1. **Špecifikácia požiadaviek a vlastností centralizovaného nástroja**
   1. Funkčné požiadavky systému pre SIEM:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Požiadavka** | **Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu. |
| SIEM-1 | SIEM 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 cloud prostredí (Microsoft Azure, Microsoft 365,..)  Bližšia špecifikácia v opise |  |
| SIEM-2 | SIEM musí zbierať, detegovať a vyhodnocovať udalosti ako sú pokusy o neautorizované prístupy, zmeny integrity vybraných častí operačného systému, útoky škodlivého kódu, botov, neoprávnený prístup k aplikáciám, neautorizovanú zmenu konfigurácií, detegovať chybové stavy siete, porušení bezp. politík (Zákazníka) |  |
| SIEM-3 | SIEM musí umožňovať monitoring, vyhodnocovanie a korelovanie udalostí a následné generovanie alertov a to všetko v reálnom čase, pričom nesmie technicky limitovať počet spracovávaných a ukladaných udalostí (napríklad pri prekročení licencie alebo výkonu riešenia). |  |
| SIEM-4 | SIEM musí umožňovať uchovávanie pôvodnej informácie zo zdroja logu o časovej značke udalosti |  |
| SIEM-5 | SIEM nesmie umožniť odstránenie alebo modifikovanie uložených logov administrátorovi systému |  |
| SIEM-6 | SIEM musí pre každý log mať unikátny identifikátor, pre jednoznačnú identifikáciu |  |
| SIEM-7 | SIEM podporuje jednoduché vyhľadávanie udalostí a okamžité vytváranie reportov bez nutnosti dodatočného programovania |  |
| SIEM-8 | SIEM musí podporovať pokročilé korelácie (časové, z viacerých zdrojov, atď.) |  |
| SIEM-9 | SIEM musí podporovať integráciu s Vulnerability Assessment pre kontextualizáciu aká zraniteľnosť na konkrétnom koncovom bode existuje. |  |
| SIEM-10 | SIEM bude podporovať úpravy alertingu, parsingu bez nevyhnutnosti učiť sa akýkoľvek programovací/skriptovací jazyk (v súlade s požiadavkou na vykonanie týchto zmien vlastnými silami objednávateľa) |  |
| SIEM-11 | SIEM bude podporovať detekciu sieťových incidentov na základe korelácie informácií z poskytnutých logov a bude podporovať behaviorálnu analýzu spracovaných udalostí. |  |
| SIEM-12 | SIEM bude obsahovať Incident Management konzolu pre správu kybernetických bezpečnostných udalostí a incidentov. V rámci konzoly je k dispozícií časový sled udalostí daného incidentu, možnosť prideľovať riešiteľov, možnosť vyvolať akcie (pre zisťovanie ďalších informácií, dopĺňanie logov, vrátane podrobných informácií z koncového bodu resp. súvisiacich aktív a pod.) |  |
| SIEM-13 | Riešenie je možné prevádzkovať vo forme on premise alebo cloud |  |
| SIEM-14 | SIEM bude bez požiadaviek na externý databázový server |  |
| SIEM-15 | SIEM bude podporovať možnosť súčasnej práce minimálne 10 analytikov |  |
| SIEM-16 | SIEM bude podporovať možnosť tvorby vlastných Dashboardov a Vizuálnych Analýz |  |
| SIEM-17 | Všetky úkony užívateľa (aj interného) v SIEMe budú auditované |  |
| SIEM-18 | SIEM bude podporovať pokročilý reporting s možnosťou schedulingu a distribúcie reportu. |  |
| SIEM-19 | SIEM podporuje zber dát so šifrovaným prenosom (TLS, prípadne šifrovaný obsah správ) na celej trase zdroj /kolektor/ centrálna konzola |  |
| SIEM-20 | SIEM Riešenie podporuje outbound API. Príkladom môže byť pripojenie sa na externé zariadenia alebo systémy (napr. Azure, AWS, Microsoft 365, ticketing system) |  |
| SIEM-21 | SIEM Riešenie podporuje inbound API. Príkladom môže byť pripojenie sa na riešenie SIEM pre vykonanie reportovacích, konfiguračných alebo iných administratívnych úloh. |  |
| SIEM-22 | SIEM Riešenie podporuje minimálne nasledujúce úrovne užívateľských oprávnení (administrátor, read/write, read/only) |  |
| SIEM-23 | SIEM musí podporovať integráciu s Active Directory. |  |
| SIEM-24 | SIEM podporuje vlastnú alebo externú integráciu na Multifaktorovú autentifikáciu. |  |
| SIEM-25 | SIEM podporuje integráciu na Microsoft Azure a Microsoft 365 pre účely monitoringu aktivít užívateľov. |  |
| SIEM-26 | SIEM podporuje spracovanie štruktúrovaných aj neštruktúrovaných dát. |  |
| SIEM-27 | SIEM podporuje vkladanie a monitorovanie vlastných IoC (indikátorov kompromitácie) vrátane manipulácie cez inbound API. |  |
| SIEM-28 | SIEM umožňuje realizáciu tzv. kaskádových dotazov (kaskádové dotazy sú dotazy generované na základe údajoch 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), |  |
| SIEM-29 | Zber udalostí v prostredí Microsoft:  - Udalosti z Microsoft prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Windows systéme. Windows agent musí súčasne podporovať ako monitoring interných windows logov, tak i monitoring textových súborových logov.  - Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií.  - Agent zabezpečuje v prípade potreby funkcionalitu kontroly integrity súborov  - Agent zabezpečuje v prípade potreby funkcionalitu auditovania prístupov k súborom na zariadení.  - Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.  - Filtrácia odosielaných udalostí agentom. Nerelevantné logy sú filtrované na strane windows agenta a nie sú odosielané po sieti.  - Windows agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému.  - Windows agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov. |  |
| SIEM-30 | Zber udalostí v prostredí Linux / MacOs:  - Udalosti z Linux / MacOs prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Linux / MacOs systéme. Linux / MacOs agent musí súčasne podporovať ako monitoring interných logov, tak i monitoring textových súborových logov.  - Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií.  - Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.  - Filtrácia odosielaných udalostí agentom. Nerelevantné logy sú filtrované na strane Linux / MacOs agenta a nie sú odosielané po sieti.  - Linux / MacOs nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému.  - Linux / MacOs agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov. |  |
| SIEM-31 | SIEM umožňuje generovať alert na základe   * Zhoda s vyhľadávaním reťazcom * Definovanej nečinnosti * Definovanej zmeny |  |
| SIEM-32 | SIEM umožňuje nastavenie sieťových zón a sieťových politík podľa ktorých budú generované alerty |  |
| SIEM-33 | SIEM umožňuje nastavenie privilegovaných skupín užívateľov Active Directory podľa ktorých budú generované alerty |  |
| SIEM-34 | SIEM umožňuje sledovať výkonnosť a efektivitu tímu bezpečnostného dohľadu prostredníctvom:   * Stavu riešenia bezpečnostných incidentov (podľa užívateľa, podľa typu alertu, podľa typu útoku,..) * Rýchlosť riešenia v čase * Najčastejších typov útokov * Znovu otvorenie incidentov |  |

