Príloha č. 1 Súťažných podkladov

|  |
| --- |
| **OPIS PREDMETU ZÁKAZKY** |

**STRUČNÝ OPIS PREDMETU ZÁKAZKY**

Predmet zákazky zahŕňa

* nákup a implementáciu softvéru pre rozšírenie monitorovacieho systému SIEM od spoločnosti Micro Focus ArcSight,
* nákup a implementáciu organizačných a technických opatrení spojených s rozšírením monitorovacieho systému SIEM a bezpečnostných riešení v rámci celého Ministerstva financií Slovenskej republiky za účelom zabezpečenia súladu so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
* dodávku, implementáciu a podporu systému integrovaného bezpečnostného dohľadu a bezpečnostné analýzy sieťovej prevádzky a dianie na koncových bodoch pre 850 koncových staníc s 30 dňovou dobou uchovávania logov,
* integrácia alertov z nástroja na detekciu a reakciu na útoky na koncové body (EDR – Endpoint Detection and Response) a z analýzy sieťového správania (Network Behavior Analysis (NBA), vytvorenie procesov a efektívne vyhodnocovanie poplachov.

Termín plnenia predmetu zákazky: do 8 mesiacov.

Dodávané riešenie úspešného uchádzača (ďalej aj „zhotoviteľ“ alebo „uchádzač“) musí spĺňať minimálne technicko-prevádzkové parametre, ktoré sú uvedené v opise predmetu zákazky/zmluvy.

Zhotoviteľ je povinný zabezpečiť dodanie kompletného riešenia predmetu zákazky/zmluvy, vrátane dovozu a požadovaných prác na miesto dodania predmetu zákazky/zmluvy. K inštalácii a uvedeniu systému do prevádzky musia byť dodané všetky časti platformy, softvér a aj všetky jeho komponenty, ktoré sú potrebné pre úspešnú inštaláciu a aj beh celého systému.

Ku každému zariadeniu zhotoviteľ dodá minimálne:

* Technickú dokumentáciu od výrobcu v slovenskom alebo českom jazyku alebo anglickom jazyku.
* Návod na použitie (manuál) v slovenskom alebo českom jazyku.
* V prípade nevyvíjaného (komerčného) SW dodá minimálne dokumentáciu od výrobcu v anglickom jazyku.

Hlavné aktivity projektu „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti MF SR“, končia v zmysle harmonogramu projektu a Zmluvy o poskytnutí nenávratného finančného príspevku č. Z311071ACY5 najneskôr 31.08.2023.

Ak sa v súťažných podkladoch uvádzajú údaje, alebo odkazy na konkrétneho výrobcu/výrobný postup/značku/patent/typ, umožňuje sa uchádzačom predloženie ponuky s ekvivalentným riešením, to znamená preukázateľne rovnakými alebo lepšími parametrami ako sú požadované (ak nie je v tejto prílohe uvedené inak).

Všetky zariadenia dodávané v rámci systému musia byť technologicky vyspelé značkové produkty, nové, nepoužité, plne kompatibilné tak, aby spolu tvorili jeden funkčný celok.

PODROBNÝ OPIS PREDMETU ZÁKAZKY

**Softvér pre rozšírenie monitorovacieho systému SIEM**

Objednávateľ vyžaduje rozšírenie existujúceho SIEM riešenia od spoločnosti Micro Focus ArcSight. Ďalej vyžaduje zabezpečenie monitorovania, zhromažďovania, centrálneho uchovávania a vyhodnocovania bezpečnostných udalostí (logov) z prvkov infraštruktúry (sieťová infraštruktúra, servery,...), databáz, aplikácií, pracovných staníc a iných zdrojov v prostredí objednávateľa.

