetickou bezpečnostnou platformou, ktorá dokáže spravovať riešenia organizácie pre Endpoint, Email, Cloud, Network, OT Security, XDR a Zero Trust v jednej konzole.	
G. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Riadenie kybernetických rizík 1. Riešenie musí byť schopné kontinuálne identifikovať, kategorizovať a dokumentovať všetky aktíva v rámci digitálneho ekosystému organizácie, vrátane: 1.1. Aktív prístupných z internetu (EASM) 1.2. Interných zariadení 1.3. Používateľských účtov 1.4. Aplikácií 2. Musí poskytovať kontextuálnu viditeľnosť do všetkých aktív, vrátane: 2.1. Kritickosti na základe atribútov a aktivity aktíva, 2.2. Grafickej prezentácie vzťahov medzi aktívami, 2.3. Historických výsledkov hodnotenia rizík. 3. Musí umožňovať správu všetkých objavených aktív z jedinej unifikovanej manažérskej konzoly. 4. Musí byť schopné integrácie s kybernetickou bezpečnostnou platformou, ktorá môže spravovať Endpoint, Email, Cloud, Network, OT Security, XDR a Zero Trust riešenia organizácie v jedinej konzole. 5. Musí umožňovať integráciu s riešeniami tretích strán pre príjem alebo obohatenie dát o útočnej ploche. 6. Musí poskytovať funkcionalitu analýzy cesty útoku, ktorá dokáže identifikovať a predpovedať potenciálne útoky z externých na interné kritické aktíva. 7. Musí mať vstavané bezpečnostné playbooky pre automatizovanú nápravu. 8. Musí byť schopné hodnotenia bezpečnostného stavu internetových a iných externe prístupných aktív organizácie (External Attack Surface Management). 9. Musí byť schopné poskytovať analýzu cesty útoku, ktorá identifikuje a predpovedá potenciálne útoky z externých aktív so zraniteľnosťami a nesprávnymi konfiguráciami na interné kritické aktíva. 10. Musí byť schopné poskytovať analýzu cesty útoku, ktorá identifikuje a predpovedá potenciálne útoky z interných aktív na iné interné kritické aktíva.	
H. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Hodnotenie rizík 1. Musí poskytovať celkové skóre rizika organizácie založené na kontinuálnom hodnotení rizík v organizácii. 2. Musí poskytovať index expozície, ktorý sumarizuje pravdepodobnosť výskytu exploitu alebo hrozby v	

prostredí. 3. Musí poskytovať index útoku, ktorý sumarizuje počet známych detekcií, ovplyvnených aktív a závažnosť každej unikátnej hrozby v prostredí. 4. Musí poskytovať index bezpečnostnej konfigurácie, ktorý sumarizuje nasadené a chýbajúce bezpečnostné kontroly v prostredí. 5. Musí zahŕňať kritickosť aktív, zraniteľnosti, aktivitu hrozieb a konfiguráciu bezpečnostných kontrol do výpočtu skóre rizika pre každý typ aktíva. 6. External Attack Surface Management (EASM) 7. Musí byť schopné zobraziť všetky domény a subdomény patriace organizácii a poskytovať trend dát o objavovaní domén mesačne za aspoň jeden rok. 8. Musí byť schopné zobraziť všetky verejné IP adresy patriace organizácii a poskytovať trend dát o objavovaní IP aktív mesačne za aspoň jeden rok. 9. Musí poskytovať pre aktíva prístupné z internetu najnovšie skóre rizika, poskytovateľa hostingu, služby, porty a čas posledného výskytu. 10. Musí poskytovať hodnotenie rizík pre každú doménu a IP adresu a priradiť im skóre rizika, ktoré možno sledovať v čase. Musí zobrazovať indikátory rizík vrátane typu rizík, udalostí a úrovne rizika pre každé objavené riziko. 11. Musí byť schopné zobraziť graf aktív pre každú doménu a IP aktívum, ktorý graficky znázorňuje spojenie aktíva s internými aktívami v prostredí. 12. Musí poskytovať skóre kritickosti aktíva pre každú doménu a IP aktívum. Administrátori by mali mať možnosť manuálne meniť kritickosť aktíva. 13. Musí byť schopné sumarizovať lokácie IP adries podľa krajiny a zobraziť ich na mape. 14. Musí umožňovať pridávanie firemných domén, subdomén a IP adries pre objavovanie.	
I. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry – Aktíva 1. Musí využívať viacero zdrojov dát pre objavovanie (existujúci agent by mal byť doplnený dodatočnými zdrojmi objavovania). 2. Musí poskytovať pre interné aktíva zariadení najnovšie skóre rizika, OS, IP adresu, posledného používateľa, zraniteľnosti, zdroj objavenia a časy prvého a posledného výskytu. 3. Musí poskytovať hodnotenie rizík pre každé aktívum zariadenia a priradiť mu skóre rizika, ktoré možno sledovať v čase. Musí zobrazovať indikátory rizík vrátane typu rizík, udalostí a úrovne rizika pre každé objavené riziko. 4. Musí byť schopné zobraziť graf aktív pre každé aktívum zariadenia, ktorý graficky znázorňuje spojenie aktíva s inými aktívami v prostredí. 5. Musí poskytovať skóre kritickosti aktíva pre každé aktívum zariadenia. Administrátori by mali mať možnosť manuálne meniť kritickosť aktíva.	

6. Musí identifikovať spravované a nespravované zariadenia. 7. Musí byť schopné zobraziť všetky objavené interné aktíva zariadení a ukázať trend objavovania mesačne za aspoň jeden rok. 8. Musí zobrazovať využitie cloudových aplikácií a aktivitu zariadenia. 9. Musí zobrazovať využitie schválených a neschválených cloudových aplikácií zariadením. 10. Musí zobrazovať aktivitu zariadenia zobrazením jeho lokácie na mape. 11. Musí zobrazovať prihlásených používateľov zariadenia vrátane používateľského mena, emailovej adresy, lokácie, pracovnej pozície a skóre rizika používateľa. 12. Musí poskytovať súhrn zariadenia vytvorením profilu aktíva. Detaily by mali zahŕňať základné informácie o zariadení, aktivitu, využitie zariadenia, informácie o pripojení, vplyv a riziko postúry identity. 13. Musí umožňovať vykonávanie akcií odozvy (napr. izolácia, vzdialený shell, spustenie vlastného skriptu) a Zero Trust akcií (napr. blokovanie prístupu k aplikácii alebo cloudovej aplikácii) na aktívach zariadení.	
J. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry – Účty a identity 1. Musí využívať viacero zdrojov dát identít pre objavovanie 2. Musí identifikovať doménové aj servisné účty. 3. Musí poskytovať pre účty najnovšie skóre rizika, typ používateľa, rolu, lokáciu, pracovnú pozíciu a časy prvého a posledného výskytu. 4. Musí poskytovať hodnotenie rizík pre doménové aj servisné účty a priradiť im skóre rizika, ktoré možno sledovať v čase. Musí zobrazovať indikátory rizík vrátane typu rizík, udalostí a úrovne rizika pre každé objavené riziko. 5. Musí byť schopné zobraziť graf aktív pre doménové aj servisné účty, ktorý graficky znázorňuje spojenie účtu s inými aktívami v prostredí. 6. Musí poskytovať skóre kritickosti pre doménové aj servisné účty. Administrátori by mali mať možnosť manuálne meniť hodnotenie kritickosti účtu. 7. Musí identifikovať exponované API spojené s objavenými servisnými účtami. 8. Musí identifikovať role aplikácií pridelené objaveným servisným účtom. 9. Musí identifikovať udelené súhlasy s oprávneniami pre objavené servisné účty. 10. Musí byť schopné zobraziť všetky objavené účty a ukázať trend objavovania účtov mesačne za aspoň jeden rok. 11. Musí zobrazovať využitie cloudových aplikácií a aktivitu účtu. 12. Musí zobrazovať využitie schválených a neschválených cloudových aplikácií účtom. 13. Musí zobrazovať aktivitu účtu zobrazením dát o prihlásení na mape. 14. Musí poskytovať podrobné informácie o účte vytvorením profilu aktíva. Detaily by mali zahŕňať základné informácie o účte, aktivitu, využitie zariadenia, informácie o využití emailu, vplyv a riziko postúry identity. 15. Musí umožňovať vykonávanie akcií odozvy (napr. izolácia, vzdialený shell, spustenie vlastného skriptu) a	