* 1. Funkčné požiadavky systému pre UBA:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Požiadavka** | **Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu. |
| UBA-1 | UBA podporuje minimálne nasledujúce korelačné pravidlá pre analýzu správania sa užívateľa:  Vytvorenie/Zablokovanie/ Resetovanie / Povolenie / Únik účtu |  |
| UBA-2 | UBA podporuje minimálne nasledujúce korelačné pravidlá pre analýzu správania sa užívateľa:  Eskalácia privilégií  Prijatie podozrivého odkazu v emailovej správe  Prístup na podozrivý odkaz cez web  Brute Force útok na heslá – lokálny účet  Brute Force útok na heslá – doménový účet  Autentifikácia užívateľa z podozrivej databázy  Manipulácia s lokálnymi udalosťami (event logs)  Prvé prihlásenie na aktívum  Prvé prihlásenie z inej krajiny  Prihlásenie z viacerých krajín súčasne  Detegovaný hash z podozrivej databázy  Spustenie procesu z podozrivej databázy  Impersonizácia administrátora  Autentifikácia servisným účtom  Autentifikácia doménovým účtom  Komunikácia s podozrivou IP  Spustenie vzdialeného súboru  Protokol poisoning  Alert s Microsoft Defender ATP  Spearphishing URL detegovaná |  |
| UBA-3 | UBA podporuje úpravu špecifických korelačných pravidiel (vytvorenie investigatívy, vytvorenie informácie, ..) |  |
| UBA-4 | UBA vytvára rizikový profil užívateľa na základe jeho správania |  |
| UBA-5 | UBA vytvára rizikový profil privilegovaného užívateľa na základe jeho správania |  |
| UBA-6 | UBA podporuje podrobný monitoring definovaných užívateľov |  |
| UBA-7 | UBA podporuje podrobný monitoring aktivít privilegovaného užívateľov v lokálnom aj cloud prostredí |  |