* Všetky potrebné komponenty musia byť súčasťou dodaného systému SIEM, vrátane databázy.
* Rozhranie všetkých komponentov systému požaduje objednávateľ v slovenskom alebo anglickom jazyku.
* Všetky požadované funkcie sú riadené a používané prostredníctvom spoločnej kontrolnej konzoly ("centrálna správa"), ktorá je tiež prístupná cez webové rozhranie z fyzického aj virtuálneho počítača alebo iným podobným spôsobom. Prezentácia údajov musí byť vykonaná v grafickej forme, prezentačné rozhranie musí byt multiplatformové alebo platformovo nezávislé a plne funkčné na Windows, Linux, Apple OS. X.
* Centrálna správa systému musí podporovať GUI (grafické užívateľské rozhranie).
* Všetky konfigurácie, definície zdrojov LOG-ov, definície korelačných pravidiel, vytváranie správ, musia byť vykonané z jedného grafického rozhrania.
* Riešenie musí umožňovať prístup viacerým používateľom v rovnakom čase, a to ako na úrovni vstupných/zdrojových dát a incidentov. Prístup užívateľov musí vychádzať z voľne definovaných, oddelených úloh s možnosťou granulovaného prideľovania práv v rámci každej úlohy, zdrojových údajov, identifikácie sledovaných zariadení, skupín zariadení a serverov, typu vstupných údajov atď.
* Riešenie musí podporovať alebo byť rozšíriteľné pre úplné oddelenie užívateľských skupín k prístupu k rôznym dátam a konfiguráciám, kde jednotlivé inštancie môžu mať možnosť vlastnej konfigurácie a správy (multi-tenant prístup).
* SIEM systém musí byť schopný vyhľadávať podľa kľúčových slov (reťazcov) v názvoch zdrojov, v korelačných pravidlách v uložených logoch a v auditných logoch systému (to znamená vyhľadávanie v konfiguračných položkách a kontextových položkách, to znamená v "contentu").
* Riešenie musí natívne podporovať protokol IPv4, IPv6.
* Komponenty SIEM musí podporovať monitorovanie vlastnej dostupnosti a jednotlivých častí (zariadení) prostredníctvom protokolu SNMP v2/v3 alebo prihlásenia na vzdialený server syslog.
* Systém musí umožňovať export/import nastavenia zo/do súboru (definícia dashbordov, reportov a korelačných pravidiel – t. j. "contentu").
* Systém SIEM musí obsahovať plne integrovaný nástroj na riadenie celého životného cyklu incidentu (ticketing).
* V prípade poruchy zberu logov z určitého zariadenia, SIEM musí byť schopný generovať alert.
* SIEM musí podporovať automatickú identifikáciu zdroja logov.

**Výkon, škálovateľnosť a licenčné požiadavky**

* V rámci dodania dodá úspešný uchádzač licencie za účelom pokrytia požadovanej funkcionality. Zaručenie požadovanej funkcionality nie je podmienené nákupom ďalších licencií.
* Systém SIEM nie je licencovaný obmedzený na počet generujúcich zariadení/zdrojov logov, počet registrovaných aktív, a počet užívateľov/konzol.
* Zložka SIEM musí mať zaručenú licenciu na spracovanie podľa fáz implementácie uvedených nižšie, ako aj fázy implementácie musia umožňovať zvýšenie vplyvu EPS (events per second – počet udalostí za sekundu).
* Súčasť Log Managementu musí mať garantovanú licenciu na spracovanie najmenej 1000EPS.
* Súčasť Log Managementu musí mať garantovaný výkon pri spracovaní 1000 EPS.
* SIEM a LM nesmú technicky obmedzovať počet udalostí (napríklad v prípade prekročenia licencie alebo výkonu zakúpeného riešenia) počas určitého časového obdobia, aby sa zabránilo ich vyradeniu.
* SIEM systém musí podporovať súčasnú prácu min. 5 užívateľov.
* Licencia musí obsahovať možnosť zhromažďovať všetky typy výrobcom podporovaných zdrojov udalostí a vlastných logov.