Zero Trust akcií (napr. blokovanie prístupu k aplikácii alebo cloudovej aplikácii) na aktívach zariadení spojených s účtom.	
K. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry – Aplikácie 1. Musí identifikovať cloudové aj lokálne aplikácie. 2. Musí umožňovať nastavenie cloudovej aplikácie ako schválenej alebo neschválenej. 3. Musí poskytovať pre aplikácie najnovšiu úroveň rizika, kategóriu, ktorí používatelia aplikáciu používajú, na ktorých zariadeniach sa k aplikácii pristupovalo, využitie aplikácie, či je aplikácia schválená, pracovnú pozíciu a čas posledného výskytu. 4. Musí poskytovať úroveň rizika pre cloudové aj lokálne aplikácie a priradiť im úroveň rizika (ktorú možno upraviť). Musí zobrazovať informácie o súlade pre cloudové aplikácie. 5. Musí zobrazovať využitie cloudových aplikácií podľa lokácie. 6. Musí zobrazovať využitie cloudových aplikácií podľa používateľov. 7. Musí zobrazovať využitie cloudových aplikácií podľa zariadení. **L. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry – Správa zraniteľností** 1. Musí poskytovať metriky správy zraniteľností pre interné aj internetové aktíva v priebehu času a umožniť porovnanie skóre organizácie s globálnym priemerom. Metrika: Vysoko zneužiteľné unikátne CVE. 2. Musí poskytovať metriky správy zraniteľností pre interné aj internetové aktíva v priebehu času a umožniť porovnanie skóre organizácie s globálnym priemerom. Metrika: Priemerný čas na opravu. 3. Musí poskytovať metriky správy zraniteľností pre interné aj internetové aktíva v priebehu času a umožniť porovnanie skóre organizácie s globálnym priemerom. Metrika: Priemerný čas bez opravy. 4. Musí poskytovať metriky správy zraniteľností pre interné aj internetové aktíva v priebehu času a umožniť porovnanie skóre organizácie s globálnym priemerom. Metrika: Zraniteľné koncové body. 5. Musí podporovať automatizačné/playbookové akcie pre udalosti detekcie zraniteľností. 6. Hodnotenie a prioritizácia zraniteľností by mali byť založené na externých faktoroch (threat intelligence, napr. či je CVE vysoko aktívne zneužívané) aj interných faktoroch (kritickosť aktíva, pokusy o zneužitie na základe detekčných logov) a bezpečnostných kontrolách (virtuálna záplata prostredníctvom IPS pravidla). 7. Musí poskytovať schopnosť detekcie zero-day zraniteľností a virtuálne záplatovanie prostredníctvom IPS pravidla na zmiernenie zero-day zraniteľností.	
M. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Náprava a zmiernenie 1. Musí automatizovať a orchestrovať akcie odozvy na zmiernenie rizík a reakciu na hrozby pomocou pokročilých AI a ML technológií. 2. Musí poskytovať kroky nápravy pre všetky objavené rizikové faktory. 3. Musí umožňovať nastavenie cieľa pre opatrenia na zníženie rizika. Musí poskytovať spôsob zníženia úrovne rizika organizácie (napr. z vysokého rizika na nízke riziko) ponúknutím zoznamu odporúčaní. 4. Musí sledovať objavené rizikové udalosti špecifikovaním stavu nápravy pre každú objavenú udalosť. Malo	

by byť možné priradiť stav každej udalosti (napr. Napravené, Zamietnuté atď.).	
N. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Modelovanie útočných ciest 1. Riešenie musí poskytovať funkcionalitu predikcie útočných ciest (Attack Path Prediction), ktorá analyzuje aktíva a ich vzťahy a identifikuje potenciálne útočné cesty na základe detegovaných rizikových udalostí na ohrozených vstupných bodoch. 2. Analýza útočných ciest musí byť vykonávaná minimálne na dennej báze a údaje pre analýzu musia byť zhromažďované z pripojeného bezpečnostného riešenia a z externých zdrojov tretích strán. 3. Riešenie musí byť schopné detegovať útočné cesty ešte predtým, ako sú tieto cesty zneužité útočníkmi, a to pomocou detekcie hrozieb, analýzy správania, skenovania zraniteľností a nesprávnych konfigurácií, ako aj analýzy vzťahov a profilov aktív. 4. Riešenie musí využívať generatívnu umelú inteligenciu na určenie aktív, ktoré budú pravdepodobne použité ako vstupné body, ktoré aktíva sú pravdepodobnými cieľmi, akú konkrétnu cestu môže útočník využiť a aké kroky sú potrebné na nápravu týchto aktív. 5. Riešenie musí poskytovať holistický pohľad na všetky potenciálne útočné cesty v organizácii, čo umožňuje porozumieť rizikám na vstupných bodoch, identifikovať kľúčové body, ktoré by mohli uľahčiť viacero útočných ciest, a prijať proaktívne nápravné opatrenia. 6. Keď riešenie identifikuje potenciálnu útočnú cestu, musí byť vygenerovaná príslušná riziková udalosť útočnej cesty popri rizikových udalostiach detegovaných na súvisiacich aktívach. Tieto udalosti musia ovplyvňovať celkový Index rizika organizácie. 7. Riešenie musí podporovať automatické a manuálne možnosti nápravy rizikových udalostí súvisiacich s útočnými cestami, aby sa zabránilo ich zneužitiu útočníkmi. 8. Riešenie musí umožňovať kontrolu jednotlivých detegovaných udalostí v prostredí, ktoré by mohli spustiť upozornenie, a to prostredníctvom podrobných preddefinovaných alebo vlastných detekčných filtrov, ktoré tvoria modely detekcie spúšťajúce upozornenia. 9. Riešenie musí využívať globálne údaje o aktivitách, informácie o CVE a údaje o lokálnej detekčnej aktivite na analýzu prostredia a na vytvorenie prispôsobených hodnotení zraniteľnosti pre každé aktívum. 10. Riešenie musí poskytovať funkcionalitu Attack Surface Discovery, ktorá umožňuje objavovať organizačné aktíva, ktoré by mohli byť vystavené útoku, vrátane zariadení, aktív vystavených internetu, účtov, aplikácií a cloudových aktív. 11. Riešenie musí byť súčasťou komplexnej platformy kybernetickej bezpečnosti, ktorá centralizuje správu vystavenia sa kybernetickým rizikám, bezpečnostné operácie a robustnú vrstvenú ochranu, čo pomáha predvídať a predchádzať hrozbám a urýchľuje proaktívne bezpečnostné výsledky. 12. Riešenie musí určovať úroveň rizika udalosti na základe dvoch faktorov: pravdepodobnosti úspešného útoku a potenciálnej škody, ktorú by udalosť mohla spôsobiť.	

