**Príloha č. 1 –** Opis predmetu zákazky, tejto Výzvy

**„Dodanie, implementácia a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov. \_CP22/2024**“

**Opis predmetu zákazky**

**Úvod**:

Predmetom zákazky je **„****Dodanie, implementácia a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov.** “ ktorého cieľom je ochrana počítačovej siete, koncových zariadení, informačných aktív a naplnenie požiadaviek legislatívy na riešenie kybernetických bezpečnostných incidentov a opatrení pre oblasť ochrany, monitorovania, testovania bezpečnosti, riešenia a analýzy incidentov a bezpečnostných auditov /ďalej ako EPPEDR/ , a to najmä:

- zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,

- vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Poskytovateľ poskytne:

**Dodanie a implementáciu komplexného nástroja pre EPPEDR s požadovanými funkciami a službami vrátane podpory prevádzky a údržby dodaného komplexného nástroja EPPEDR pre zaistenie spoľahlivej, kontinuálnej a bezpečnej prevádzky v súlade s dokumentáciou systému a aktuálnymi požiadavkami Objednávateľa, vrátane riešenia Problémov a Incidentov**

1. **Kapacitné požiadavky na komplexný systém**

Definovanie vstupných zdrojov verejného obstarávateľa

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lokalít | Počet AD užívateľov | Počet AD administrátorov | Počet serverov (virtualizačné + virtuálne) a počet fyzických serverov | Počet pracovných staníc |
| 12 | 560 | 5 | 60 | 500 |

Počet koncových zariadení pre implementáciu komplexného nástroja EPPEDR s riešením problémov a incidentov je **560.** To sú zariadenia na ktorých bude EPPEDR nainštalovaný a prevádzkovaný a na ktorých budú riešený dohľad, problémy a incidenty **24/7 na obdobie 36 mesiacov** .

1. **Špecifikácia požadovaných služieb** 
   1. **Dodanie a implementáciu komplexného nástroja EPPEDR s požadovanými funkciami, ktorými sú**

|  |
| --- |
| Singularity Platform. Access to the Singularity Platform, includes initial XDR Ingest |
| Complete Protection Platform (Per Workstation). EPP + EDR, with NGAV (AI), Rogues IoT, Firewall Control, Device Control, Remote Shell, EDR Hunting and Investigation and up to 100 concurrent STAR Rules, Standard Support Plan |
| Complete Cloud Workload Security (Per Server). EPP + EDR, with NGAV (AI), Rogues IoT, Firewall Control, Device Control, Remote Shell, EDR Hunting and Investigation and up to 100 concurrent STAR Rules, Standard Support Plan |
| Ranger Attack Surface Management Platform (per Endpoint). Enterprise-wide Discovery of IT/IoT, Attack Surface Reduction, Peer-to-Peer Deployment Capability for SentinelOne Agents |
| Singularity Ranger AD (Per User). Cloud-based enterprise wide active directory and Azure AD Assessment and real time attack detection |
| Vigilance Respond Pro (Per Endpoint). Vigilance Respond Pro: 24x7 MDR, and incident response |

**Pre realizáciu činností**

Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov spolu so softvérovými licenciami pre Komplexný nástroj alebo predplatenými službami na poskytovanie Komplexného nástroja na obdobie **36 mesiacov** pre **560** koncových staníc z ktorých je **60** serverov.

