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

**STRUČNÝ OPIS PREDMETU ZÁKAZKY**

Predmet zákazky zahŕňa:

1. Dodávku, implementáciu a podporu integrovaného bezpečnostného systému monitoringu sieťovej prevádzky pre testovacie pracovisko.
2. Dodávku, implementáciu 2ks Next Generation Firewall zariadení s funkciou IPS
3. Dodávku a implementáciu systému na centralizovanú správu logov a iných strojových dát z ľubovoľných zdrojov
4. Dodávku pracovných staníc a zobrazovacích zariadení pre zamestnancov centra pre bezpečnostný monitoring, detekciu bezpečnostných incidentov a riešenie kybernetických bezpečnostných incidentov (Security Operations Centra)
5. Služby zahŕňajúce inštalačné práce, implementačné prace a školenia obslužného personálu

Termín plnenia predmetu zákazky: do 7 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 ako aj hardvér, 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**

1. **Všeobecné požiadavky na systém bezpečnostného systému monitoringu sieťovej prevádzky pre testovacie pracovisko.**

Požadujeme, aby systém vedel:

* Rozpoznávať a zabraňoval pohybu škodlivého kódu cez sieť.
* Odhaľovať iné praktiky útočníkov – napríklad pokusy o zneužitie zraniteľnosti, pokusy o vyhýbanie (lateral movements) a ex-filtráciu údajov.
* Poskytovať retrospektívne informácie o udalostiach v oblasti IKT zaznamenávaním informácií o sieťových udalostiach s možnosťou ich následného zobrazenia a analýzy.
* Umožniť vyšetrovanie incidentov.

**Kvalitatívne požiadavky na systém dohľadu a bezpečnostnej analýzy sieťovej prevádzky:**

Systém bude slúžiť ako nástroj pre bezpečnostných špecialistov, preto očakávame možnosť:

* Jednoducho a rýchlo definovať vlastné pravidlá detekcie javov, ktoré považujeme za zaujímavé a ktoré nie sú pokryté bezpečnostnou databázou (threat-intel) dodanou výrobcom technológie.
* Vytvárať a upravovať predvolené prehľady vrátane špecifikovania periodicity ich automatickej vytvárania a odoslania.
* Vytvárať ad hoc vyšetrovaní, upozornení a záznamov o sieťovej premávke

**Monitorovanie NetFlow a DPI zariadenia:**

* Pasívne zapojenie bez vplyvu na monitorovanie sieť (SPAN/mirror portami)
* Jednoduchá inštalácia do existujúcej sieťovej infraštruktúry - racková montáž 1U
* Manažment rozhranie: min. 1 x (administratívne) porty 10/100 / 1000Mb / s pre zabezpečenú vzdialenú správu a prenos NetFlow dát dohľad a konfigurácia - SSH, HTTPS.
* Správa užívateľov a prístupových práv na zariadení prostredníctvom užívateľských rolí.
* Nastaviteľná rýchlosť monitorovacej linky min. 1x (4 x 1 Gb/s) HW na metalickom fyzickom rozhraní.
* Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.
* Výkon: Min1,48 Mpp/s na 1 Gb/s monitorovací port.
* Podpora protokolov pre výmenu dát: NetFlow dáta vo formátoch verzii 5 a 9, IPFIX.
* Integrácia do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov technológií SNMP.
* Vzorkovanie: Na úrovni paketov a na úrovni tokov.
* Prevedenie: HW zariadenie.

**NetFlow kolektor:**

* Granularita vizualizácie: min. spracovanie dátových tokov / paketov a vizualizácia v 5-minútových, 1-minútových alebo 30-sekundových intervaloch.
* Podpora štandardov dátových tokov: min. NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite a ich zber z desiatok zdrojov v sieti.
* Možnosť dohľadania ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty, databázy aktívnych zariadení na sieti vr. identifikácie zariadení.
* Jednoduchá konfigurácia pomocou dostupných konfiguračných šablón, ktoré umožňujú výber z dostupných “Presets” a ich aplikáciou vytvárať profily, kapitoly, reporty, widgety a dashboardy bez nutnosti manuálnej konfigurácie.
* Prevedenie: šablóny pre nasadenie virtuálneho stroja (VmWare, KVM, Hyper-V).
* Kapacita dátového úložiska: Min 2 TB.
* Výkon kolektora min:100000 fps (dátových tokov / s).
* Manažment rozhranie: min. 1 x (administratívne) port 10/100 / 1000Mb / s pre zabezpečenú vzdialenú správu a prenos NetFlow dát.
* Zabezpečená vzdialená správa, dohľad a konfigurácia - SSH, HTTPS.
* Integrácia do pohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov technológií SNMP.
* Prijímanie a preposielanie IPFIX dát pomocou spoľahlivého TCP spojenia s možnosťou šifrovania (TCP/TLS) podľa štandardu RFC 7011.
* Kolektor poskytuje dokumentované API pre získavanie a spracovanie dát. Prostredníctvom API je možné kolektor tiež konfigurovať (napr. definovať vlastné prehľady, reporty, apod.).
* Prevedenie: virtuálne zariadenie (appliance).