13. Riešenie musí poskytovať detailné informácie o komponentách útočných ciest vrátane vstupných bodov, cieľov, zraniteľností, nesprávnych konfigurácií a vzťahov medzi aktívami. 14. Riešenie musí podporovať integráciu s existujúcimi bezpečnostnými nástrojmi a systémami, aby poskytovalo komplexnejšiu analýzu útočných ciest a lepšie rozpoznávanie rizík.	
O. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Dashboardy a reporty 1. Musí poskytovať prehľad o bezpečnostnom stave organizácie pomocou dashboardu na úrovni výkonného manažmentu. Musí byť schopné zobraziť celkové skóre rizika spoločnosti, riziká jednotlivých aktív, pohľad na prebiehajúce útoky a ich prispievajúce rizikové faktory. 2. Musí poskytovať možnosť hodnotenia a zmierňovania zraniteľností súvisiacich s používateľmi, zariadeniami a aktívami zariadení na operačnom dashboarde. 3. Hlavný dashboard riešenia by mal byť prispôsobiteľný a podporovať widgety. Widgety špecifické pre objavovanie útočnej plochy by mali byť k dispozícii minimálne pre: 3.1. Aktíva prístupné z internetu 3.2. Aktíva účtov 3.3. Aktíva aplikácií 3.4. Cloudové aktíva 3.5. API 3.6. Reporty musia byť generovateľné na vyžiadanie alebo podľa plánu. 3.7. Generované reporty musia byť možné posielať e-mailom. 3.8. Obsah reportov musí byť možné filtrovať na zúženie výstupu na základe vybraných kritérií.	
P. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry - Bezpečnosť súborov 1. Riešenie musí poskytovať modulárnu bezpečnostnú službu (skenovacie jadro - engine) na detekciu hrozieb v súboroch, primárne určenú pre on-premise infraštruktúru, s možnosťou rozšírenia na cloudové úložiská. 2. Riešenie musí zabrániť prieniku a šíreniu škodlivých súborov v rámci firemnej siete, bez ohľadu na ich pôvod alebo cieľové úložisko. 3. Riešenie musí byť integrovateľné do akéhokoľvek procesu alebo aplikácie, kde súbory vstupujú do infraštruktúry. Medzi kľúčové prípady použitia patria: 3.1. Súbory nahrávané cez webové stránky a portály. 3.2. Dokumenty vkladané do Document Management Systémov (DMS). 3.3. Prílohy spracovávané e-mailovými systémami alebo bránami. 3.4. Súbory prenášané cez FTP servery alebo MFT (Managed File Transfer) platformy. 3.5. Artefakty a závislosti v rámci CI/CD pipeline ukladané na lokálne úložiská. 4. Integrácia musí byť možná prostredníctvom poskytnutého SDK (Software Development Kit) alebo cez štandardizované API (napr. REST API), čo umožní vývojárom priamo začleniť funkciu skenovania do vlastných aplikácií.	

5. Riešenie musí podporovať flexibilné spôsoby spúšťania skenovania, vrátane: 5.1. Priamym volaním cez API/SDK z aplikácie, ktorá prijala súbor. 5.2. Monitorovaním určených priečinkov na sieťových diskoch alebo NAS úložiskách (tzv. "watch-folder" funkcionalita). 5.3. Integráciou s natívnymi udalosťami cloudových úložísk, ak sa používajú. 6. Riešenie musí využívať pokročilé metódy detekcie a najnovšie spravodajstvo o hrozbách (threat intelligence) na identifikáciu malvéru, exploitov a iných typov hrozieb. 7. Riešenie musí poskytovať synchrónnu odpoveď (okamžitý výsledok skenovania) pre interaktívne aplikácie, kde je potrebné ihneď rozhodnúť o prijatí alebo zamietnutí súboru. 8. Riešenie musí po dokončení skenovania jednoznačne označiť stav súboru. Spôsob označenia musí byť flexibilný a prispôsobiteľný danému systému (napr. vrátenie stavu cez API, presun súboru, zápis do databázy). 9. Na základe výsledku skenovania musí byť možné automaticky spúšťať nápravné akcie, ako je presun do karanténneho priečinku, zmazanie súboru alebo zaslanie notifikácie administrátorovi. 10. Architektúra riešenia musí byť škálovateľná a flexibilná, aby zvládla spracovať veľké objemy súborov bez významného dopadu na výkon produkčných aplikácií. 11. Riešenie musí ponúkať flexibilné možnosti nasadenia skenovacieho jadra, vrátane nasadenia ako Docker kontajner, virtuálné zariadenie (appliance) alebo ako softvérový balík pre podporované operačné systémy. 12. Všetky výsledky a udalosti zo skenovania, bez ohľadu na ich pôvod (on-premise alebo cloud), musia byť reportované do centrálnej manažment konzoly pre jednotný prehľad, audit a správu. 13. Riešenie musí byť schopné skenovať súbory s veľkosťou minimálne do 2 GB, s možnosťou konfigurácie limitov. 14. Licenčný model musí byť flexibilný a umožňovať licencovanie na základe objemu skenovaných dát alebo počtu skenovacích jadier, prispôsobený pre hybridné nasadenie.	
<u>Q. Požiadavky na oblasť zabezpečenia ochrany kritických prvkov infraštruktúry – Sanboxing</u> 1. Riešenie musí poskytovať schopnosť hĺbkovej analýzy podozrivých súborov a URL adries v izolovanom a bezpečnom virtuálnom prostredí (sandbox). 2. Riešenie musí byť schopné spustiť (detonovať) analyzovaný objekt a monitorovať jeho správanie v reálnom čase s cieľom odhaliť škodlivé aktivity, ktoré by pri statickej analýze neboli zjavné. 3. Analýza musí kombinovať výsledky z dynamickej analýzy (sandboxing) s výsledkami iných metód (napr. statická analýza), aby poskytla komplexný a konsolidovaný pohľad na hrozbu. 4. Riešenie musí podporovať manuálne nahrávanie objektov (súborov, URL) na analýzu priamo analytikmi cez manažment konzolu. 5. Riešenie musí podporovať automatické odosielanie podozrivých objektov z iných integrovaných	

bezpečnostných modulov (napr. z ochrany koncových bodov, e-mailu alebo sieťovej ochrany). 6. Riešenie musí podporovať analýzu širokej škály typov súborov, vrátane, ale nie výlučne: spustiteľných súborov (Windows PE), dokumentov Microsoft Office (vrátane makier), PDF súborov, skriptov, komprimovaných archívov a ďalších bežne zneužívaných formátov. 7. Riešenie musí poskytovať možnosť vybrať si pre analýzu špecifické virtuálne prostredie (sandbox image), ktoré najlepšie zodpovedá produkčným systémom organizácie (napr. konkrétna verzia Windows s nainštalovaným softvérom). 8. Počas detonácie musí riešenie monitorovať a zaznamenávať široké spektrum aktivít, vrátane: sieťovej komunikácie (C&C servery), zmien v súborovom systéme, modifikácií registrov, vytvárania nových procesov a volaní systémových funkcií. 9. Riešenie musí po dokončení analýzy vygenerovať podrobný report, ktorý je zrozumiteľný pre bezpečnostných analytikov. 10. Report musí obsahovať minimálne nasledujúce informácie: 10.1. Celkové skóre rizika a konečný verdikt (škodlivý, podozrivý, bezpečný). 10.2. Zoznam pozorovaných Indikátorov Kompromitácie (IOCs), ako sú IP adresy, domény, hashe súborov. 10.3. Mapovanie pozorovaného správania na techniky a taktiky v rámci rámca MITRE ATT&CK®. 10.4. Grafickú vizualizáciu reťazca udalostí (process tree), ktorá zobrazuje, ako sa procesy vytvárali a ovplyvňovali. 10.5. Snímky obrazovky (screenshots) z virtuálneho prostredia zachytávajúce kľúčové momenty aktivity (napr. zobrazené okná, falošné chybové hlášky). 10.6. Detailný záznam sieťovej aktivity a vytvorených/modifikovaných súborov. 11. Výsledky analýzy musia byť dostupné cez centrálnu manažment konzolu a tiež prostredníctvom API pre integráciu s inými systémami (napr. SOAR, SIEM). 12. Administrátori musia mať možnosť konfigurovať nastavenia pre automatické odosielanie objektov, vrátane definovania prahových hodnôt rizika alebo špecifických spúšťačov (triggers) z iných častí platformy. 13. Riešenie musí umožňovať správu a prispôsobenie dostupných sandboxových obrazov, aby čo najvernejšie simulovali reálne prostredie. 14. Riešenie musí uchovávať históriu analyzovaných objektov a ich výsledkov pre účely spätného vyhľadávania a korelácie.	
R. Požiadavky pre oblasť - Bezpečnosť identít 1. Riešenie musí poskytovať centrálny a jednotný inventár všetkých identít v organizácii, ktorý sa integruje s kľúčovými zdrojmi identít. 2. Riešenie musí podporovať integráciu s hlavnými cloudovými a on-premise adresárovými službami (napr.	