* + 1. **Funkčné požiadavky na EPPEDR**

|  |  |
| --- | --- |
| The proposed solution must identify rogue devices discovery capability to reduce the potential attack surface. | Navrhované riešenie musí mať schopnosť identifikovať neautorizované zariadenia na redukciu bodov, ktoré by mohli byť využité na potencionálny útok. |
| The proposed solution must provide a software/application inventory for the environment | Navrhované riešenie musí poskytovať inventár softvéru/aplikácií pre prostredie. |
|  | Navrhované riešenie musí umožňovat inštaláciu agentov metódou Peer-to-Peer |
| Dashboards & Reporting | Dashboards & Reporting |
| The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option | Navrhované riešenie musí hlásiť všetky známe zraniteľnosti v programoch nainštalovaných na koncovom bode, spolu s možnosťou exportu dát. |
| The proposed solution have option to export data into 3rd party reporting tools such as Tableau or PowerBI | Navrhované riešenie musí mať možnosť exportovať dáta do nástrojov na správu dát tretích strán, ako sú Tableau alebo PowerBI. |
| The proposed solution must have customizable dashboards as per user | Navrhované riešenie musí mať možnosť prispôsobiteľných informačných panelov podľa požiadaviek používateľa. |
| Compliance | Compliance |
|  | Výrobca navrhovaného riešenia musí byť zaradený podľa nezávislého a medzinárodne uznávaného hodnotenia jednotlivých bezpečnostných produktov spoločností Gartner, Inc., Magic Quadrant for Endpoint Protection Platforms do kategórie „Leaders“, minimálne posledné dva roky. |
| The proposed solution must be fulfilling following compliances such as HIPAA compliant ,PCI compliant,GDPR compliant,ISO27001 compliant | Navrhované riešenie musí spĺňať súladové požiadavky, ako sú súlad s HIPAA, súlad s PCI, súlad s GDPR. SaaS platforma výrobcu musí byť certifikovaná podľa SOC 2 Type II. |
| Integrations | Integrácia |
| The proposed solution should support integration with Active Directory | Navrhované riešenie musí podporovať integráciu s Active Directory. |
| The proposed solution should have integrations to Virus Total or similar tools | Navrhované riešenie musí mať integrácie s nástrojmi ako Virus Total alebo podobnými. |
| The proposed solution should have native integrations/integrations with SIEM solutions such as Splunk, Qradar & etc. | Navrhované riešenie musí mať natívne integrácie alebo integrácie so SIEM riešeniami ako Splunk, Rapid 7, Qradar a podobnými. |
| The proposed solution should have option to send event logs via Syslog. | Navrhované riešenie musí mať možnosť odoslať udalostné protokoly cez protokol Syslog. |
|  | Bezpečnost Active Directory |
|  | Riešenie musí vykonávať testy na detekciu zraniteľností Active Directory spojených s autentifikáciou, autorizáciou, nastavením účtu, certifikačnými službami, oprávneniami/delegáciami a bezpečnostnými problémami priamo súvisiacimi so zabezpečením Domain Controller(ov) a Azure AD. |
|  | Riešenie musí kategorizovať testy do najmenej štyroch závažností od najkritickejších po najnižšiu |
|  | Riešenie musí byť schopné príjmať oznámenia z on-premise AD (provozné udalosti) v reálnom čase. |
|  | Riešenie nesmie vyžadovať plné administrátorské oprávnenia na Active Directory alebo Domain Controlleroch. |
|  | Riešenie musí obsahovať bezpečnostné hodnotenia pre on-premise a Azure AD. |
|  | Riešenie musí mať možnosť nasadenia on-premise. |
|  | Overenia on-prem AD musia byť vykonávané jediným zariadením pripojeným k doméne. |
|  | Riešenie nesmie vyžadovať VPN pripojenie medzi on-prem komponentmi a cloudovou konzolou. |
|  | Riešenie musí byť schopné automaticky objaviť viaceré domény a zahrnúť ich do rozsahu testov a ochrany. |
|  | Riešenie musí byť schopné vykonávať overenia Azure-AD prostredníctvom API poskytovaného spoločnosťou Microsoft. |
| ● The solution must be able to detect attacks against the AD, including: o ‘Low and slow’ brute force attempts like ‘Password Spray’ o Mass account lockouts o Mass Password changes o Mass account disabling/deletion o Suspicious password changes for sensitive accounts o Reactivation of disabled privileged accounts o DCSync attacks o Rouge Domain Controller attacks (DCShadow) o Use of the default “Administrator” account o Suspicious service creation on Domain Controller(s) | Riešenie musí byť schopné detegovať útoky voči Active Directory, vrátane:   Low and slow pokusy o hrubú silu, ako je Password Spray,  Hromadné uzamknutie účtov,  Hromadná zmena hesiel,  Hromadné vypnutie/zmazanie účtov,  Podozrivé zmeny hesiel pre citlivé účty,  Znovuaktivácia deaktivovaných privilegovaných účtov,  Útoky DCSync,  Útoky na rouge Domain Controller (DCShadow),  Použitie default účtu Administrator,  Podozrivé vytváranie služieb na Domain Controller(och). |
| ● Threat detection must not rely on scheduled AD replication to minimize impact on the AD. | Detekcia hrozieb nesmie spočívať v plánovanom replikovaní AD, aby sa minimalizovalo zaťaženie na AD |
|  | Riešenie musí umožnovať externé spracovanie detekcie hrozieb do riešení SIEM, SOAR a XDR |
|  | Riešenie musí poskytovať podrobné usmernenia na odstránenie zistených zraniteľností, vrátane  Odkazy na taktiky a techniky MITRE Att&ack,  Kroky na prípravu remediacie,  Kroky na vykonanie remediacie,  Odkazy na doplnkové informácie od širšej komunity pre zabezpečenie AD. |
|  | Riešenie musí byť schopné generovať skripty na remediaciu, ktoré možno vykonať v príslušných doménach s nasledujúcimi schopnosťami:  Podrobný výber zraniteľností na odstránenie,  Podrobný výber objektov, na ktorých sa bude remediacia vykonávať,  História remediacie o stave procesu remediacie (vygenerovaný skript, stiahnutý, vykonaný s výsledkom úspechu alebo zlyhania),  Skripty na vrátenie zmien pri bývalej remediacii na základe skriptu. |
|  | Riešenie musí byť schopné automaticky spúšťať celý testovací cyklus v konfigurovateľnom rozvrhu používateľa (napr. každých X dní), pridať výsledky do svojej databázy a generovať podrobné testovacie správy bez ďalšieho zásahu používateľa. |
|  | Riešenie musí podporovať ad-hoc spustenia celého testovacieho cyklu a prezentovať výsledky v GUI a v podrobných správach. |
|  | Riešenie musí podporovať spustenie individuálnych testov ad-hoc, bez potreby spúšťať celý testovací cyklus. |
|  | Systém musí podporovať vytváranie a dokumentovanie výnimiek pre budúce testovacie behy na nasledujúcich úrovniach:  Domény,  Jednotlivé testy pre doménu,  Jednotlivé objekty (užívateľ alebo skupina) pre test a doménu. |
|  | Riešenie musí podporovať vytváranie týchto výnimiek na centrálnej lokalite v GUI alebo priamo z príslušných testov/výsledkov s možnosťou pridávania komentárov k tomu, prečo boli tieto výnimky vytvorené. |
|  | Riešenie musí obsahovať informačný panel, ktorý poskytuje rýchle informácie o výsledkoch testov, ako sú:  Počet testov podľa závažnosti a ich výsledky (úspech/zlyhanie/skipované) celkom a pre testované domény,  Zistená topológia domény a vzťahy medzi doménami,  Skóre zdravia a priradená úroveň rizika celkovo a individuálne pre jednotlivé domény,  Najkritickejšie/závažné zistenia a počet ovplyvnených objektov,  Grafická reprezentácia zlyhaných testov v posledných behoch, ktorá umožňuje používateľovi rýchlo vidieť zmeny v zabezpečení v čase. |
| ● The solution must provide extensive filtering capabilities of test results including at least: o Previous tests o Severity o Domain name o Forest name o Detection name o Acknowledgement status o Vulnerability status o Computer(s) affected o Group(s) affected o User(s) affected | Riešenie musí poskytovať rozsiahle možnosti filtrovania výsledkov testov, vrátane aspoň:  Predchádzajúce testy,  Závažnosť,  Názov domény,  Názov forest,  Názov zistenia,  Stav potvrdenia,  Stav zraniteľnosti,  Počítač(y) ovplyvnené/postihnute,  Skupina(y) ovplyvnená/postihnuta,  Užívateľ(ia) ovplyvnení/postihnuty. |
|  | Riešenie musí byť schopné porovnávať výsledky testov s predchádzajúcimi . |
|  | Riešenie musí poskytovať minimálne nasledujúce podrobnosti o každom vykonanom teste:  Popis testu,  Odkaz na relevantné webové stránky MITRE Att&ck,  Mitigačné kroky,  Nástroje na útok, ktoré môžu využívať zistenú zraniteľnosť,  Odkazy na relevantné články od komunity pre zabezpečenie AD. |
|  | Riešenie musí poskytovať podrobné informácie o dôvodoch zistenia zraniteľností, vrátane:  Typy objektov, napr. Užívateľ alebo Skupina,  Názvy objektov,  Porušené nastavenia na úrovni objektu, napr. aké oprávnenia boli zistené. |
|  | Služby a podpora |
|  | Súčasťou riešenia musia byť dohľadové služby MDR - Managed Detection and Response, kontrola incidentov z prostredí zákazníka poskytované výrobcom riešenia. |
|  | Výrobca musí poskytovať aj voliteľnú možnosť priameho riešenia a uzatvárania týchto incidentov MDR týmom. |
|  | V rámci služby musí byť k dispozícii analýza prvotnej príčiny incidentu dostupná na vyžiadanie. |
|  | Služba musí byť poskytovaná v režime 24x7 |
|  | Súčasťou služby musí byť ročný balík konzultačných hodín, ktorý zákazník môže použiť podľa potreby na podrobné vyšetrovanie, alebo proaktívné služby spojené s bezpečnosťou. |
|  |  |

Alebo ekvivalentné riešenie.

**2.1.2 Implementácia komplexného EPPEDR nástroja v  rozsahu**

* + - nastavenie a konfigurácia prostredí verejného obstarávateľa,
      * konfigurácia Windows systémov
      * overenie funkčných a výkonových parametrov Windows agentov,
      * konfigurácia Linux systémov
      * overenie funkčných a výkonových parametrov Linux agentov,
      * predvedenie vytvorenia a uloženia vlastného dashboardu a reportu,
      * predvedenie vytvorenia a uloženia užívateľsky definovaného parseru,
      * konfigurácia cloudovej služby
    - nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom verejného obstarávateľa,
    - zaškolenie obsluhy a správy systému pre minimálne 2 zamestnancov verejného obstarávateľa,
    - vytvorenie a odovzdanie prevádzkovej dokumentácie systému, administrátorskej dokumentácie,

1. **Služby podpory prevádzky a údržby dodaného komplexného nástroja pre EPPEDR**
   * post-implementačná podpora v rozsahu **10 človekodeň na obdobie 36 kalendárnych mesiacov**, ktorá obsahuje:

* Technická  podpora prostredia
  + Inštalácia a konfigurácia
  + Konfigurácia systémových nastavení
  + Konfigurácia kolektorov
  + Konfigurácia alertov
  + Konfigurácia queries
  + Konfigurácia dashboard
  + Konfigurácia custom parser a event sources (data management)
  + podpora pri riešení technických problémov s platformou
* Konzultačná podpora pri identifikovaných bezpečnostných incidentoch
* Podpora ďalšieho rozvoja riešenia
  + zdroje udalostí,
  + integrácie
  + využitie funkcionalít systému,
  + licenčný model
* Komunikácia s výrobcom
  + hlásenie technických problémov výrobcovi,  dotazy na obchodnú podporu

1. **Postup pri riešení Problémov/požiadaviek – Helpdesk:**

Na hlásenie problémov zo strany Objednávateľa bude Poskytovateľ prevádzkovať Helpdesk, ktorý bude poskytovať službu, ktorá pozostáva z nasledujúcich činností:

* Identifikácia Problému – poskytnutie pomoci Objednávateľovi s cieľom identifikovať príčinu daného Problému v rozsahu podporovaného IS Objednávateľa,
* Poskytovanie informácií o stave riešenia požiadaviek prostredníctvom on-line vzdialeného prístupu oprávnených osôb Objednávateľa do Helpdesku.

**Postup**

1. Oprávnená osoba Objednávateľa zadáva/hlási problém/požiadavku v systéme Helpdesk na adrese: XXXXXX, v prípade nedostupnosti e-mailom na xxx Oprávnená osoba Objednávateľa nahlasuje problém podľa predchádzajúcej vety Poskytovateľovi až potom, ako nebolo možné vyriešiť tento problém v prvom stupni Oprávnenou osobou Objednávateľa.

Uskutočniť takéto hlásenie môže výlučne Oprávnená osoba Objednávateľa. Každé hlásenie Problému prijaté akýmkoľvek spôsobom sa zaeviduje v Helpdesku. Helpdesk vygeneruje identifikačné číslo požiadavky/problému. Helpdesk eviduje minimálne: čas odoslania hlásenia a oprávnenú osobu, kritickosť , čas prijatia hlásenia oprávnenou osobou Poskytovateľa, čas pridelenia riešiteľovi, čas zahájenia riešenia a čas vyriešenia požiadavky alebo Problému. Akákoľvek budúca komunikácia medzi Poskytovateľom a Objednávateľom sa uskutočňuje použitím priradeného identifikačného čísla požiadavky/Problému. Všetky záznamy, prílohy a komunikácia Oprávnených osôb Poskytovateľa a Objednávateľa sú evidované najmä v Helpdesku dostupnom on-line.

1. Špecialista Poskytovateľa preverí požiadavku/Problém a začne ich prešetrenie. Podľa potreby kontaktuje Oprávnenú osobu Objednávateľa. Komunikácia pracovníka Poskytovateľa prebieha priamo s Oprávnenou osobou Objednávateľa. Špecialista Poskytovateľa oznámi výsledok prešetrenia a odporúčané riešenie Oprávnenej osobe Objednávateľa. Na základe výsledkov prešetrenia bude pokračovať riešenie Problému.
2. Problém bude riešený na základe priority určenej dohodou a definíciou kategórie požiadavky/Problému Oprávnenými osobami Objednávateľa a Poskytovateľa. Oprávnená osoba Objednávateľa má právo zmeniť poradie priorít riešenia otvorených Problémov/požiadaviek po dohode s oprávneným zástupcom zo strany Poskytovateľa dokumentovateľným spôsobom – záznamom v Helpdesku.
3. Oprávnená osoba Objednávateľa po vykonaní služieb pracovníkom Poskytovateľa v priestoroch Objednávateľa alebo na diaľku vzdialeným pripojením, potvrdí poskytnutie služby a funkčnosť riešenia v Helpdesku.
4. Všetky vyriešené požiadavky /Problémy Objednávateľa musia byť potvrdené a ich vyriešenie musí byť zaevidované v Helpdesku. Splnenie požiadavky/Problému bude potvrdené v rozsahu ich riešenia Oprávnenou osobou Objednávateľa. Objednávateľ je povinný potvrdiť vyriešenie každej požiadavky/Problému najneskôr do 5 pracovných dní odo dňa jej vyriešenia. Akceptovanie riešenia požiadavky/Problému bude zaevidované priamo v Helpdesku. V prípade, ak Objednávateľ riešenie požiadavky/Problému neakceptuje, v rovnakej lehote svoje pripomienky a výhrady uvedie v Helpdesku. Ak Objednávateľ bez závažného dôvodu neakceptuje vyriešenie požiadavky/Problému a ani nevznesie pripomienky k riešeniu požiadavky/Problému ani do 5 pracovných dní od ich vykonania, považuje sa riešenie požiadavky/Problému za akceptované a Helpdesk automaticky vykoná mailovú notifikáciu.

Reakčná doba Poskytovateľa na problém Objednávateľa sa určuje na základe príslušnej úrovne spracovania Problémov. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do Helpdesku alebo v prípade nedostupnosti Helpdesku od momentu nahlásenia Problému alternatívnym spôsobom, t. j. od momentu doručenia hlásenia Problému emailom.

* 1. **Služby podpory prevádzky a údržby dodaného komplexného nástroja softvéru**

|  |  |  |
| --- | --- | --- |
| **Popis** | **Parameter** | **Poznámka** |
| Prevádzkové hodiny | 9 hodín | 08:00 – 17:00 hod, počas pracovných dní |

### 

* + 1. **Mimoriadna pohotovosť**

V prípade potreby, na základe žiadosti Objednávateľa, Poskytovateľ zabezpečí mimoriadnu pohotovosť a mimoriadne výkony nespadajúce do bežnej pracovnej doby. Objednávateľ je povinný takéto mimoriadne akcie nahlásiť Poskytovateľovi v predstihu minimálne desať (10) pracovných dní vopred.

|  |  |
| --- | --- |
| **Popis** | **Poznámka** |
| Pohotovosť – nočná | Od 17:00 – 8:00 hod počas pracovných dní |
| Pohotovosť – 24 hod. | 00:00 – 24:00 hod počas pracovných dní |
| 00:00 – 24:00 hod počas pracovných dní počas sviatkov a dní pracovného pokoja |

* + 1. **Úroveň spracovania požiadaviek/Problémov**

Prevádzkové hodiny Poskytovateľa pre Služby podpory prevádzky a údržby ,Služby podpory aplikačného programového vybavenia a systémového softvéru sú počas pracovných dní od 08:00 do 17:00 hod.

Čas mimo prevádzkové hodiny Poskytovateľa podľa predchádzajúcej vety sa do Reakčnej doby nezapočítava.

Reakčná doba Poskytovateľa na Problém sa určuje na základe príslušnej úrovne Problému. Poskytovateľ poskytuje Služby podpory prevádzky a Služby podpory aplikačného programového vybavenia a systémového softvéru podľa tabuľky uvedenej nižšie. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do Helpdesku.

|  |  |
| --- | --- |
| **Typ požiadavky** | **Reakčná doba v prevádzkových hodinách** |
| Kategória A - Kritický problém  Kritické poruchy alebo vady spôsobujúce nefunkčnosť komplexného nástroja | do 8 hod. |
| Kategória B - Nekritický problém | do 24 hod. |
| Kategória C – Modifikácia komplexného nástoja, iné požiadavky | do 48 hod. |

* + 1. **Akceptačné konanie**

Poskytovateľ sa zaväzuje poskytovať Služby podpory prevádzky a údržby, Služby podpory aplikačného programového vybavenia a systémového softvéru sústavne počas trvania Servisnej zmluvy, pričom akceptácia tohto plnenia je vykonaná na mesačnej báze na konci daného mesiaca.