**Monitorovací systém:**

* Vizualizácia štatistických dát podľa objemu (min . počet prenesených bytov, tokov, paketov), IP prevádzky (min. TCP, UDP, ICMP, ostatné) alebo protokolu (min. HTTP, IMAP, SSH), vrátane plnej konfigurácie grafov a pohľadov užívateľom.
* Podpora autentizácie voči LDAP (Active Directory).
* Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.
* Použitie DNS cache na zariadení pre rýchlejší preklad IP adries na doménové mená.
* Monitorovanie rozšírených L3 / L4 informácií: Podpora pre monitorovanie rozšírených L3 / L4 informácií - TTL (Time to live), TCP Window size, TCP SYN.
* Monitorovanie a reportovanie MAC adries vo flow štatistikách. Možnosť použiť MAC adresu ako položku kľúča flow záznamu.
* Spracovanie dátovej prevádzky min. IPv4 a IPv6, VLAN, MPLS, AS, HTTP, HTTPS (SNI) VoIP,DNS, DHCP,SMB / CIFS a emailovej prevádzky.
* Analýza oneskorenia na sieti min. RTT, SRT, delay, jitter, retransmisiu, out-of-order pakety ako súčasť flow štatistík a podpora pre analýzu CISCO AVC.
* Podpora vyplňovania AS na základe vstavaného či dodaného zoznamu.
* Monitoring aktívnych zariadení na sietí a viditeľnosť do šifrovanej komunikácie SSL/TLS.
* Monitoring využívaných externých cloudových služieb (MS Azure, AWS, GPC) s podporou end-to-end visibility dátovej komunikácie.
* Systém musí umožňovať vizualizáciu monitorovaných liniek a prepojov a sieťovej topológie.
* Generovanie štatistík a podrobných výpisov nad voliteľnými časovými intervalmi s voliteľnými filtrami. Rôzne formáty výstupov, minimálne PDF, CSV.
* Monitorovanie zariadení pripojených k dátovej sieti, dlhodobá história aktívnych zariadení, identifikácia na základe IP adresy, MAC adresy, sledovanie VLAN, operačného systému, prihláseného používateľa na danom zariadení.
* Centralizovaný dashboard s možnosťou tvorby vlastných náhľadov a widgetov, poskytuje preddefinované náhľady na používané služby na sieti (napr. sociálne siete, videokonferčné aplíkácie, antivírusové aplikácie, služby verejných cloudov, Office 365 a pod pre rýchlejšiu konfiguráciu) a umožňuje tieto dashboardy zdielať pre jednotlivé užívateľské role a rôzne oddelenia (prevádzka a bezpečnosť).