* 1. Funkčné požiadavky systému pre ABA:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Požiadavka** | **Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu. |
| ABA-1 | ABA podporuje korelačné pravidlá pre analýzu správania sa útočníka:  Ako príklad (Zistenie externej IP pomocou príkazového riadku, Spustenie klúča z registra Windows , Spúšťanie procesov pomocou MMC konzole, Rundl32.exe spúšťa súbor s adresára Program Data, Premenovanie netcat, Windows debug v príkazovom riadku a dalšie |  |
| ABA-2 | ABA má integrovaných viac ako 1500 takýchto korelačných pravidiel správania sa útočníka |  |
| ABA-3 | ABA umožňuje mapovať správanie sa útočníka podľa taktík z metodiky MITRE ATT&CK  Reconnaissance  Resource Development  Initial Access  Execution  Persistence  Privilege Escalation  Defense Evasion  Credential Access  Discovery  Lateral Movement  Collection  Command And Control  Exfiltration  Impact |  |
| ABA-4 | ABA podporuje úpravu korelačných pravidiel prostredníctvom výnimiek |  |
| ABA-5 | Databáza korelačných pravidiel správania sa útočníka je kontinuálne aktualizovaná o nové techniky používane útočníkmi. |  |

* 1. Funkčné požiadavky systému pre EDR & FIM:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Požiadavka** | **Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu. |
| EDR-1 | EDR podporuje základnú funkcionalitu odozvy na incident (zrušenie bežiaceho procesu, karanténa aktíva) prostredníctvom Windows/Linux agenta priamo z centrálnej konzole |  |
| EDR-2 | EDR podporuje 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 |  |
| EDR-3 | EDR podporuje funkcionalitu vyšetrovania incidentu prostredníctvom zberu dôkazov preverovaného uživateľa o nasledujúce udalosti:  Account modified  Advanced malware alert  Asset authentication  Cloud service account modified  DNS query  Firewall  IDS  Ingress authentication  Virus infection  Web proxy |  |
| EDR-4 | EDR podporuje rozšírenú funkcionalitu odozvy na incident (spustenie automatizačného workflow,..) |  |
| EDR-5 | EDR podporuje funkcionalitu auditovania integrity súborov pre nasledujúce typy súborov Windows:  .bat  .cfg  .conf  .config  .dll  .exe  .ini  .sys |  |
| EDR-6 | EDR podporuje funkcionalitu auditovania integrity súborov pre nasledujúce typy súborov Linux:  /bin  /boot  /etc  /sbin  /usr/bin  /usr/local/bin  /usr/local/sbin  /usr/sbin  /usr/share/keyrings  /var/spool/cron |  |

* 1. Funkčné požiadavky systému pre NTA

|  |  |  |
| --- | --- | --- |
| **Č.** | **Požiadavka** | **Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu. |
| NTA-1 | NTA podporuje zber nasledujúcich sieťových udalostí:  IDS udalosti  DHCP udalosti  DNS udalosti  IPv4 Flows |  |
| NTA-2 | NTA môže byť nasadené do internej či externej časti siete bez licenčného obmedzenia množstva nasadených zariadení |  |
| NTA-3 | NTA poskytuje špecifické korelačné pravidlá pre SIEM súvisiace s analýzou sieťovej prevádzky. |  |
| NTA-4 | NTA poskytuje špecifické vyhľadávacie vzory (queries) pre SIEM súvisiace s analýzou sieťovej prevádzky. |  |
| NTA-5 | NTA poskytuje špecifické šablóny pre tvorbu dashboard v SIEM súvisiace s analýzou sieťovej prevádzky. |  |
| NTA-6 | Zariadenie pre NTA môžeme inštalovať do fyzického , virtualizačného alebo cloud prostredia. |  |

* 1. Funkčné požiadavky systému pre DT

|  |  |  |
| --- | --- | --- |
| **Č.** | **Požiadavka** | **Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu. |
| DT-1 | DT podporuje tvorbu nasledujúcich pascí pre identifikovanie aktivít útočníka  HoneyPots  HoneyFiles  HoneyUsers  HoneyCredentials |  |
| DT-2 | DT poskytuje špecifické korelačné pravidlá pre SIEM súvisiacich s pascami |  |
| DT-3 | DTumožňuje vyhladávať vzory (queries) pre SIEM súvisiacich s pascami |  |
| DT-4 | DT pasce môžu byť nasadené do internej časti siete bez licenčného obmedzenia množstva nasadených zariadení |  |