Fakturácia je vykonávaná mesačne, pričom prílohou faktúry je report (výkaz):

* vykonaných Službách podpory prevádzky a údržby obsahujúci štatistiku (prehľad) a parametre poskytnutých služieb,
* o vykonaných Službách podpory aplikačného programového vybavenia a systémového softvéru evidovaných v Helpdesku uzatvorených v danom mesiaci.
* **Špecifikácia požiadaviek a vlastností komplexného nástroja**
  + Funkčné požiadavky systému pre EPPERP:

|  |  |  |  |
| --- | --- | --- | --- |
| Číslo. | Management Console | Manažment | **Konkrétne a zrozumiteľne popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu**. |
| 1 | The proposed solution should support either saas based platform or on-premises deployment  (Solution should have management infrastructure, operational monitoring, upgrades, reporting, notifications & 24x7 support.) | Navrhované riešenie musí podporovať platformu založenú na službe SaaS (Software as a Service) alebo lokálne nasadenie (on-premises). (Riešenie musí mať riadiacu infraštruktúru, operačný monitoring, aktualizácie, správy, oznámenia a podporu 24x7.) |  |
| 2 |  | Navrhované riešenie musí poskytovať všetky funkcie, nástroje a strojové informácie v rámci jednej konzoly. |  |
| 3 | The proposed solution should provide a web-based console and should allow administrators to access the management interface from any machine, without installing additional software Unified Web-based console for all functionalities | Navrhované riešenie musí poskytovať webovú konzolu a umožňovať administrátorom prístup k riadiacemu rozhraniu z akéhokoľvek počítača, bez potreby inštalácie dodatočného softvéru. Jednotná webová konzola pre všetky funkcie. |  |
| 4 | The proposed solution should support multi-site configuration and multi-tenancy without any additional cost. | Navrhované riešenie musí podporovať konfiguráciu viacerých lokalít a multi-tenancy bez dodatočných nákladov. |  |
| 5 | The proposed solution should have Policy inheritance from Top to bottom (like parent/child, group/sub-group, site/group, etc) with the ability to inheritance if needed and should also provide the flexibility to have individual policies for every group. | Navrhované riešenie musí umožňovať dedičnosť politík z hora na dol (nadradený/podradený, skupina/podskupina, lokalita/skupina atď.) s možnosťou dedičnosti, ak je to potrebné, a malo by tiež ponúkať flexibilitu, aby bolo možné mať individuálne politiky pre každú skupinu. |  |
| 6 | The proposed solution should have Integrated KB/documentation into the management console without requiring logging in to another system / URL. | Navrhované riešenie musí mať integrovanú znalostnú bázu/dokumentáciu do riadiacej konzoly bez potreby prihlásenia sa do iného systému/URL. |  |
| 7 | The proposed solution console should be easy to understand and navigate with simple work flows. The console's focus should be on incident response workflows vs feature configuration and management | Navrhovaná konzola musí byť jednoducho pochopiteľná a ľahko sa ňou navigovať s jednoduchými pracovnými postupmi. Konzola by sa mala sústrediť na pracovné postupy reakcie na incidenty a nie na konfiguráciu a riadenie funkcií. |  |
| 8 | The proposed solution should have support role based access control (RBAC) | Navrhované riešenie musí mať podporu pre riadenie prístupu na základe rolí (RBAC). |  |
| 9 | The proposed solution should support two factor or single sign on solutions for the management console and sensitive functions such as remote shell. | Navrhované riešenie musí podporovať dvojfaktorovú autentifikáciu alebo jednorazové prihlásenie pre riadiacu konzolu a citlivé funkcie, ako je vzdialený prístup cez shell. |  |
| 10 | The proposed solution should have capability of centralized auditing and logging of activity should be maintained in the management console. | Navrhované riešenie musí mať schopnosť centralizovaného auditovania a udržiavať záznamy o aktivitách v riadiacej konzole. |  |
| 11 | The proposed solution should have capability logged and audited the management activity ,with the ability to send logs to an external source (like SIEM etc.) | Navrhované riešenie musí mať schopnosť zaznamenávať a auditovať riadiace aktivity, s možnosťou odosielania záznamov do externého zdroja (ako SIEM atď.). |  |
|  | **Operating System Support** | **Podpora operačných systémov** |  |
| 12 | The proposed solution should have support the following versions of windows  Windows Server Core 2012, 2016, 2019 & 2022 Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Windows Storage Server 2016, 2012 R2, 2012 Windows 7 SP1, 8, 8.1, 10, 11 | Navrhované riešenie musí podporovať nasledujúce verzie systému Windows:  Windows Server Core 2012, 2016, 2019 a 2022  Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1  Windows Storage Server 2016, 2012 R2, 2012  Windows 7 SP1, 8, 8.1, 10, 11 |  |
| 13 | The proposed solution should have support the following virtual environments  Citrix XenApp Citrix XenDesktop Microsoft Hyper-V  Oracle VirtualBox VMware Fusion VMware Horizon VMware vSphere VMware Workstation | Navrhované riešenie musí podporovať nasledujúce virtuálne prostredia:  Citrix XenApp  Citrix XenDesktop  Microsoft Hyper-V  Oracle VirtualBox  VMware Fusion  VMware Horizon  VMware vSphere  VMware Workstation |  |
| 14 | The proposed solution should have support the following macOS  macOS Catalina macOS Big Sur macOS Monterey macOS Ventura | Navrhované riešenie musí podporovať prinajmenším nasledujúce verzie systému macOS:  macOS Monterey  macOS Ventura macOS Sonoma |  |
| 15 | The proposed solution should have support the following the following (add if any other Linux platforms are supported) Amazon CentOS Debian Fedora Oracle Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server Ubuntu Virtuozzo | Navrhované riešenie musí podporovať nasledujúce platformy Linux:  Amazon  CentOS  Debian  Fedora  Oracle  Red Hat Enterprise Linux (RHEL)  SUSE Linux Enterprise Server  Ubuntu  Virtuozzo |  |
| 16 | The proposed solution should support native cloud deployments, AWS, Azure, Google Cloud etc. | Navrhované riešenie musí podporovať nasadzovanie v native cloud prostrediach, ako sú AWS, Azure, Google Cloud atď. |  |
| 17 | The proposed solution should support cloud workloads protection ( Azure, AWS and Google Cloud). | Navrhované riešenie musí podporovať ochranu cloudových pracovných workloadov (Azure, AWS a Google Cloud). |  |
| 18 | The proposed solution vendor must provide support for the latest major OS Updates/Versions within 60 days of release. | Poskytovateľ navrhovaného riešenia musí zabezpečiť podporu pre najnovšie hlavné aktualizácie/verzie operačných systémov do 60 dní od ich uvedenia na trh. |  |
|  | **Agent** | **Agent** |  |
| 19 | The proposed solution must have EPP and EDR capabilities available in a single agent without requiring multiple software packages to be installed. | Navrhované riešenie musí mať funkcie EPP (Endpoint Protection Platform) a EDR (Endpoint Detection and Response) dostupné v jednom agentovi bez potreby inštalovať viacero softvérových balíkov. |  |