**Požadované služby pre rozšírenie monitorovacieho systému SIEM**

* Analytické práce pre posúdenie existujúcich bezpečnostných riešení a nástrojov pre integráciu do SIEM prostredia.
* Dizajn wokflow-u, implementácia bezpečnostných politík.
* Návrh a implementácia operačných postupov pre rutinné operácie správy s využitím funkcionality delenia práce pre jednotlivé tými v rámci perimetra siete.
* Mapovanie požiadaviek technického návrhu na funkčné celky infraštruktúry.
* Detailný design.
* Import bezpečnostných politík.
* Inštalácia SW a všetkých nástrojov.
* Zohľadnenie backup politík a vytvorenie backup plánu, pre Log Data na zabezpečenie konzistencie a retencie.
* Komplexná technická dokumentácia na všetkých vrstvách dodaného riešenia.
* Zabezpečenie zaškolenia pre obslužný personál v rozsahu uvedenom v návrhu na plnenie kritérií, v zmysle Prílohy č. 4 týchto súťažných podkladov.

**Organizačné a technické opatrenia spojené s rozšírením monitorovacieho systému SIEM požiadavky na dodanie služieb**

1. Komplexné ohodnotenie zraniteľností organizácie s transferom znalostí na zamestnancov objednávateľa.

Poskytnutá služba musí zahŕňať:

* ohodnotenie zraniteľností z externého prostredia,
* ohodnotenie zraniteľností z interného prostredia,
* transfer znalostí – školenie.

Ohodnotenie zraniteľností z externého prostredia musí zahŕňať:

* identifikácia informácií zistiteľná prostredníctvom techník OSINT,
* automatizovaný test sieťových a webových služieb,
* manuálne overenie zistených zraniteľností,
* exploatácia zistených zraniteľností.

Pre dostupné webové portály aj overenie webových služieb v zmysle metodiky OWASP 4.2

* klasifikáciu zraniteľností a návrh bezpečnostných opatrení,
* tréning a vysvetlenie procesu testovania zamestnancom zákazníka minimálne v rozsahu 60 hodín.

Ohodnotenie zraniteľností z interného prostredia musí zahŕňať:

* mapovanie aktív,
* automatizované overenie zraniteľností v interných infraštruktúrach,
* manuálna verifikácia zistených zraniteľností,
* overenie možností lateral movement v organizácií,
* exploatácia zraniteľností,
* tréning zamestnanca zákazníka na vykonanie ohodnotenia zraniteľností zákazníka minimálne v rozsahu 60 hodín,
* klasifikácia zraniteľností a návrh bezpečnostných opatrení.

Výsledkom služby musí byť správa z ohodnotenia zraniteľností, ktorá minimálne zahŕňa:

* manažérske zhrnutie,
* použité metodiky,
* použité nástroje a spôsob ich použitia,
* zoznam a podrobný nájdených bezpečnostných zraniteľností a vektorov útoku,
* pre každú zraniteľnosť,
* popis zraniteľnosti,
* CVSS maticu a ohodnotenie,
* dôkaz existencie zraniteľnosti,
* návrh bezpečnostných opatrení.

Súčasťou poskytnutých služieb sú aj bezpečnostné konzultácie k navrhovaným opatreniam a ich implementácie minimálne v rozsahu uvedenom v návrhu na plnenie kritérií, v zmysle Prílohy č. 4 týchto súťažných podkladov.

**Systém integrovaného bezpečnostného dohľadu a bezpečnostné analýzy sieťovej prevádzky a dianie na koncových bodoch**

Všeobecné požiadavky na systém – systém musí umožňovať:

1. Detegovať pohyb škodlivého kódu po sieti, jeho uloženie na koncových staniciach a jeho prípadné spustenie.
2. Detegovať ďalšie praktiky útočníkov - napríklad pokusy zneužiť zraniteľnosti, pokusy o laterálna pohyb a exfiltrácia dát.
3. Poskytovať retrospektívne informácie o dianí v ICT záznamom informácií o dianí na sieti (predovšetkým na perimetra siete) a na koncových bodoch (staniciach s OS Windows, Linux a MacOS a serveroch s OS Windows Server a OS Linux) s možnosťou ich následného zobrazenia a prehľadávanie.
4. Umožňovať vyšetrovanie incidentov vykonávaním vzdialených aktivít na koncových bodoch.
5. Umožňovať vykonávať nápravu stavu po útoku vzdialeným vykonávaním akcií na koncových bodoch.