Microsoft Entra ID, Active Directory) na automatické získavanie a synchronizáciu dát o identitách. 3. Riešenie musí v inventári jednoznačne rozlišovať medzi ľudskými identitami (používateľské účty) a ne-ľudskými identitami (napr. servisné účty, spravované identity). 4. Riešenie musí nepretržite vyhodnocovať a prideľovať skóre rizika pre každú identitu na základe viacerých faktorov, vrátane, ale nie výlučne: stavu účtu, aktivity prihlásenia, úrovne oprávnení a konfigurácie zabezpečenia. 5. Riešenie musí poskytovať podrobný prehľad o každej ľudskej identite, vrátane informácií o stave účtu (aktívny/neaktívny), stave viacfaktorovej autentifikácie (MFA), dátume posledného prihlásenia a priradených oprávneniach. 6. Riešenie musí poskytovať prehľadnú vizualizáciu oprávnení (entitlements) a rolí priradených každej identite, aby bolo možné ľahko identifikovať nadmerne privilegované účty. 7. Riešenie musí proaktívne identifikovať a upozorňovať na bezpečnostné riziká a expozície spojené s identitami, ako sú neaktívne (stale) účty, účty bez povinnej MFA alebo účty s vysoko rizikovými oprávneniami. 8. Riešenie musí monitorovať prihlasovacie aktivity a správanie identít v reálnom čase s cieľom detegovať anomálie a podozrivé aktivity. 9. Riešenie musí byť schopné detegovať špecifické útoky cielené na identity, ako sú podozrivé prihlásenia z neobvyklých lokalít, scenáre nemožného cestovania (impossible travel) alebo prihlásenia z anonymizujúcich služieb. 10. Dáta o riziku identity, jej expozícii a detegovaných hrozbách musia byť integrované s ostatnými bezpečnostnými signálmi (z koncových bodov, cloudu, e-mailu) v rámci jednotnej platformy na účely korelácie a kontextového vyšetrovania (XDR). 11. Stav a riziko identity musia slúžiť ako kľúčový signál pre vynucovanie dynamických a kontextovo-závislých politík prístupu v súlade s princípmi Zero Trust. 12. Všetky informácie o identitách, ich rizikách a súvisiacich bezpečnostných udalostiach musia byť prehľadne zobrazené v centrálnej manažment konzole. 13. Riešenie musí podporovať automatizované reakčné akcie na identity-based hrozby, ako je napríklad vynútenie odhlásenia, vyžadovanie opätovnej MFA autentifikácie alebo dočasné zablokovanie účtu.	

Bezpečnostný nástroj 4
(Nástroj pre bezpečnostný monitoring)

Požiadavka	Návrh na plnenie / Dôkaz (doplní uchádzač)
Bezpečnostný nástroj 4 musí spĺňať nasledovné certifikačné požiadavky alebo ekvivalent: • SOC2 Type II • EU General Data Protection Regulation (GDPR) • ISO 27001	
Verejný obstarávateľ požaduje, aby sa centrálny zber logov vykonával v rámci verejného komerčného cloudového prostredia uchádzačom ponúkaného riešenia, pričom je požadovaná minimálna retencia logov na úrovni 13 mesiacov. Riešenie nesmie licenčne a funkčne obmedzovať zber a spracovávanie logov v prípade neštandardnej sieťovej prevádzky s vysokým objemom dát. Bezpečnostný nástroj má byť implementovaný do IT prostredia Verejného obstarávateľa skladajúceho sa z 1x hlavnej lokality a minimálne 65 vzdialených lokalít (informácia pre uchádzačov: počet vzdialených lokalít sa môže meniť v závislosti od organizačných zmien).	

Minimálne funkčné požiadavky:

- SIEM (Security Information & Event management)
- UBA (User Behavior Analytics)
- ABA (Attacker Behavior Analytics)
- Ďalšie požiadavky na detekciu
- EDR (Endpoint Detection & Response)
- FIM (File Integrity Monitoring)
- FAAM (File Access Activity Monitoring)
- NTA (Network Traffic Analysis)
- DT (Deception Technology)

Požiadavka	Návrh na plnenie / Dôkaz (doplní uchádzač)
SIEM (Security Information & Event management) Základné vlastnosti systému: 1. centrálne úložisko logov a centrálna konzola systému musí byť mimo IT infraštruktúru Verejného obstarávateľa z dôvodu zabezpečenia integrity a dostupnosti v prípade ransomvérového útoku a / alebo výpadku IT infraštruktúry, 2. centrálne úložisko a centrálna konzola musí využívať niektorú zo služieb verejného komerčného	

cloudového prostredia, 3. centrálne úložisko a centrálna konzola musí zabezpečovať geografické rozloženie dát pre úložisko logov a manažment systému, pričom uložené logy nesmú opustiť geografický región EÚ, 4. prístup do centrálnej konzoly musí byť zabezpečeným spôsobom prostredníctvom webového prehliadača (podpora minimálne Chrome, Firefox), 5. musí podporovať pokročilé korelácie z viacerých typov zdrojov (časové, používateľ, zariadenie, služba), 6. musí podporovať detekciu sieťových incidentov na základe korelácie informácií z poskytnutých logov a musí podporovať behaviorálnu analýzu spracovaných udalostí, 7. musí podporovať možnosť integrácie s Vulnerability Management systémom pre kontextualizáciu aká zraniteľnosť na konkrétnom koncovom bode existuje.	
Správa systému a autentifikácia: 1. musí podporovať minimálne nasledujúce úrovne užívateľských oprávnení (administrátor, analytik, užívateľ iba na prezeranie údajov), 2. riadenie prístupov (administrátorov, analytikov, užívateľov iba na prezeranie údajov) musí byť podporované prostredníctvom RBAC (Role-Based Access Control) - členstva účtu v skupine a priradenej roly oprávnení, 3. priraďovanie roly oprávnení musí obsahovať funkcionalitu detekcie konfliktu priradených rolí (v súlade s požiadavkou na vykonanie týchto zmien internými kapacitami Verejného obstarávateľa), 4. musí podporovať integráciu Single Sign-On (SSO) SAML 2.0 pre externých poskytovateľov identít ako sú Active Directory Federation Services, MS Azure, Cisco Duo, Okta, 5. musí umožňovať konfiguráciu politiky pre silu hesla a doby exspirácie hesla, 6. musí podporovať vlastnú alebo externú integráciu s navrhovaným riešením pre Multi-faktorovú autentifikáciu (MFA), 7. musí podporovať Multifaktorovú autentifikáciu (MFA) pomocou meniaceho sa číselného kódu (napr. Google Authenticator), bezpečnostných kľúčov WebAuthn a prostredníctvom krátkej textovej správy SMS zasielanej na telefónne číslo mobilného telefónu.	
Zber logov: 1. musí podporovať možnosť inštalácie kolektorov – bodov, v ktorých sa zbierajú logy / udalosti / údaje na pred-spracovanie dát ako sú normalizácia, komprimácia ešte pred zaslaním do centrálnej konzoly (pre zníženie šírky potrebného dátového toku a zjednodušenie počtu firewallových pravidiel), 2. kolektor po prvotnej inštalácii musí byť automaticky aktualizovaný bez potreby dodatočných administrátorských zásahov, 3. musí umožňovať zber aplikačných, databázových aj systémových logov zo sieťových aj bezpečnostných zariadení (napr. firewally, sieťové alebo host. IPS/IDS), pracovných staníc, serverov,	