| 20 | The proposed solution agent size should be less then 100 MB. | Veľkosť inštalačného balíka agenta navrhovaného riešenia musi byť menšia ako 100 MB. |  |
| 21 | The proposed solution must have strong anti-tamper capabilities (Ensure that an end user (even with local admin credentials) can not remove, disable or modify the product in any way.) | Navrhované riešenie musí mať silné schopnosti proti zasahovaniu (zabezpečiť, že koncový používateľ (aj s miestnymi správcovskými oprávneniami) nemôže produkt odstrániť, zakázať alebo akýmkoľvek spôsobom upravovať). |  |
| 22 | The proposed solution must have ability to kick off On-Demand Scans to look for malware, or ensure a threat has been remediated (from console and/or endpoint) | Navrhované riešenie musí mať schopnosť spustiť skenery na požiadanie na vyhľadávanie malvéru alebo na zabezpečenie, že hrozba bola odstránená (z konzoly a/alebo koncového bodu). |  |
| 23 | The proposed solution should be signtureless (No need of daily signature updates) to detect all types of Malware without compromising the security posture. | Navrhované riešenie by malo byť bez signatúr (bez potreby denných aktualizácií signatúr) pre detekciu všetkých typov malvérov bez ohrozenia bezpečnostnej pozície. |  |
| 24 | The proposed solution must have ability to schedule agent upgrades from the management console | Navrhované riešenie musí mať schopnosť plánovať aktualizácie agenta z riadiacej konzoly. |  |
| 25 | The proposed solution must have ability to limit the amount of agents that can download an update at any given point of time. | Navrhované riešenie musí mať schopnosť obmedziť množstvo agentov, ktoré môžu sťahovať aktualizácie v akomkoľvek danom čase. |  |
| 26 | The proposed solution must have Ability to upgrade agents with no impact to the end user | Navrhované riešenie musí mať schopnosť aktualizovať agentov bez vplyvu na koncového používateľa. |  |
| 27 | The proposed solution should not stop functioning if license count is exceeded. | Navrhované riešenie nesmie prerušiť svoju činnosť v prípade prekročenia počtu licencií. |  |
| 28 | The proposed solution should automatically remove old agents from console, if agent haven't communicated to the management console for a configurable period of time | Navrhované riešenie musí automaticky odstraňovať starých agentov z konzoly, ak sa agent neprihlásil do riadiacej konzoly po konfigurovateľnom období. |  |
| 29 | The proposed solution should have minimal impact on system performance. | Navrhované riešenie by malo mať minimálny vplyv na výkonnosť systému |  |
| 30 | The proposed solution should must have capability to uninstalled agents remotely from the management console directly or through script. | Navrhované riešenie musí mať schopnosť odinštalovať agentov vzdialene z konzoly priamo alebo cez skript. |  |
| 31 | The proposed solution should capability to temporarily disabled via the management console for temporary troubleshooting or testing. | Navrhované riešenie musí mať schopnosť dočasne zakázať agenta cez riadiacu konzolu na dočasné ladenie alebo testovanie. |  |
| 32 | The proposed solution agents should have ability to communicate with Management Console via a proxy | Agenti navrhovaného riešenia musia mať schopnosť komunikovať s riadiacou konzolou cez proxy. |  |
| 33 | The proposed solution must support linux agent running solely in user space to avoid kernel panics and tainted kernels that invalidate support | Navrhované riešenie musí podporovať linuxových agentov, ktorí bežia výhradne v užívateľskom priestore, aby sa zabránilo nestabilite a problémom s verziami kernelu. |  |
| 34 | The proposed solution should not required any downtime while installing/upgrading Linux agents | Navrhované riešenie nesmie vyžadovať žiadny výpadok počas inštalácie/aktualizácie linuxových agentov. |  |
| 35 | The proposed solution should provide ability to send notification messages to the end user computer. | Navrhované riešenie musí poskytovať možnosť posielať oznámenia používateľom počítača. |  |
|  | **Threat Prevention** | **Threat Prevention** |  |
| 36 | The proposed solution should provide prevention capability across all major Operating Systems – Windows, MacOS & Linux. | Navrhované riešenie musí poskytovať schopnosť prevencie na všetkých hlavných operačných systémoch - Windows, MacOS a Linux. |  |
| 37 | The proposed solution must provide protection against known and unknown malware | Navrhované riešenie musí poskytovať ochranu pred známym a neznámym malvérom. |  |
| 38 | The proposed solution must have capability to checked the files for any infection for both on write and execute. | Navrhované riešenie musí mať schopnosť kontroly súborov na prítomnosť infekcie pri zápise aj pri vykonávaní. |  |
| 39 | The proposed solution must be effective against Zero-Day Attacks by Analysing Behaviours on an endpoint, rather than only looking at daily signatures | Navrhované riešenie musí byť efektívne proti útokom typu Zero-Day tým, že analyzuje správanie na koncovom bode, namiesto toho, aby sa iba pozeralo na denné signatúry. |  |
| 40 | The proposed solution must protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need to have any dependency on Management Server or Cloud or ANY resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less , Memory based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected. | Navrhované riešenie musí chrániť koncový bod pred malvérom aj v prípade, keď nie je pripojený k sieti. Agent musí byť plne autonómny, čo znamená, že nepotrebuje žiadnu závislosť na riadiacom serveri, cloude ani žiadnych externých prostriedkoch na detekciu a adekvátnu reakciu na sofistikované hrozby (Zero Day, bezsúborové, založené na pamäti, Zero Day útoky, vydieračský softvér, ťažiari, laterálne pohyby, APT) v reálnom čase pri ich detekcii. |  |
| 41 | The proposed solution should have capacity to detect dormant threats | Navrhované riešenie musí mať kapacitu na detekciu neaktívnych hrozieb. |  |
| 42 | The proposed solution should leverage Artificial Intelligence or Machine Learning to analyse files pre-execution & behaviours while a file is running | Navrhované riešenie musí využívať umelú inteligenciu alebo strojové učenie na analýzu súborov pred ich vykonaním a na správanie súborov počas ich behu. |  |
| 43 | The proposed solution should protect from malicious scripts and documents | Navrhované riešenie musí chrániť pred škodlivými skriptami a dokumentami. |  |
| 44 | The proposed solution should monitor and protect from lateral movement | Navrhované riešenie musí monitorovať a chrániť pred laterálnym pohybom. |  |
| 45 | The proposed solution should monitor and protect from exploits and fileless attacks | Navrhované riešenie musí monitorovať a chrániť pred útokmi a bezsúborovými útokmi (fileless attacks). |  |
| 46 | The proposed solution should look for potentially unwanted programs | Navrhované riešenie musí vyhľadávať potenciálne nežiaduce programy. |  |
| 47 | The proposed solution should monitor and protect from insider threats | Navrhované riešenie musí monitorovať a chrániť pred hrozbami od vnútorných útočníkov. |  |