Kvantitatívne požiadavky na systém:

EDR systém požadujeme pre 850 koncových staníc s 30 dňovou dobou uchovávania logov.

Kvalitatívne požiadavky na systém:

Systém bude slúžiť ako nástroj bezpečnostných špecialistov - očakávame teda možnosť:

1. Jednoducho a rýchlo definovať vlastné detekčné pravidlá pre javy, ktoré budeme považovať za zaujímavé, a ktoré nie sú pokryté popisom hrozieb (threat-intel) dodávaným výrobcom technológie.
2. Tvoriť a upravovať predvolené reporty vrátane určenia periodicity ich automatického generovania a odosielanie.
3. Tvoriť ad-hoc dotazy do alertov a záznamov o sieťovej prevádzke a činnosti na koncových bodoch.
4. Vykonávať úlohy na koncových bodoch s cieľom investigácie alebo remediácie stavu koncového bodu.

Požiadavky na funkčnosť časti systému:

Ostatné Systém bezpečnostného monitorovania koncových bodov (staníc a serverov) s funkcionalitou EDR

 Systémová správa:

* správa užívateľov,
* inštalácia a odinštalovanie aplikácií,
* zmena nastavenia operačného systému (napríklad zapnutie firewallu a AV).

Detekcia Pokročilá detekcia hrozieb:

* detekcia škodlivého kódu jeho rozpoznaním podľa vzorov pre obsah,
* detekcia škodlivého kódu pomocou pravidiel popisujúce správanie,
* detekcia prejavov činnosti útočníka na koncovom bode,
* analýza bežiacich procesov na stanicu a ich ohodnotenie z hľadiska činností, ktoré vykonávajú alebo by mohli vykonávať.

Vyšetrovanie Systém bude kontinuálne zaznamenávať činnosti na koncových bodoch v podobe meta-dát v týchto oblastiach:

* spustenie a ukončenie procesov,
* súborové manipulácia,
* manipulácia s registrami,
* sieťových spojenie vrátane URL pre http spojenie,
* DNS prekladov,
* Manipulácia s USB médiami a prenosy súborov na ne,
* Windows udalosti (Windows Events).

Reakcia Systém umožní vykonanie akcie na koncovom bode alebo bodoch odoslaním úlohy na vykonanie a tiež interakcií s koncovým bodom v reálnom čase.

 Automatizácia reakcie na incidenty:

* Automatickým spúšťaním podujatí (pripraveným aj užívateľom definovaných) na koncových bodoch v prípade výskytu určitého alarmu, ktorý sa ku koncovému bodu vzťahuje.

 Ochrana koncového bodu:

* Zabránenie spusteniu procesu podľa hash alebo výrazu YARA.

Požiadavky v oblasti otvorenosti platformy:

Rozhranie Zdokumentované štandardizované aplikačné rozhranie pre zákaznícke integrácie s ďalšími bezpečnostnými komponentmi. Preferujeme http & XML alebo JSON API rozhrania.

 Predpripravené integračné väzby na aplikácie typu SIEM

 Systém musí pre budúce potreby podporovať integráciu s:

* komponentov pre detekciu APT útokov na sieťovej prevádzke (NDR / NTA),
* komponenty sieťových návnad (honeypots).

 Systém umožní zhodnotenie hrozby integráciou na službu Vírus Total alebo obdobnú službu.

 Jednotné užívateľské rozhranie pre analytiku, vyšetrovanie a reakciu spoločnú pre prostredie siete i koncových bodov.

Ostatné Systém bude napojený na zdroj aktualizovaných informácií o hrozbách (threat-intelligencia) a bude z toho zdroja vykonávať pravidelne aktualizácie.

 Systém bude možné napojiť na vlastné alebo otvorené zdroje informácií o hrozbách vo formátoch JSON, CSV a STIX.

 Systém bude umožňovať import popisu IOC vo formáte OpenIOC a YARA.