ako aj cloudových prostredí (Microsoft Azure, Microsoft 365, AWS, Google Cloud,...) 4. musí zbierať, detegovať a vyhodnocovať udalosti ako sú pokusy o neautorizované prístupy, zmeny integrity vybraných častí operačného systému, útoky škodlivého kódu, protocol poisoning, botov, neoprávnený prístup k aplikáciám, neautorizovanú zmenu konfigurácií, porušení bezp. politík siete, 5. musí umožňovať uchovávanie pôvodnej informácie zo zdroja logu o časovej značke udalosti, 6. zber systémových a bezpečnostných logov z koncových staníc musí byť podporovaný prostredníctvom agentskej aplikácie, 7. zber systémových a bezpečnostných logov zo serverov musí byť podporovaný prostredníctvom agentskej aplikácie, 8. zber aplikačných logov a logov prevádzkovaných služieb serverov musí byť podporovaný prostredníctvom agentskej aplikácie a zároveň podporovaný aj bez-agentsky (bez potreby inštalácie agentskej aplikácie), 9. zber aplikačných logov a logov prevádzkovaných služieb zo serverov musí podporovať metódu zberu PUSH t.j. logy sú zasielané do komponentov riešenia SIEM, 10. zber aplikačných logov a logov prevádzkovaných služieb zo serverov musí podporovať metódu zberu PULL t.j. logy sú vyčítavané niektorým z komponentov riešenia SIEM zo serverov (v prípade nemožnosti inštalácie agentskej aplikácie), 11. systém musí podporovať e-mailovú notifikáciu výpadku zberu logov zo serverov a sieťových prvkov, 12. musí podporovať zber dát s prenosom protokolmi TCP a UDP, 13. musí podporovať zber dát so šifrovaným prenosom (TCP/TLS ver. 1.2, alebo ver. 1.3, prípadne šifrovaný obsah správ) na celej trase (zdroj logov / kolektor / centrálna konzola), 14. musí podporovať outbound API (príkladom môže byť pripojenie sa na externé zariadenia, alebo systémy napr. Azure, AWS, Microsoft 365, ticketing system), 15. podporuje integráciu na cloudové služby Microsoft Azure a Microsoft 365 pre účely monitoringu aktivít používateľov, 16. musí podporovať zber logov minimálne zo systémov poskytujúcich logy Active Directory, DHCP, DNS, Firewall, VPN, Web Proxy, logy antimalvérových riešení, logy sieťových IDS/IPS, MS SQL, MS IIS, 17. musí poskytovať zber logov Syslog s automatickým štruktúrovaním údajov, 18. musí poskytovať zber logov Syslog zo sieťových zariadení (firewall, switch, router) s automatickým štruktúrovaním údajov podľa RFC 3164, 19. musí poskytovať zber logov z textových súborov a adresárov, 20. musí poskytovať zber logov z textových súborov a adresárov zo zdieľaných sieťových úložísk, 21. musí podporovať spracovanie štruktúrovaných aj neštruktúrovaných dát, 22. musí podporovať úpravy parsovania logov bez nevyhnutnosti učiť sa akýkoľvek programovací / skriptovací jazyk pomocou grafického rozhrania GUI bez nutnosti práce v príkazovom riadku CLI	

(Command Line Interface) (v súlade s požiadavkou na vykonanie týchto zmien internými kapacitami Verejného obstarávateľa), 23. musí podporovať identifikáciu používateľských účtov prostredníctvom vyčítavania Active Directory / LDAP, 24. musí podporovať identifikáciu používateľských účtov zo zbieraných logov (identifikácia používateľov, ktorí nie sú v Active Directory), 25. musí umožňovať nastavenie privilegovaných skupín monitorovaných používateľov (administrátorov) Active Directory, pričom podľa týchto monitorovaných skupín majú byť generované kybernetické bezpečnostné hlásenia a incidenty, 26. musí umožňovať zobrazenie zoznamu identifikovaných účtov s informáciami ako je členstvo v privilegovanej skupine, nastavenie účtu bez exspirácie hesla alebo že je účet v Active Directory zapnutý alebo vypnutý, 27. musí umožňovať realizáciu tzv. kaskádových dotazov (kaskádové dotazy sú dotazy generované na základe údajov vrátených z predchádzajúceho dotazu, príkladom by mohlo byť zobrazenie aktív, na ktoré sa vzťahuje alert, s následnou možnosťou rozbalenia na používateľov, ktorých sa táto stránka s výsledkami vyhľadávania týka), 28. musí umožňovať sledovanie aktuálneho stavu konektivity agentskej aplikácie, ako sú stavy pripojený, nepripojený, dlhodobo nepripojený, 29. musí umožňovať automatické odstránenie agentskej aplikácie zo zoznamu s možnosťou definovania max. doby, po ktorej má byť agentská aplikácia zo zoznamu automaticky odstránená (napr. ukončenie životného cyklu zariadenia alebo dlhodobé vypnutie). V prípade zapnutia zariadenia po dlhej dobe, musí byť zariadenie automaticky zaradené do zoznamu a monitorované na bezpečnostné kybernetické hrozby, 30. musí umožňovať sledovanie diagnostiky chyby agentskej aplikácie, 31. musí umožňovať integráciu so systémom na ochranu kritických prvkov infraštruktúry, pričom musí umožňovať zber údajov, vyhodnocovať ich a generovať kybernetické bezpečnostné udalosti a incidenty.	
Zber logov v prostredí MS Windows a MS Windows Server - Agent musí podporovať zber udalostí v prostredí MS Windows a MS Windows Server: 1. udalosti z MS Windows a MS Windows Server prostredí musia byť získavané pomocou agenta inštalovaného priamo na koncovom systéme s operačným systémom MS Windows, alebo MS Windows Server, 2. agent určený pre MS Windows a MS Windows Server prostredia musí súčasne podporovať monitoring interných Windows logov, ako aj monitoring textových súborových logov, 3. MS Windows a MS Windows Server agent musí umožňovať hromadnú inštaláciu prostredníctvom	

Active Directory GPO (Group Policy Object), 4. zber udalostí v prostredí MS Windows a MS Windows Server musí byť minimálne v nasledovnom rozsahu ID udalostí: 1102, 4624, 4625, 4648, 4704, 4720, 4722, 4724, 4725, 4728, 4732, 4738, 4740, 4741, 4756, 4767, 4768, 4769, 5. MS Windows a MS Windows Server agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovávanie informácií má prebiehať až v centrálnej konzole z dôvodu zabezpečenia nízkeho vyťaženia systémových zdrojov na zariadení na ktorom má byť nainštalovaný, 6. MS Windows a MS Windows Server agent musí zabezpečiť funkcionalitu kontroly integrity súborov, 7. MS Windows a MS Windows Server agent musí zabezpečiť v prípade potreby funkcionalitu auditovania prístupov k súborom zdieľaných sieťových úložísk, 8. MS Windows a MS Windows Server agent musí filtrovať odosielané udalostí - nerelevantné logy majú byť odfiltrované už na strane MS Windows a MS Windows Server agenta a nie sú odosielané po sieti na ďalšie spracovanie, 9. MS Windows a MS Windows Server agent po prvotnej inštalácii nesmie vyžadovať dodatočné administrátorské zásahy na koncovom systéme na ktorom má byť nainštalovaný a musí byť automaticky aktualizovaný, 10. centrálna konzola musí umožňovať hromadné riadenie požadovanej inštalovanej verzie MS Windows a MS Windows Server agenta, 11. MS Windows a MS Windows Server agent musí mať buffer (schopnosť dočasne uschovať logy) pre prípad straty spojenia medzi koncovým systémom, na ktorom je nainštalovaný, a centrálnym úložiskom logov po dobu, pokiaľ sa obnoví sieťové spojenie medzi koncovým systémom a centrálnym úložiskom, 12. MS Windows a MS Windows Server agent musí umožniť natívnu analýzu logov Microsoft Windows Defender Antivirus zo zariadenia, na ktorom je nainštalovaný, bez potreby inštalácie dodatočného softvéru.	
Zber logov v prostredí Linux - Agent musí podporovať zber udalostí v prostredí Linux: 1. udalosti z Linux prostredí musia byť získavané pomocou agenta inštalovaného priamo na koncovom systéme s operačným systémom OS Linux, 2. agent určený pre Linux prostredie musí podporovať monitoring interných Linux logov, 3. Linux agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovávanie informácií má prebiehať až v centrálnej konzole z dôvodu zabezpečenia nízkeho vyťaženia systémových zdrojov na zariadení, na ktorom má byť nainštalovaný, 4. Linux agent musí zabezpečiť v prípade potreby funkcionalitu kontroly integrity súborov, 5. Linux agent musí filtrovať odosielané udalostí - nerelevantné logy majú byť odfiltrované už na strane Linux agenta a nie sú odosielané po sieti na ďalšie spracovanie,	