| 48 | The proposed solution should provide the flexibility to safely download of malicious or convicted file from the management console | Navrhované riešenie musí poskytovať flexibilitu pre bezpečné stiahnutie škodlivého súboru alebo súboru označeného ako hrozba z manažment konzoly. |  |
| 49 | The proposed solution must have ability to store the malicious/alert data for at least 365 days without any additional charge | Navrhované riešenie musí mať schopnosť uchovávať dáta o zistených malvéroch a upozorneniach aspoň 365 dní bez ďalších poplatkov. |  |
| 50 | The proposed solution must have ability to correlate together automatically if incident elated to the same attack and not create separate alerts. | Navrhované riešenie musí mať schopnosť automaticky korelovať incidenty, ak súvisia s tým istým útokom, a nemá vytvárať samostatné upozornenia. |  |
| 51 | The proposed solution must have ability to store raw data / telemetry s for a minimum of 180 days | Navrhované riešenie musí mať schopnosť uchovávať surové dáta / telemetriu aspoň 180 dní. |  |
|  | **EDR/Forensic Functionality** | **EDR/Forenzná funkcionalita** |  |
| 52 | The proposed solution must have ability to store EDR data centrally for hunting and forensic purposes . | Navrhované riešenie musí mať schopnosť uchovávať EDR dáta centrálne na účely vyhľadávania a forenzného vyšetrovania. |  |
| 53 | The proposed solution must provide EDR telemetry data for Windows, Mac & Linux | Navrhované riešenie musí poskytovať EDR telemetrické dáta pre systémy Windows, Mac a Linux. |  |
| 54 | The proposed solution should provide the flexibility for the data should be searched even if the originating system is offline or has been removed from console. | Navrhované riešenie musí poskytovať flexibilitu pre vyhľadávanie dát, aj keď pôvodný systém je offline alebo bol odstránený z konzoly. |  |
| 55 | The proposed solution should support threat hunting workflows. | Navrhované riešenie musí podporovať pracovné postupy hľadania hrozieb. |  |
| 56 | The proposed solution must have Threat hunting queries configurability as custom rules to automatically trigger detections. | Navrhované riešenie musí mať možnosť konfigurovateľných hľadacích dotazov pre hľadanie hrozieb a automatické spúšťanie detekcií ako vlastné pravidlá. Navrhované riešenie musí mať možnosť vytvárania vlastných pravidiel pomocou dotazov, ktoré budú automaticky detegovať hrozby. |  |
| 57 | The proposed solution should by default group all related alerts together | Navrhované riešenie musí predvolene zoskupovať všetky súvisiace upozornenia dohromady. |  |
| 58 | The proposed solution should provide a visual process tree browser | Navrhované riešenie musí poskytovať vizuálny prehliadač stromu procesov. |  |
| 59 | The proposed solution should provide the flexibility to mark an entire group of events as a threat and take response or remediation actions accordingly | Navrhované riešenie musí umožniť označiť celú skupinu udalostí ako hrozbu a podniknúť následné kroky na odstránenie alebo riešenie. |  |
| 60 | The proposed solution should provide the option to mark discovered items as suspicious or threats during threat hunting. | Navrhované riešenie musí ponúkať možnosť označiť objavené položky ako podozrivé alebo hrozby počas vyhľadávania hrozieb. |  |
| 61 | The proposed solution should have option to search for MITRE ATT&CK Indicator for instances of Initial Access, Execution, Persistence, etc. in a single search string | Navrhované riešenie musí mať možnosť vyhľadávať MITRE ATT&CK Indikátory pre prípady Initial Access, Execution, Persistence atď. v jednom vyhľadávacom reťazci. |  |
| 62 | The proposed solution should have option to search for MITRE ATT&CK Indicators based onInitial AccessCredential AccessDiscoveryLateral MovementCollectionCommand & ControlExfiltrationImpactIndicators | Navrhované riešenie musí mať možnosť vyhľadávania MITRE ATT&CK Indikátorov na základe: Initial Access Credential Access Discovery Lateral Movement Collection Command & Control Exfiltration Impact Indicators |  |
| 63 | The proposed solution should have search capabilities for the following (add if any more search capabilities available):  Hostnames Operating System File name Date creation Date modified Hash (MD5,SHA1,SHA256) Registry Information File path URL IP address Port traffic and or Traffic source | Navrhované riešenie musí mať schopnosť vyhľadávania pre nasledujúce:  Hostname (názov hostiteľa)  Operačný systém  Názov súboru  Dátum vytvorenia  Dátum úpravy  Hash (MD5, SHA1, SHA256)  Informácie o registri  Cesta k súboru  URL (internetová adresa)  IP adresa  Port prenosu a/zdroj prenosu |  |
|  | **Response & Remediation Capabilities** | **Reakcia a funkcie remediácie** |  |
| 64 | Solution should support a full remote shell for all OS (Windows, Linux & Mac) and not limit or restrict to set of commands. | Riešenie musí podporovať plný remote shell pre všetky operačné systémy (Windows, Linux a Mac) a nesmie obmedzovať alebo zakazovať dostupné príkazy |  |
| 65 | The proposed solution should track all remote shell commands and logged during a remote shell session | Navrhované riešenie musí sledovať všetky príkazy remote shellu a zaznamenávať ich počas relácie. |  |
| 66 | The proposed solution should alert on both suspicious and malicious threat behaviour | Navrhované riešenie musí vydávať upozornenia na podozrivé aj malvérové správanie. |  |
| 67 | The proposed solution should have ability to kill and quarantine an offending process | Navrhované riešenie musí mať schopnosť ukončiť a izolovať proces, ktorý predstavuje hrozbu. |  |
| 68 | The proposed solution should able to unquarantine a file from the management interface or API | Navrhované riešenie musí byť schopné zrušiť izoláciu súboru z rozhrania riadenia alebo cez API. |  |
| 69 | The proposed solution should have ability to remediate all operating system changes and perform corrective action in machine speed. Tool should also be able to undo any system level changes related to the attack such as Registry edits, configuration changes etc. | Navrhované riešenie musí mať schopnosť odstrániť všetky zmeny v operačnom systéme a vykonávať korekčné opatrenia v rýchlosti stroja. Nástroj musí byť schopný vrátiť všetky úpravy na úrovni systému týkajúce sa útoku, ako sú úpravy registra, zmeny konfigurácie atď. |  |
| 70 | The proposed solution should reverse destructive data event including but not limited to ransomware,The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state | Navrhované riešenie musí byť schopné obnoviť znehodnotené dáta vrátane, ale nie obmedzené na, ransomware. Nástroj musí tiež byť schopný obnoviť súbory, ktoré boli vymazané alebo zašifrované ako súčasť útoku, a obnoviť súbory do ich stavu pred útokom. |  |
| 71 | The proposed solution should provide option to network quarantine a device and provide flexibility to configure the same. | Navrhované riešenie musí poskytovať možnosť izolovať zariadenie v sieti a umožniť prispôsobiť konfiguráciu tejto izolácie. |  |
| 72 | The proposed solution should have automated threat response capabilities. | Navrhované riešenie musí mať automatizované schopnosti na reakciu na hrozby. |  |