**Detekcia , odozva a automatizácia:**

* Automatické vyhodnocovanie NetFlow dát a detekcia anomálií na sieti s podporou deduplikácie, vzorkovania na úrovni tokov, identity používateľov, persistencii doménových mien.
* Architektúra systému umožňuje streamové spracovávanie flow dát pre rýchlu detekciu bezpečnostných alebo prevádzkových anomálií.
* Sada detekčných metód a algoritmov pre analýzu flow štatistík, detekciu bezpečnostných incidentov, prevádzkových problémov a sieťových anomálií pre min.1000 fps (dátových tokov / s) / min 3 rozdielnych dátových zdrojov ( subnet, sieťový segment a pod.).
* Systém umožňuje spravovať zdroje sieťových tokov, umožňuje dočasne pozastaviť príjem tokov a indikovať poruchu zdroja sieťových tokov.
* Detekčné mechanizmy: Detekcia skenovanie portov, slovníkové útoky, útoky odopretia služieb (DoS), útoky na sieťové protokoly SSH, RDP, Telnet. Detekcia anomálií v DNS, DHCP, SMTP, multicast prevádzky a neštandardnej komunikácie. Detekcia P2P sietí, VPN služieb a anonymizačných služieb (napr. TOR). Detekcia nadmernej záťaže siete, nových a cudzích zariadení pripojených k sieti, výpadkov služieb, chýbajúcich reverzných DNS záznamov, nových a cudzích zariadení pripojených k sieti. Detekcia NAT. Detekcia ťažby kryptomien, únikov dát, supply chain útokov a ransomware.
* Systém umožňuje Threat Inteligence napojenie - identifikácia bezpečnostných udalostí (napr. komunikáciu s botnet command & control centrom, prístup na phishingové servery, ransomware, cryptojacking apod.) využívaním zdrojov IP a host reputačných databáz poskytovaných výrobcom a aktualizovaných najmenej každých 24 hodín. Systém umožňuje zapojiť ďalšie zdroje IP a host reputačných dát pre automatickú detekciu z cez CSV alebo MISP.
* Detekcia sieťových anomálií na základe predikcie budúceho správania siete s využívaním znalosti histórie komunikácie.
* Vstavaná funkcionalita detekcie narušenia (Intrusion Detection System).
* Systém musí mapovat a vizualizovať kontextuálne MITTRE ATT&CK taktiky a techniky voči jednotlivým udalostiam pre výskyt anomálií a bezpečnostných hrozieb na sieti.
* Prípadné udalosti, ktoré predstavujú falošné poplachy (false positives) je možné odstrániť prostredníctvom jednoduchej konfigurácie pravidiel vylúčenia falošných poplachov dostupné v používateľskom rozhraní.
* Preddefinované priority udalostí s možnosťou používateľského nastavenia závažnosti udalostí na základe IP adresných rozsahov, typov udalostí, miest výskytu alebo detailov udalosti. Jedna udalosť môže mať v závislosti na konfigurácii priradených viac priorít.
* Udalosti je možné automaticky exportovať vo formáte Syslog. Predpokladané využitie tejto funkcionality je integrácia so systémami typu SIEM, SOAR alebo log management.
* Udalosti je možné reportovať do dohľadových systémov prostredníctvom funkcionality SNMP trap.
* Notifikácia o detekovaných udalostiach prostredníctvom e-mailu s podporou rôznych formátov (HTML, incident handling systém, úsporný textový formát). Možnosť pripojiť vzorku flow dát, na základe ktorých bola udalosť detekovaná k emailovému reportu.
* Vizualizácia priebehu prevádzky s vyznačením detekovaných udalostí v závislosti od nastavenej závažnosti udalostí.
* Systém integruje informácie zo služieb DNS, WHOIS, geolokačná služby. Užívateľsky definované externé služby fungujúce na protokole HTTP.