Ďalšie požiadavky na vlastnosti časti systému pre bezpečnostné monitorovanie koncových bodov:

Ostatné Systém musí podporovať koncové body s operačnými systémami:

* Windows 7 a vyššie,
* Windows Server 2008 R2 a vyššie,
* Linux CentOS 6 a vyššie,
* RedHat Enterprise Linux 6 a vyššie,
* MacOS 10.11 a vyššie.

 Na koncových staniciach musí Agentské časť využívať zanedbateľnú časť zdrojov - agent by nemal prekročiť po väčšinu času jednotky (max. 4%) využitie CPU.

 Agent systému musí byť odolný proti odinštalovaniu a pokusom ho zastaviť alebo poškodiť.

 Odinštalovanie agentov musí vyžadovať zvláštne autentizáciu (heslo pre odinštalovanie).

 Udalosti budú zaznamenávané do centrálneho úložiska v reálnom čase a budú spätne dostupné s časovou retenciou min. 30 dní.

 Systém musí byť schopný zaznamenávať metadáta o správaní koncových bodov, alerty a výsledky úloh aj pre koncové body, ktoré sú dočasne mimo siete, ich uchovaním na koncovom bode až do ich odoslania so systému aspoň počas 5 dní.

Rozhranie Alerty generované systémom musia byť zobrazované v centrálnej konzole.

Požadované funkcionality v oblasti viditeľnosti, vyšetrovanie a analýzy na koncových bodoch:

Vyšetrovanie Systém musí byť schopný nájsť súbor na disku koncového bodu podľa:

* obsahu,
* hashe,
* názvu,
* veľkosti,
* koncovky,
* času vytvorenia / modifikácie,
* kombinácia vyššie uvedeného.

 Systém bude umožňovať vyhľadávanie súboru aj pre zmazané súbory.

 Systém bude umožňovať vyhľadávanie súboru na súborovom systéme, logickom aj fyzickom disku v ich využité (obsadené / alokovanej) i nevyužité časti.

 Systém bude pre bežiace procesy schopný extrahovať:

* otvorené sokety,
* súborové handle,
* informácie o DDL, ktoré boli dynamicky prelinkované vrátane informácie, či boli injektované,
* obsadený virtuálny priestor adries.

 Systém musí byť schopný na požiadanie - alebo ako súčasť automatickej reakcie - získať informácie o okamžitom stave koncového bodov minimálne v oblastiach:

* prihlásenie užívatelia,
* vystavená sieťové spojením,
* bežiaci procesy,
* zoznam zavedených lokálnych Správcov,
* zoznam nainštalovaného software,
* zoznam nainštalovaných dôveryhodných certifikátov,
* čas od zapnutím počítača,
* stav Antivirus,
* stav firewallu,
* zoznam do Pamäti nahratých ovládačov,
* zoznam kľúčov a hodnota autorun v registroch,
* výpis obsahu DNS a APR vyrovnávacích pamäti,
* HW inventár,
* obsah smerovacími tabuľky,
* zoznam aktívnych sieťových rozhraní.

 V prípade potreby musí byť systém schopný spustiť rozšírené úlohy zisťujúce stav koncového bodu v oblasti:

* získanie histórie navštívených stránok webového prehliadača,
* získanie záznamu sieťovej prevádzky koncového bodu,
* získanie obrazu logického disku alebo fyzického disku,
* získanie obrazu pamäte.

 Systém musí byť schopný zobraziť činnosti určitého procesu vo vzťahu k:

* súborovým manipuláciám,
* manipuláciám s registrami,
* sieťovým spojením,
* spusteným vláknam,
* to všetko ideálne na časovej osi.

 Forenzná analýza:

* vzdialene - získaním obrazu pamäte určitého procesu.

 Forenzná analýza:

* vzdialene - získaním obrazu celej pamäte,
* vzdialene - získaním obrazu disku.

Rozhranie Systém bude umožňovať vyhľadávanie v metadátach podľa ľubovoľného parametra udalosti (napríklad meno procesu, meno rodiča, PID, hash, meno súboru, meno kľúče v registroch, IP adresa servera, URL spojenia).