| 73 | The proposed solution should have capability to take the remediation actions on multiple systems or events at once | Navrhované riešenie musí mať schopnosť vykonávať remediačné kroky na viacerých systémoch alebo udalostiach naraz. |  |
| 74 | The proposed solution should have ability for an analyst to add notes/comments to an event | Navrhované riešenie musí umožňovať analytikovi pridávať poznámky/komentáre k udalosti. |  |
| 75 | The proposed solution should have options to set the status of an issue or event (i.e. resolved, in progress, unresolved) | Navrhované riešenie musí mať možnosť nastaviť stav problému alebo udalosti (napr. vyriešené, v riešení, neriešené) |  |
|  | **Policy & Installation** | **Politiky a inštalácia** |  |
| 76 | The proposed solution should provide ability to support policy inheritance across the endpoints. | Navrhované riešenie by malo poskytovať možnosť podpory dedenia politík na koncových bodoch. |  |
| 77 | The proposed solution should have the option to provide dynamic policy assignment based on device attributes | Navrhované riešenie musí mať možnosť poskytovať dynamické priradenie politík na základe vlastností zariadenia. |  |
| 78 | The proposed solution should cappabilty to placed the installed devices directly into a specific device group at time of installation | Navrhované riešenie musí byť schopné umiestňovať inštalované zariadenia priamo do špecifických skupín zariadení v čase inštalácie. |  |
| 79 | The proposed solution policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines). | Politiky navrhovaného riešenia musia poskytovať možnosť zapnúť alebo vypnúť jedinečné moduly alebo typy modulov (moduly pred spustením a moduly počas behu). |  |
| 80 | The proposed solution policy modifications should be applied in near real time | Zmeny politík navrhovaného riešenia musia byť aplikované v takmer reálnom čase. |  |
|  | **Exclusions** | **Výnimky** |  |
| 81 | The proposed solution should have predefined list of known or recommended exclusions | Navrhované riešenie musí mať preddefinovaný zoznam známych alebo odporúčaných výnimiek. |  |
| 82 | The proposed solution should include workflows to easily exclude false positives | Navrhované riešenie musí zahŕňať pracovné postupy na jednoduché vylúčenie falošných pozitívnych výsledkov. |  |
| 83 | The proposed solution should provide the option for the administrators to make policy exclusions of the console at multiple levels. | Navrhované riešenie musí poskytovať možnosť administrátorom vylúčiť politiky z konzoly na viacerých úrovniach. |  |
| 84 | The proposed solution have capability to exclusions configured by the administrator to handle performance issues down to specific paths or single executables by reducing or disabling monitoring of parent processes and/or parent processes and all of their spawned child processes | Navrhované riešenie musí mať možnosť konfigurácie výnimiek správcom na riešenie problémov s výkonom, nastavením konkrétnej cesty alebo spustiteľného súboru s obmedzením alebo zakázaním monitorovania týchto procesov alebo týchto procesov a všetkých ich podradených procesov. |  |
|  | **Device Control, Network Control and Application Visibility ,Discovery** | **Device Control, Network Control and Application Visibility ,Discovery** |  |
| 85 | The proposed solution device Control capabilities should be available on Windows | Navrhované riešenie musí mať schopnosť kontroly zariadení dostupnú na systémoch Windows. |  |
| 86 | The proposed solution device Control should support block, read only and allow read-write on USB /Bluetooth. | Kontrola zariadenia v navrhovanom riešení musí podporovať blokovanie, read only a read-write prístup na USB/Bluetooth |  |
| 87 | The proposed solution should have granular device control capability which can be applied to a Class, Serial Number Product ID or Type of Device. | Navrhované riešenie musí mať detailnú schopnosť kontroly zariadení, ktorá sa môže aplikovať na triedu, sériové číslo, identifikátor produktu alebo typ zariadenia. |  |
| 88 | The proposed solution should have provide Firewall Control for Windows / Linux. | Navrhované riešenie musí mať kontrolu firewallu pre systémy Windows/Linux. |  |
| 89 | The proposed solution should have Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups) | Pravidlá firewallu musia byť v navrhovanom riešení vytvorené tak, aby sa uplatňovali na konkrétnu skupinu zariadení (s využitím označovania alebo skupín politík). |  |
| 90 | The proposed solution should have location aware firewall rules to apply different policies when on or off network | Navrhované riešenie musí mať pravidlá firewallu citlivé na umiestnenie, aby sa mohli aplikovať rôzne politiky pri pripojení a odpojení od siete. |  |
| 91 | The proposed solution must identify rogue devices discovery capability to reduce the potential attack surface. | Navrhované riešenie musí mať schopnosť identifikovať neautorizované zariadenia na redukciu bodov, ktoré by mohli byť využité na potentionálny útok. |  |
| 92 | The proposed solution must provide a software/application inventory for the environment | Navrhované riešenie musí poskytovať inventár softvéru/aplikácií pre prostredie. |  |
| 93 |  | Navrhované riešenie musí umožňovat inštaláciu agentov metódou Peer-to-Peer |  |
|  | Dashboards & Reporting | Dashboards & Reporting |  |
| 94 | The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option | Navrhované riešenie musí hlásiť všetky známe zraniteľnosti v programoch nainštalovaných na koncovom bode, spolu s možnosťou exportu dát. |  |
| 95 | The proposed solution have option to export data into 3rd party reporting tools such as Tableau or PowerBI | Navrhované riešenie musí mať možnosť exportovať dáta do nástrojov na správu dát tretích strán, ako sú Tableau alebo PowerBI. |  |
| 96 | The proposed solution must have customizable dashboards as per user | Navrhované riešenie musí mať možnosť prispôsobiteľných informačných panelov podľa požiadaviek používateľa. |  |
|  | Compliance | Compliance |  |
| 97 |  | Výrobca navrhovaného riešenia musí byť zaradený podľa nezávislého a medzinárodne uznávaného hodnotenia jednotlivých bezpečnostných produktov spoločností Gartner, Inc., Magic Quadrant for Endpoint Protection Platforms do kategórie „Leaders“, minimálne posledné dva roky. |  |
| 98 | The proposed solution must be fulfilling following compliances such as HIPAA compliant ,PCI compliant,GDPR compliant,ISO27001 compliant | Navrhované riešenie musí spĺňať súladové požiadavky, ako sú súlad s HIPAA, súlad s PCI, súlad s GDPR. SaaS platforma výrobcu musí byť certifikovaná podľa SOC 2 Type II. |  |
|  | Integrations | Integrácia |  |
| 99 | The proposed solution should support integration with Active Directory | Navrhované riešenie musí podporovať integráciu s Active Directory. |  |
| 100 | The proposed solution should have integrations to Virus Total or similar tools | Navrhované riešenie musí mať integrácie s nástrojmi ako Virus Total alebo podobnými. |  |