6. Linux agent po prvotnej inštalácii nesmie vyžadovať dodatočné administrátorské zásahy na koncovom systéme, na ktorom má byť nainštalovaný a musí byť automaticky aktualizovaný, 7. centrálna konzola musí umožňovať hromadné riadenie požadovanej inštalovanej verzie Linux agenta, 8. Linux agent musí mať buffer (schopnosť dočasne uschovať logy) pre prípad straty spojenia medzi koncovým systémom, na ktorom je nainštalovaný, a centrálnym úložiskom logov po dobu, pokiaľ sa obnoví sieťové spojenie medzi koncovým systémom a centrálnym úložiskom.	
Zber logov v prostredí MacOS - Agent musí podporovať zber udalostí v prostredí MacOS: 1. udalosti z MacOS prostredí musia byť získavané pomocou agenta inštalovaného priamo na koncovom systéme s operačným systémom MacOS, 2. agent určený pre MacOS prostredia musí podporovať monitoring interných MacOS logov, 3. MacOS agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovávanie informácií má prebiehať až v centrálnej konzole z dôvodu zabezpečenia nízkeho vyťaženia systémových zdrojov na zariadení na ktorom má byť nainštalovaný, 4. MacOS agent má zabezpečiť v prípade potreby funkcionalitu kontroly integrity súborov, 5. MacOS agent musí filtrovať odosielané udalostí - nerelevantné logy majú byť odfiltrované už na strane MacOS agenta a nie sú odosielané po sieti na ďalšie spracovanie, 6. MacOS agent po prvotnej inštalácii nesmie vyžadovať dodatočné administrátorské zásahy na koncovom systéme, na ktorom má byť nainštalovaný a musí byť automaticky aktualizovaný, 7. centrálna konzola musí umožňovať hromadné riadenie požadovanej inštalovanej verzie MacOS agenta, 8. MacOS agent musí mať buffer (schopnosť dočasne uschovať logy) pre prípad straty spojenia medzi koncovým systémom, na ktorom je nainštalovaný, a centrálnym úložiskom logov po dobu, pokiaľ sa obnoví sieťové spojenie medzi koncovým systémom a centrálnym úložiskom.	
Log manažment: 1. súčasťou systému musí byť centrálna konzola pre vyhľadávanie v logoch, 2. musí podporovať jednoduché vyhľadávanie udalostí a možnosť okamžitého vytvorenia reportov bez nutnosti dodatočného programovania, 3. musí podporovať vyhľadávanie v logoch bez nevyhnutnosti učiť sa akýkoľvek programovací / skriptovací jazyk, 4. vyhľadávanie v logoch musí podporovať kaskádové reťazenie podmienok vyhľadávania, 5. vyhľadávanie v logoch musí podporovať zoskupovanie výsledkov podľa vybraného parametra, 6. vyhľadávanie v logoch musí podporovať limitovanie maximálneho počtu vrátených výsledkov, 7. vyhľadávanie v logoch musí podporovať zoraďovanie výsledkov v vzostupnom a zostupnom poradí.	
Incident Management konzola: 1. súčasťou systému musí byť centrálna konzola Incident Management-u pre spravovanie	

kybernetických bezpečnostných udalostí a incidentov generovaných formou ticketu, 2. Incident Management konzola musí podporovať správu kybernetických bezpečnostných udalostí a incidentov, pričom v rámci konzoly musí byť k dispozícií uvedený časový sled danej kybernetickej bezpečnostnej udalosti a incidentu, možnosť prideľovať riešiteľov, možnosť vyvolať akcie (pre zisťovanie ďalších informácií, dopĺňanie logov, vrátane podrobných informácií z koncového bodu, možnosť dopĺňania poznámok, vkladania príloh (podpora viacerých súborov do veľkosti 50 MB na jeden súbor) pričom umožní pripojiť do jednej kybernetickej bezpečnostnej udalosti viaceré súbory do celkovej kapacity 2 GB na jeden ticket, 3. musí poskytovať možnosť priradenia ticketu (kybernetickej bezpečnostnej udalosti a incidentu) zodpovednej osobe, ktorá bude o priradení ticketu notifikovaná napr. emailovou správou, 4. riešenie musí byť bez požiadaviek na externý databázový server, 5. riešenie musí byť bez požiadaviek na externý webový server, 6. všetky úkony zodpovednej osoby za vyšetrovanie kybernetickej bezpečnostnej udalosti, alebo incidentu musia byť logované a auditovateľné, 7. musí umožniť zmenu úrovne závažnosti (nízka, stredná, vysoká, kritická) už vytvorenej kybernetickej bezpečnostnej udalostí a incidentu, 8. musí umožniť vyhodnotenie kybernetickej bezpečnostnej udalostí a incidentu pri uzatváraní na stavy ako sú: Malicious, False Positive, Test, Unknown a pod., 9. musí umožniť zmenu už vytvorenej a/alebo priradenej kybernetickej bezpečnostnej udalosti a incidentu priradením ticketu na inú zodpovednú osobu.	
Reporting: 1. musí podporovať pokročilý reporting s možnosťou schedulingu (plánovania) a distribúcie reportu prostredníctvom e-mailovej správy, 2. musí podporovať možnosť tvorby vlastných grafických prezentácii vyhľadávaných informácii formou Dashboardov a Vizuálnych Analýz, 3. musí podporovať možnosť editácie reportov bez nevyhnutnosti učiť sa akýkoľvek programovací / skriptovací jazyk pomocou grafického rozhrania GUI (v súlade s požiadavkou na vykonanie týchto zmien internými silami obstarávateľa).	
<u>UBA (User Behavior Analytics)</u> 1. riešenie musí v sebe obsahovať už preddefinované (vstavané) detekčné pravidlá pre identifikáciu správania sa používateľa, 2. rozširovanie počtu pravidiel a ich aktualizácia musí byť kontinuálne spravovaná výrobcom bez nutnosti manuálneho zásahu a potreby dodatočných finančných nákladov, 3. musí podporovať minimálne nasledujúce korelačné pravidlá pre analýzu správania sa používateľa: Vytvorenie/Zablokovanie/ Resetovanie / Povolenie / Zamknutie / Odomknutie,	

4. musí podporovať minimálne nasledujúce korelačné pravidlá pre analýzu správania sa používateľa: 4.1. Eskalácia privilégií 4.2. Prístup na podozrivý web odkaz 4.3. Doručenie podozrivého odkazu do e-mailovej schránky 4.4. Útok hrubou silou (Brute Force) na heslá – lokálny účet 4.5. Útok hrubou silou (Brute Force) na heslá – doménový účet 4.6. Útok hrubou silou (Brute Force) na zariadenie – lokálne účty 4.7. Autentifikácia účtu používateľa z komerčných služieb VPN 4.8. Autentifikácia účtu administrátora z verejnej IP adresy 4.9. Manipulácia s lokálnymi udalosťami - logmi 4.10. Prvé prihlásenie na zariadenie 4.11. Prvé prihlásenie z inej krajiny 4.12. Prvá aktivita administrátora 4.13. Prihlásenie sa z viacerých krajín súčasne 4.14. Prvé prihlásenie sa z mobilného zariadenia 4.15. Detegovaný hash z podozrivej databázy 4.16. Spustenie procesu z podozrivej databázy 4.17. Impersonizácia administrátora 4.18. Autentifikácia servisným účtom 4.19. Pokus o autentifikáciu deaktivovaným doménovým účtom 4.20. Komunikácia s podozrivou IP adresou 4.21. Komunikácia s podozrivou doménou 4.22. Prvé použitie cloudovej služby 4.23. Prvé použitie cloudovej služby v inom geo regióne 4.24. Spustenie vzdialeného súboru 4.25. Protokol poisoning 4.26. Spearphishing URL detegovaná 5. musí podporovať možnosť vytvárania vlastných detekčných pravidiel s možnosťou výberu závažnosti (nízka, stredná, vysoká, kritická) v prípade detekcie, 6. musí podporovať úpravu špecifických korelačných pravidiel (vytvorenie kybernetickej bezpečnostnej udalosti a incidentu, alebo iba zalogovanie udalosti, 7. musí umožniť deaktiváciu detekčného pravidla, 8. musí vytvárať rizikový profil používateľa na základe jeho správania, 9. musí vytvárať rizikový profil privilegovaného užívateľa na základe jeho správania, 10. musí podporovať možnosť manuálneho označenia servisného účtu a označenia používateľa za rizikového,	