Požadované funkcionality v oblasti odpovedi na hrozbu na koncových bodoch:

Reakcie Systém musí umožniť na stanici:

* zmazať súbor,
* ukončiť proces,
* sieťová izolácia koncového bodu (pri zachovaní komunikácie systému s agentom na koncovom bode),
* modifikácia / mazanie obsahu registrov,
* inštalácia a odinštalovanie aplikácií a záplat,
* odhlásenie užívateľa,
* zapnutie a vypnutie firewallu,
* reštartovanie, vypnutie a hybernácie koncového bodu.

 Systém musí byť schopný automatického spustenia vybranej akcie ako automatické odpovede na určitý alert.

 Schopnosť agenta systému vykonávať viac akcií súčasne.

 Systém musí umožniť prístup ku koncovému bodu v reálnom čase (konzolový prístup) na účely vyšetrovania a remediácie.

 Systém musí umožniť zobrazenie bežiacich procesov na koncovom bode v reálnom čase a základné manipuláciu s nimi - napríklad ich ukončenie a získanie obrazu pamäte procesu.

 Systém musí umožniť zobrazenie vzdialeného súborového systému koncového bodu a základné manipulácia so súbormi - napríklad získanie súboru, zmazanie súboru.

 Automatizácia reakcie na incidenty:

* automatickým spúšťaním session (preddefinované aj užívateľom definovaných) na koncových bodoch v prípade výskytu určitého alarmu, ktorý sa ku koncovému bodu vzťahuje.

Požadované funkcionality v oblasti klasifikácie udalosti podľa MITRE ATT & AC framework:

Ostatné Systém musí klasifikovať udalosti podľa MITRE ATT & CK frameworku uvedením zodpovedajúce techniky a / alebo taktiky útočníka:

 Vlastné pravidlá možno definovať tak, aby používali kategórie MITRE ATT & CK frameworku.

Požadované funkcionality v oblasti rozpoznania zraniteľností SW:

Detekcia Systém musí rozpoznať zraniteľnosti nainštalovaného softvéru na koncových bodoch.

Implementačné práce

* Vypracovanie “Low Level Designu “ pred začatím implementačných prác.
* Inštalácia softvéru a všetkých požadovaných nástrojov.
* Zohľadnenie backup politík a vytvorenie backup plánu, pre Log Data na zabezpečenie konzistencie a retencie.
* Komplexná technická dokumentácia na všetkých vrstvách dodaného riešenia.
* Zabezpečenie zaškolenia pre obslužný personál v rozsahu uvedenom v návrhu na plnenie kritérií, v zmysle Prílohy č. 4 týchto súťažných podkladov.

**Integrácia alertov z nástroja na detekciu a reakciu na útoky na koncové body (EDR – Endpoint Detection and Response) a z analýzy sieťového správania (Network Behavior Analysis - NBA), vytvorenie procesov a efektívne vyhodnocovanie poplachov.**

Poskytnutá služba musí zahŕňať :

* Analýzu prostredia z pohľadu zbieraných údajov z NBA, Endpointov a EDR.
* Vytvorenie postupov a procesov na integráciu informácií z EDR, NBA a vytvorenie reportov z identifikovaných alertov.
* Vyškolenie zamestnancov objednávateľa v procesoch riešenia incident response na úrovni riešenia incidentov identifikovaných EDR, NBA a bezpečnostnými technológiami do úrovne L2 vo forme vedeného riešenia identifikovaných incidentov priamo v organizácií v rozsahu uvedenom v návrhu na plnenie kritérií, v zmysle Prílohy č. 4 týchto súťažných podkladov.
* Manažment konfigurácie EDR a NBA pre efektívnu identifikáciu bezpečnostných udalostí.
* Poskytovanie L3 podpory zamestnancom objednávateľa po dobu 24 mesiacov.
* Vykonávanie proaktívneho vyhľadávania hrozieb minimálne raz týždenne prostredníctvom implementovaných nástrojov EDR a NBA, počas trvania 24 mesiacov.

Technické prostriedky a služby spojené s prevádzkou, pre inštaláciu softvéru potrebného pre prevádzku systému správy mobilných zariadení (klastrové virtualizácie prostredia) **nie sú súčasťou požadovanej dodávky.**