| 101 | The proposed solution should have native integrations/integrations with SIEM solutions such as Splunk, Qradar & etc. | Navrhované riešenie musí mať natívne integrácie alebo integrácie so SIEM riešeniami ako Splunk, Rapid 7, Qradar a podobnými. |  |
| 102 | The proposed solution should have option to send event logs via Syslog. | Navrhované riešenie musí mať možnosť odoslať udalostné protokoly cez protokol Syslog. |  |
|  |  | Bezpečnost Active Directory |  |
| 103 |  | Riešenie musí vykonávať testy na detekciu zraniteľností Active Directory spojených s autentifikáciou, autorizáciou, nastavením účtu, certifikačnými službami, oprávneniami/delegáciami a bezpečnostnými problémami priamo súvisiacimi so zabezpečením Domain Controller(ov) a Azure AD. |  |
| 104 |  | Riešenie musí kategorizovať testy do najmenej štyroch závažností od najkritickejších po najnižšiu |  |
| 105 |  | Riešenie musí byť schopné príjmať oznámenia z on-premise AD (provozné udalosti) v reálnom čase. |  |
| 106 |  | Riešenie nesmie vyžadovať plné administrátorské oprávnenia na Active Directory alebo Domain Controlleroch. |  |
| 107 |  | Riešenie musí obsahovať bezpečnostné hodnotenia pre on-premise a Azure AD. |  |
| 108 |  | Riešenie musí mať možnosť nasadenia on-premise. |  |
| 109 |  | Overenia on-prem AD musia byť vykonávané jediným zariadením pripojeným k doméne. |  |
| 110 |  | Riešenie nesmie vyžadovať VPN pripojenie medzi on-prem komponentmi a cloudovou konzolou. |  |
| 111 |  | Riešenie musí byť schopné automaticky objaviť viaceré domény a zahrnúť ich do rozsahu testov a ochrany. |  |
| 112 |  | Riešenie musí byť schopné vykonávať overenia Azure-AD prostredníctvom API poskytovaného spoločnosťou Microsoft. |  |
| 113 | ● The solution must be able to detect attacks against the AD, including: o ‘Low and slow’ brute force attempts like ‘Password Spray’ o Mass account lockouts o Mass Password changes o Mass account disabling/deletion o Suspicious password changes for sensitive accounts o Reactivation of disabled privileged accounts o DCSync attacks o Rouge Domain Controller attacks (DCShadow) o Use of the default “Administrator” account o Suspicious service creation on Domain Controller(s) | Riešenie musí byť schopné detegovať útoky voči Active Directory, vrátane:   Low and slow pokusy o hrubú silu, ako je Password Spray,  Hromadné uzamknutie účtov,  Hromadná zmena hesiel,  Hromadné vypnutie/zmazanie účtov,  Podozrivé zmeny hesiel pre citlivé účty,  Znovuaktivácia deaktivovaných privilegovaných účtov,  Útoky DCSync,  Útoky na rouge Domain Controller (DCShadow),  Použitie default účtu Administrator,  Podozrivé vytváranie služieb na Domain Controller(och). |  |
| 114 | ● Threat detection must not rely on scheduled AD replication to minimize impact on the AD. | Detekcia hrozieb nesmie spočívať v plánovanom replikovaní AD, aby sa minimalizovalo zaťaženie na AD |  |
| 115 |  | Riešenie musí umožnovať externé spracovanie detekcie hrozieb do riešení SIEM, SOAR a XDR |  |
| 116 |  | Riešenie musí poskytovať podrobné usmernenia na odstránenie zistených zraniteľností, vrátane  Odkazy na taktiky a techniky MITRE Att&ack,  Kroky na prípravu remediacie,  Kroky na vykonanie remediacie,  Odkazy na doplnkové informácie od širšej komunity pre zabezpečenie AD. |  |
| 117 |  | Riešenie musí byť schopné generovať skripty na remediaciu, ktoré možno vykonať v príslušných doménach s nasledujúcimi schopnosťami:  Podrobný výber zraniteľností na odstránenie,  Podrobný výber objektov, na ktorých sa bude remediacia vykonávať,  História remediacie o stave procesu remediacie (vygenerovaný skript, stiahnutý, vykonaný s výsledkom úspechu alebo zlyhania),  Skripty na vrátenie zmien pri bývalej remediacii na základe skriptu. |  |
| 118 |  | Riešenie musí byť schopné automaticky spúšťať celý testovací cyklus v konfigurovateľnom rozvrhu používateľa (napr. každých X dní), pridať výsledky do svojej databázy a generovať podrobné testovacie správy bez ďalšieho zásahu používateľa. |  |
| 119 |  | Riešenie musí podporovať ad-hoc spustenia celého testovacieho cyklu a prezentovať výsledky v GUI a v podrobných správach. |  |
| 120 |  | Riešenie musí podporovať spustenie individuálnych testov ad-hoc, bez potreby spúšťať celý testovací cyklus. |  |
| 121 |  | Systém musí podporovať vytváranie a dokumentovanie výnimiek pre budúce testovacie behy na nasledujúcich úrovniach: Domény, Jednotlivé testy pre doménu, Jednotlivé objekty (užívateľ alebo skupina) pre test a doménu. |  |
| 122 |  | Riešenie musí podporovať vytváranie týchto výnimiek na centrálnej lokalite v GUI alebo priamo z príslušných testov/výsledkov s možnosťou pridávania komentárov k tomu, prečo boli tieto výnimky vytvorené. |  |
| 123 |  | Riešenie musí obsahovať informačný panel, ktorý poskytuje rýchle informácie o výsledkoch testov, ako sú:  Počet testov podľa závažnosti a ich výsledky (úspech/zlyhanie/skipované) celkom a pre testované domény,  Zistená topológia domény a vzťahy medzi doménami,  Skóre zdravia a priradená úroveň rizika celkovo a individuálne pre jednotlivé domény,  Najkritickejšie/závažné zistenia a počet ovplyvnených objektov,  Grafická reprezentácia zlyhaných testov v posledných behoch, ktorá umožňuje používateľovi rýchlo vidieť zmeny v zabezpečení v čase. |  |
| 124 | ● The solution must provide extensive filtering capabilities of test results including at least: o Previous tests o Severity o Domain name o Forest name o Detection name o Acknowledgement status o Vulnerability status o Computer(s) affected o Group(s) affected o User(s) affected | Riešenie musí poskytovať rozsiahle možnosti filtrovania výsledkov testov, vrátane aspoň:  Predchádzajúce testy,  Závažnosť,  Názov domény,  Názov forest,  Názov zistenia,  Stav potvrdenia,  Stav zraniteľnosti,  Počítač(y) ovplyvnené/postihnute,  Skupina(y) ovplyvnená/postihnuta,  Užívateľ(ia) ovplyvnení/postihnuty. |  |
| 125 |  | Riešenie musí byť schopné porovnávať výsledky testov s predchádzajúcimi . |  |
| 126 |  | Riešenie musí poskytovať minimálne nasledujúce podrobnosti o každom vykonanom teste:  Popis testu,  Odkaz na relevantné webové stránky MITRE Att&ck,  Mitigačné kroky,  Nástroje na útok, ktoré môžu využívať zistenú zraniteľnosť,  Odkazy na relevantné články od komunity pre zabezpečenie AD. |  |
| 127 |  | Riešenie musí poskytovať podrobné informácie o dôvodoch zistenia zraniteľností, vrátane:  Typy objektov, napr. Užívateľ alebo Skupina,  Názvy objektov,  Porušené nastavenia na úrovni objektu, napr. aké oprávnenia boli zistené. |  |
|  |  | Služby a podpora |  |
| 128 |  | Súčasťou riešenia musia byť dohľadové služby MDR - Managed Detection and Response, kontrola incidentov z prostredí zákazníka poskytované výrobcom riešenia. |  |
| 129 |  | Výrobca musí poskytovať aj voliteľnú možnosť priameho riešenia a uzatvárania týchto incidentov MDR týmom. |  |
| 130 |  | V rámci služby musí byť k dispozícii analýza prvotnej príčiny incidentu dostupná na vyžiadanie. |  |
| 131 |  | Služba musí byť poskytovaná v režime 24x7 |  |
| 132 |  | Súčasťou služby musí byť ročný balík konzultačných hodín, ktorý zákazník môže použiť podľa potreby na podrobné vyšetrovanie, alebo proaktívné služby spojené s bezpečnosťou. |  |