* Systém detekcie anomálií poskytuje dokumentované RestAPI pre získavanie, odosielanie a spracovanie udalostí. Prostredníctvom RestAPI je možné systém detekcie anomálií takisto konfigurovať (napr. vytvárať filtre, meniť nastavenia detekčných metód, apod.).
* Systém umožňuje vytvárať správcovi vlastné aplikovateľné detekčné metódy na základe vzorcov chovania siete napr. na báze jednoduchého SQL syntaxu.
* Na výskyt udalosti je možné automaticky reagovať spustením užívateľsky definovaných skriptov.
* Automatizovaná analýza sieťovej prevádzky a výsledky analýzy sú prezentované v zrozumiteľnej podobe v rámci udalostí, ktoré popisujú, ako jednotlivé komunikácie v zázname prevádzky prebiehali. Udalosti sú rozdeľované podľa závažnosti do niekoľkých úrovní a indikujú problémy vzniknuté v sieťovej prevádzke na podporovaných protokoloch.
* Automatizácia mitigácie a blokovanie bezpečnostných hrozieb na inštalovanej báze s využitím EDL (External Dynamic List) na aktívnych prvkoch (switche, firewall atd.) alebo vytvárania bezpečnostných a konfiguračných pravidiel cez API - automatizované prepojenie medzi detekovanou udalosťou a jej zablokovaním / mtigáciou v rámci odozvy.
* Systém musí umožňovať blokovanie/mitigáciu udalostí plne automatizovanou a poloautomatizovanou formou.
* Systém musí byť ako platforma pripravený na doplnenie, doprogramovanie a nasadenie custom zdrojov dát vo formáte Syslog, PlainText, Json a pod., parserov a automatizáciu v rámci činností IT bezpečnostných operácií, či preddefinovanie tvorby bezpečnostných pravidiel pre SOC operátoro a analytikov, doprogramovanie integrácií v rámci inštalovanej bázy pre potreby CTI a ich nasadenie v prostredí infraštruktúry zadávateľa.
* Systém musí umožniť zvoliť rozsahy siete, na ktoré sa má, alebo nemá aplikovať pravidlo pre automatizkú mitigáciu kybernetických hrozieb.
* Vstavaná natívna podpora alebo doprogramovanie pre automatizovaných audit chybných konfiguračných a bezpečnostných politík na firewaloch a s možnosťou automatizovaného odmazania chybných politík bez nutnosti konfigurovať firewall.
* Vstavaný tester udalostí a výstrah, ktorý simuluje workflow, keď sa incident stane v sieti. Tester musí byť schopný generovať skutočný incident.
* Vstavaný tester konfiguračných a bezpečnostných politík, ktorý umožňuje presne zistiť, či bude dané spojenie (do urovne aplikácie) povolené na konkrétnom firewalle, a ktoré pravidlo ho povolí.
* Používateľsky definované severity a kritickosti udalostí a bezpečnostných pravidiel.
* Systém musí umožniť custom prepojenie externých zdrojov informácií pre potreby CTI a CDN cez vstavané API rozhranie vrátane existencie preddefinovaných zdrojov pre look up typu NIST CVE, Shodan, Virustotal, Bitcoin, Maclookup, Cmd, Hostio, RIPE.
* Systém musí mať preddefinované zdroje dát min typu Office365, Phistank a umožňovať automatizovanú formu tvorby adresných IP listov, URL a DNS pre využitie EDL (externých dynamických listov).
* Webové centrálne užívateľské rozhranie, používateľsky definované (konfigurácia per používateľ).
* Systém loguje všetky zmeny konfigurácie s cieľom zaistiť auditovateľnosť činnosti používateľov a vykonané zmeny s dopadom na detekcie a blokovanie udalostí. Zmeny konfigurácie je možné tiež odosielať protokolom syslog pre auditovanie formou externého systému typu SIEM alebo log management.
* Reporting min. vo formáte PDF alebo CSV, email, Json a Syslog a možnosť nastavovania rôznych alertovacích mechanizmov per udalosť.