11. musí podporovať podrobný monitoring definovaných užívateľov, 12. podporuje podrobný monitoring aktivít privilegovaného používateľa v lokálnom aj cloudovom prostredí.	
ABA (Attacker Behavior Analytics) 1. riešenie musí v sebe obsahovať už preddefinované (vstavané) detekčné pravidlá pre identifikáciu správania sa útočníka, 2. musí podporovať korelačné pravidlá pre analýzu správania sa útočníka, napr. zistenie externej IP pomocou príkazového riadka; spustenie kľúča z registra Windows; spúšťanie procesov pomocou konzoly MMC; Rundl32.exe spúšťa súbor z adresára Program Data, alebo Users; premenovanie netcat; windows debug v príkazovom riadku; používanie nástrojov Anydesk, VNC, 7-zip, WinRar, a ďalšie; zneužitie legitímnych nástrojov CMD, PowerShell a pod. aj bez použitia Malvéru tzv. útok „Living off the land (LOTL)“; používanie nástroja certutil.exe; memory dump; stiahnutie súborov pomocou príkazov wget, alebo curl a pod. 3. musí umožniť mapovať správanie sa útočníka podľa taktík z metodiky MITRE ATT&CK framework: Reconnaissance; Resource Development ; Initial Access; Execution; Persistence; Privilege Escalation; Defense Evasion; Credential Access; Discovery; Lateral Movement; Collection; Command And Control; Exfiltration; Impact, 4. musí podporovať identifikáciu hrozieb vo vzťahu ku škodlivým dokumentom, 5. musí podporovať identifikáciu hrozieb vo vzťahu ku APT (Advanced Persistent Threat) skupinám na úrovni spúšťaných procesov, DNS request-ov a Web request-ov, 6. musí podporovať úpravu korelačných pravidiel prostredníctvom definovania výnimiek, 7. musí umožniť zobrazenie kontextu prečo bola daná detekcia vykonaná a odporúčanie na investigatívu, alebo mitigáciu hrozby, 8. databáza korelačných pravidiel správania sa útočníka je kontinuálne aktualizovaná o nové techniky používane útočníkmi, rozširovanie počtu pravidiel a ich aktualizácia musí byť kontinuálne spravovaná výrobcom bez nutnosti manuálneho zásahu a potreby dodatočných finančných nákladov, minimálny počet detekčných pravidiel musí byť 2000 ks s postupným rozširovaním výrobcom bez dodatočných nákladov, 9. musí podporovať možnosť vytvárania vlastných detekčných pravidiel s možnosťou výberu závažnosti (nízka, stredná, vysoká, kritická) v prípade detekcie, 10. musí podporovať úpravu špecifických korelačných pravidiel (kybernetickej bezpečnostnej udalosti a incidentu, alebo iba zalogovanie udalosti), 11. musí umožniť deaktiváciu detekčného pravidla.	
Ďalšie požiadavky pre detekciu 1. musí umožňovať vytvorenie vlastných detekčných pravidiel pre generovanie kybernetických bezpečnostných udalostí na základe:	

1.1. zhody s vyhľadávaním reťazcom v logoch, 1.2. definovanej nečinnosti v logoch, 1.3. definovanej zmeny v logoch, 2. musí poskytovať možnosť nastavenia sieťových zón prostredníctvom definovania IP adries alebo rozsahov IP adries, 3. musí poskytovať možnosť nastavenia sieťových politík pre detekciu narušenia používateľmi a administrátormi generujú kybernetické bezpečnostné udalosti, 4. musí poskytovať funkcionalitu monitorovania indikátorov kompromitácie (IoC), 5. musí podporovať minimálne nasledovné typy indikátorov kompromitácie (IoC): 5.1. MD5 hash procesu, IP adresa, Doména, URL adresa, 6. musí podporovať vkladanie a monitorovanie vlastných indikátorov kompromitácie (IoC), 7. musí podporovať manipuláciu vlastných indikátorov kompromitácie (IoC) prostredníctvom API rozhrania, 8. musí podporovať import vlastných indikátorov kompromitácie (IoC) z textových súborov (TXT, CSV a pod.), 9. musí podporovať možnosť použiť pre detekciu zoznamy indikátorov kompromitácie (IoC) poskytovaných výrobcom, alebo tretími stranami.	
EDR (Endpoint Detection & Response) 1. musí podporovať základnú funkcionalitu reakcie na bezpečnostnú udalosť a kybernetický bezpečnostný incident (ukončenie bežiaceho procesu, karanténa zariadenia) prostredníctvom Windows/Linux agenta priamo z centrálnej konzole, 2. musí podporovať funkcionalitu vyšetrovania incidentu prostredníctvom zberu dôkazov minimálne v rozsahu: Arp Cache; Current Process; Directory Entry; Dns Cache; Installed Service; Network Connection; Prefetch Entry; Registry Key; Scheduled Task; User Session, 3. musí podporovať funkcionalitu vyšetrovania incidentu prostredníctvom zberu dôkazov preverovaného používateľa o nasledujúce udalosti: Account modified; Advanced malware alert; Asset authentication; Cloud service account modified; DNS query; Firewall; IDS; Ingress authentication; Virus infection; Web proxy, 4. podporuje rozšírenú funkcionalitu odozvy na incident (spustenie automatizačného workflow).	
FIM (File Integrity Monitoring) 1. musí podporovať auditovanie integrity súborov a adresárov na úrovni modifikácie: minimálne vytvorenie, zmazanie, zápis, 2. musí podporovať funkcionalitu modifikácie operačných systémov MS Windows a MS Windows Server minimálne pre nasledujúce prípony súborov: .bat; .cfg; .conf; .config; .dll; .exe; .ini; .sys, 3. musí podporovať auditovanie integrity adresárov operačných systémov Linux minimálne pre nasledujúce adresáre: /bin; /boot; /etc; /sbin; /usr/bin; /usr/local/bin; /usr/local/sbin; /usr/sbin; /usr/share/keyrings; /var/spool/cron.	