**Ďalšie požiadavky pre oblasti :**

|  |  |
| --- | --- |
| **Oblasť žiadosti** | **Špecifikácia požiadavky** |
| Sieťová analýza | Sieťové prenosy sa analyzujú pre všetky sieťové prenosy a bez ohľadu na použité komunikačné protokoly. Monitoruje všetky prebiehajúce pripojenia na všetkých ip sieťových portoch. |
| Sieťová analýza | Funkčnosť analyzovať a zaznamenávať popis sieťovej prevádzky cez zrkadlený port, ktorý obstarávateľ poskytuje na vyhradenom prepínači. |
| Sieťová analýza | Na základe analýzy operácie bude systém tiež schopný uskutočňovať preventívne zásahy – ukončenie spojenia. Na tento účel zadávateľ poskytne dodatočný prepínač s možnosťou jeho použitia na tento účel. |
| Sieťová analýza | Záznam popisu sieťovej prevádzky bude obsahovať informácie o:   1. Protokol pripojenia a jeho parametre, minimálne:    * pre http atribúty - URL, príkaz, Referer, Stavový kód, user agent, x-forwarder-for, host    * pre SMTP - od, komu, odpoveď kód, User a pre MIME obálky podľa -od, do, message-id, odpoveď-k, Return-Path, predmet    * pre POP3 - User    * Pro IMAP – user, from, to, subject    * pre FTP - Command, Mode, názov súboru    * Uchádzač uvedie iné protokoly, ktoré sú uznané v analýze sieťovej prevádzky a súbor atribútov, ktoré sú pre ne generované. 2. Prenášané súbory akýmkoľvek protokolom- aspoň ich meno, veľkosť, hash a informácie o skutočnom type súboru, bez ohľadu na príponu jeho názvu. 3. V prípade archívov alebo vložených súborov, bude tiež obsahovať ich parametre, do ľubovoľnej hĺbky vnorenia. |
| Sieťová analýza | Pravidlá analýzy návštevnosti umožňujú definovať podmienky odkazujúce na prenášaný obsah a všetky zaznamenané atribúty súborov alebo protokolov , napríklad na odhalenie prenášaných súborov, ak Nezodpovedá obsahu, alebo typické TCP a UDP port čísla nesúhlasia s typom zisteného komunikačného protokolu. |
| Sieťová analýza | Škálovateľnosť systému na monitorovanie eternetových rozhraní s rýchlosťou 1Gbps a 10Gbps pre budúcu expanziu systému na monitorovanie prevádzky internej siete. |
| Sieťová analýza | Je možné definovať pravidlá, ktoré hľadajú prekrývajúce sa udalosti alebo postupnosť udalostí v sieťovej premávke a generovať upozornenia (alerty) priebežnou analýzou okamžitej akcie ako aj spätnej analýzy už uložených historických záznamov o premávke.  V pravidlách je možné odkazovať na ľubovoľný atribút v zaznamenanom opise komunikácie. |
| Sieťová analýza | Systém poskytuje webové používateľské rozhranie na analyzovanie zaznamenanej návštevnosti a upozornení bezpečnostnými špecialistami, ktoré budú súčasťou zjednoteného užívateľského rozhrania systému. |
| Sieťová analýza | K dispozícii sú historické informácie o prevádzke s určeným obdobím uchovávania pre následnú analýzu a tieto informácie možno vyhľadávať podľa základného parametra zaznamenaného popisu prevádzky a kombinácie parametrov v logickom výraze. |
| Sieťová analýza | Systém bude môcť monitorovať prevádzku prechádzajúcu cez existujúcu web-proxy, ktorá je schopná poskytnúť http/https informácie pre pripojenie ICAP. |
| Detekcia malwaru | Detekcia škodlivého softvéru sa vykonáva pomocou vyhľadávania signatúr, analýzy správania(behavioral analysis) a detekciou spustenia na virtuálnom izolovanom systéme(sandbox). |
| Detekcia malwaru | Dodávka obsahuje priebežnú aktualizáciu signatúr /definícií malware, aktualizáciu behaviorálnych sandbox pravidiel z komerčného zdroja. |
| Detekcia malwaru | Rovnako ako DLP, systém je schopný detekovať malware skrytý hlboko v prenášaného obsahu-bez obmedzenia hĺbky vnorenia. |
| Detekcia malwaru | Bude nasadený sandboxing ako metóda detekcie nových/neznámych malwarov. |
| Detekcia malwaru | Systém bude môcť použiť aktualizované signatúry na historický Popis prevádzky nájsť malware, ktorý nebol zistený v minulosti. |
| APT | Schopnosť systému zabezpečiť viditeľnosť všetkých fáz APT útoku (podľa kill-chain fáz - od počiatočného kompromisu až po ex-filtráciu dát). (APT - Advanced Persistent Threat) |
| APT | Schopnosť zobraziť všetky relevantné sieťové aktivity a udalosti pri vyšetrovaní konkrétneho incidentu hľadaním udalostí a vyhľadávaním v záznamoch o aktivite v sieti. |
| APT | Sieťové aktivity súvisiace s jedným koncovým ukazovateľom budú môcť zobraziť systém na obrazovke jedného používateľského rozhrania podľa nastaviteľných filtrov, pokiaľ ide o čas, sieťový protokol, číslo portu alebo porty, IP adresy alebo rozsahy, podľa hash alebo názvu prenášaného súboru, e-mailovej adresy a predmetu správy pre e-maily, atď. |
| Reporting | Schopnosť generovať zostavu (v ideálnom prípade vo forme dokumentu PDF) a odoslať ju na e-mailovú adresu s definovanou periodicitou. |
| Reporting | Riešenie ponúka sadu preddefinovaných zostáv(reportov) s možnosťou ich úpravy, ako aj definovanie vlastných zostáv. |
| Reporting | Schopnosť zaznamenávať prevádzkové štatistiky riešení a incidentov, vytvárať exportovateľné výstupy vrátane grafov.  Možnosť odoslať log do externého úložiska aspoň vo formáte syslog. |
| Podpora vyšetrovania | Systém umožní realizovať aspoň základný pracovný postup pre prácu so zaznamenanými upozorneniami (stav, priradenie Riešiteľ, História aktivít, dôvod uzavretia). |
| Podpora vyšetrovania | Systém umožní zhromaždenie dôkazov/zistení týkajúcich sa jediného incidentu a ich exportu vo forme dokumentu PDF s cieľom zdokumentovať postup vyšetrovania konkrétneho incidentu. |
| Podpora vyšetrovania | Systém umožní delegovať vyšetrenie alertov na iného bezpečnostného špecialistu. |
| Vlastnosti integrácie | Zdokumentované aplikačné rozhranie pre integráciu zákazníkov s inými bezpečnostnými súčasťami. Preferujeme HTTP & XML alebo JSON API rozhranie. |
| Vlastnosti integrácie | Natívna podpora a integrácia so SIEM aplikáciou. |
| Vlastnosti integrácie | Systém musí podporovať prevádzku v hierarchickom režime pre prípadné budúce zaradenie orgánov dohľadu alebo podriadených v bezpečnostnom dohľade. |
| Vlastnosti integrácie | Systém umožní pripojenie a import Threat-Intel z iných zdrojov v štandardných formátoch-STIX/TAXII, OpenIOC, YARA. |