FAAM (File Access Activity Monitoring) 1. musí podporovať auditovanie prístupu ku súborom na zdieľanom úložisku Windows minimálne na úrovni: ReadData; WriteData; AppendData; ReadEA; WriteEA; Execute/Traverse; DeleteChild; ReadAttributes; WriteAttributes; DELETE; READ_CONTROL; WRITE_DAC; WRITE_OWNER; SYNCHRONIZE; ACCESS_SYS_SEC, 2. musí podporovať auditovanie prístupu ku súborom na cloudovej službe Microsoft 365.	
ENTA (Enhanced Network Traffic Analysis) 1. musí podporovať identifikáciu a zber nasledujúcich sieťových udalostí: DNS udalosti; DHCP udalosti; IDS udalosti, 2. zariadenie musí byť možné nasadiť do internej či externej časti siete bez licenčného obmedzenia množstva nasadených zariadení a dodatočných finančných nákladov, 3. musí poskytovať špecifické korelačné pravidlá pre SIEM súvisiace s analýzou sieťovej prevádzky, 4. musí poskytovať špecifické vyhľadávacie vzory (queries) pre SIEM súvisiace s analýzou sieťovej prevádzky, 5. zariadenie pre monitoring siete musí byť možné inštalovať voliteľne do fyzického, virtualizačného alebo cloudového prostredia. V prípade viacerých zariadení musí byť zachovaná možnosť voľby ľubovoľného prostredia do ktorého majú byť jednotlivé zariadenia pre monitoring siete nainštalované, 6. zariadenie musí byť technicky schopné analyzovať sieťovú prevádzku v prenosovej rýchlosti až 10 Gb/s, analyzovaná sieťová prevádzka nesmie byť zariadením obmedzovaná, 7. zariadenie po prvotnej inštalácii nesmie vyžadovať dodatočné administrátorské zásahy na koncovom systéme, na ktorom má byť nainštalované, a musí byť automaticky aktualizované, 8. riešenie musí v sebe obsahovať už preddefinované (vstavané) detekčné pravidlá pre identifikáciu hrozieb na analyzovanej sieťovej prevádzky, 9. rozširovanie počtu pravidiel a ich aktualizácia musí byť kontinuálne spravovaná výrobcom bez nutnosti manuálneho zásahu a potreby dodatočných finančných nákladov, 10. minimálny počet detekčných pravidiel 7000 ks s postupným rozširovaním výrobcom bez dodatočných nákladov, 11. musí podporovať analýzu sieťovej prevádzky pre identifikáciu hrozieb vo vzťahu ku APT (Advanced Persistent Threat) skupinám, 12. zariadenie musí podporovať analýzu sieťovej prevádzky fyzických sieťových portov ako sú SPAN Port, alebo Mirror Port a virtuálnych sieťových portov virtualizačnej platformy, 13. zariadenie musí podporovať analýzu sieťovej prevádzky bez požiadavky na špecifikáciu výrobcu komponentov sieťovej infraštruktúry.	
DT (Deception Technology) 1. systém musí podporovať tvorbu nasledujúcich typov návnad za účelom identifikácie a detekcie aktivít útočníka:	

1.1. návnada vo forme zariadenia / aktíva Honeypot so samostatnou internou IP adresou, ktorá prezentuje útočníkovi minimálne porty nasledovných služieb dostupných v sieti LAN: DCE/RPC; DNS; FTP; H.323; HTTP; HTTPS; IMAP; IMAPS; LDAP; LDAPS; MSSQL; MySQL; NetBIOS; NTP; OpenVPN; POP3; POP3S; PostgreSQL; RADIUS; RDP; SIP; SIPS; SMB; SMTP; SMTPS; SSH; TeamViewer; TELNET; TFTP; VNC; 1.2. musí podporovať neobmedzený počet návnad typu Honeypot a to bez licenčného obmedzenia množstva nasadených zariadení a dodatočných finančných nákladov, alebo bez potreby dodatočného rozšírenia licencie, 1.3. návnada vo forme súboru Honeyfile umiestnenom na zdieľanom sieťovom úložisku, 1.4. musí podporovať neobmedzený počet návnad typu Honeyfile bez potreby dodatočného rozšírenia licencie, 1.5. návnada Honeyuser vo forme monitorovaného Active Directory účtu , 1.6. musí podporovať neobmedzený počet návnad typu Honeyuser bez potreby dodatočného rozšírenia licencie, 1.7. návnada vo forme prihlasovacích údajov uložených v operačnej pamäti RAM (Honeycredentials), 1.8. musí podporovať neobmedzený počet návnad typu Honeycredentials bez potreby dodatočného rozšírenia licencie, 2. súčasťou riešenia musia byť návnady (decoy) pre odhalenie útočníka po úspešnej infiltrácii do siete, alebo na zariadenie, 3. návnady musí byť možné nasadiť do internej časti siete bez licenčného obmedzenia množstva nasadených zariadení.	

Skenovanie zraniteľností

V rámci služieb bezpečnostných testovaní verejný obstarávateľ požaduje počas doby trvania projektu vykonanie 4 samostatných testovaní, na základe vyžiadania, s výstupnými správami a osobnou prezentáciou výstupov pre nasledujúce oblasti:

Požiadavka na vykonanie skenu technických zraniteľností interných aktív (systémov a zariadení) v IT infraštruktúre:

1. vykonanie skenu musí byť uskutočnené v internom IT prostredí organizácie, bez skenovania verejných IP adries,
2. skenovacie zariadenie musí byť umiestnené na hardvéri dodávateľa poskytnutom po nevyhnutnú dobu potrebnú pri dodaní služby, ktoré bude pripojené do IT LAN siete organizácie
3. sken zraniteľností nesmie požadovať inštalovanie agentskej aplikácie na skenované aktíva,
4. požaduje sa vykonanie skenu z dvoch pohľadov
   4.1. z vonkajšej strany aktíva (ako útočník, ktorý nemá prihlasovacie údaje),
   4.2. z vnútornej strany aktíva (ako útočník, ktorý kompromitoval účet administrátora),
5. výstupná správa môže byť v slovenskom, alebo českom jazyku,
6. výstupná správa má byť vo formáte PDF,
7. informácie o vykonaných skenoch zraniteľností majú byť dodané v podobe súborov, s ktorými je možné dynamicky pracovať napr. v tabuľkovom procesore MS EXCEL, alebo OpenOffice Calc,
8. hodnotiaci model musí podporovať štandardy CVSSv2, CVSSv3, CVSSv3.1,
9. hodnotiaci model musí podporovať hodnotenie na úrovni rizika aj z pohľadu existencie malvéru, alebo exploitu pre dané zraniteľnosti,

Reportovanie celkových nálezov za celú IT sieť LAN:

1. samostatná výstupná správa má obsahovať celkovú podrobnú auditnú správu v textovej a grafickej podobe za IT sieť LAN vrátane odporúčaní pre odstránenie nálezov,
2. samostatná výstupná správa má obsahovať zoznam odporúčaní pre odstránenie nálezov celkom za celú IT sieť LAN,
3. samostatná výstupná správa má obsahovať zoznam 10 aktív, ktoré predstavujú najväčšie riziko v rámci celej IT siete LAN,
4. samostatná výstupná správa má obsahovať zoznam 25 odporúčaní pre odstránenie nálezov v rámci celej IT siete LAN,
5. samostatnou výstupnou správou má byť súbor s obsahom s ktorým je možné dynamicky pracovať napr. v tabuľkovom procesore MS EXCEL, alebo OpenOffice Calc, pričom tento dokument má obsahovať nálezy za celú IT sieť LAN.

Reportovanie parciálnych nálezov podľa segmentov aktív v rámci IT siete LAN:

1. samostatné výstupné správy majú obsahovať podrobné auditné správy v textovej a grafickej podobe granulované podľa typov aktív (pracovné stanice, notebooky, servery, periférie [tlačiarne, skenery], sieťové prvky IT infraštruktúry, virtualizačná platforma, IoT zariadenia) vrátane odporúčaní pre odstránenie nálezov,
2. samostatné výstupné správy majú obsahovať zoznam odporúčaní pre odstránenie nálezov granulovaných podľa typov aktív (pracovné stanice, notebooky, servery, periférie [tlačiarne, skenery], sieťové prvky IT infraštruktúry, virtualizačná platforma, IoT zariadenia) vrátane odporúčaní,
3. samostatné výstupné správy majú obsahovať zoznam 10 aktív, ktoré predstavujú najväčšie riziko pre danú skupinu aktív, pričom má byť granularita na úrovni typov aktív (pracovné stanice, notebooky, servery, periférie [tlačiarne, skenery], sieťové prvky IT infraštruktúry, virtualizačná platforma, IoT zariadenia),
4. samostatné výstupné správy majú obsahovať zoznam 25 odporúčaní pre odstránenie nálezov, ktoré predstavujú najväčšie riziko pre danú skupinu aktív, pričom má byť granularita na úrovni typov aktív (pracovné stanice, notebooky, servery, periférie [tlačiarne, skenery], sieťové prvky IT infraštruktúry, virtualizačná platforma, IoT zariadenia),
5. samostatné výstupné správy majú obsahovať súbory s obsahom s ktorým je možné dynamicky pracovať napr. v tabuľkovom procesore MS EXCEL, alebo OpenOffice Calc, pričom má byť granularita súborov na úrovni typov aktív (pracovné stanice, notebooky, servery, periférie [tlačiarne, skenery], sieťové prvky IT infraštruktúry, virtualizačná platforma, IoT zariadenia).