Sieťový systém bude pripojený k zdrojom zrkadlenej prevádzky agregovanej šírky min. **500Mps** a bude vykonávať bezpečnostnú analýzu v testovacom pracovisku.

Pre koncové body je požadovaná licencia pre minimálne **10 koncových zariadení.**

Doba uchovávania popisu sieťovej prevádzky a popisu udalostí na koncových bodoch bude min.**30 dní**.

Všetky systémové komponenty, budú nasadené v prostredí zadávateľa, a dodávateľ môže definovať požiadavky na VMware zdroje zadávateľa a používať ho ako operačnú platformu systému.

Podporné služby a Threat-Intel aktualizácie pre systém bude pokrývať obdobie **2 rokov**.

**Záruka a podpora**:

* Podpora od výrobcu s dostupnosťou 7/24/365 po dobu 24 mesiacov.
* Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou vadného komponentu do 24h, po dobu trvania 2 roky.

**Požiadavky na výpočtové a úložné kapacity systému pre detekciu a riešenie kybernetických bezpečnostných incidentov.**

|  |  |
| --- | --- |
| **Názov** | **Sieťová sonda** |
| Počet | 1 |
| Kapacita (analytická rýchlosť) | min. 1 Gbps |
| Prevedenie | HW prevedenie, 2U rack |
| Riešenie musí byť prevádzkované v rámci infraštruktúry objednávateľa | Áno (on premise) |
| Požadované pripojenie | min. 4x 1GbE a 4x 1/10/25GbE a 4x SFP+ (Optical, multi- mode, 1G/10G) |
| Napájanie | Redundantné AC |

|  |  |
| --- | --- |
| **Názov** | **Dedikované dátové úložisko pre sieťovú sondu** |
| Počet | 1 |
| Kapacita (analytická rýchlosť) | min. schopnosť zaznamenať informácie postačujúce na analýzu sieťovej prevádzky o šírke 1Gbps s utilizáciou 50% po dobu min.30Dní |
| Prevedenie | HW prevedenie, rack, max 2U |
| Úložná kapacita | Min. 2x HDD 300GB a 22x HDD 1,2TB |
| Požadované pripojenie | min. 4x 1GbE |
| Napájanie | Redundantné AC |

|  |  |
| --- | --- |
| **Názov** | **Manažment prostredia bezpečnostnej sieťovej platformy** |
| Počet | 1 |
| Porty | Min 4x1GbE |
| Prevedenie | Rack, 1U |
| Priepustnosť | „Nonblocking“ pre akékoľvek veľkosti rámcov |
| Funkcionality | Min. VLANs; SPAN/MIRROR/TAP funkcionalita; RSTP; Static Routing, Appliance s Licencovaním pre manažment komponentov celej sieťovej bezpečnostnej platformy |
| Napájanie | Redundantné AC |

**Záruka a podpora**:

* Podpora od výrobcu s dostupnosťou 7/24/365 minimálne po dobu 24 mesiacov.
* Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou vadného komponentu do 24h, po dobu trvania 2 roky.

1. **Všeobecné požiadavky na Next Generation Firewall (NGFW) s IPS funkcionalitou**

**Počet:**

* 2ks identických NGFW

**Počet portov:**

* 10GE SFP+ min. 4
* GbE RJ45 min. 18
* GE SFP min. 8
* Konzola (RJ45) min.1

**Systémové požiadavky:**

* Firewall priepustnosť (1518/512/64 byte UDP paketov) min. 27/27/11 Gbps
* Firewall priepustnosť (pakety za sekundu) min. 16.5 Mpps
* Počet súbežných relácií (TCP) min. 3 milióny
* Nové relácie za sekundu (TCP) min. 280 000
* IPSec VPN priepustnosť (512 bajtové pakety) min. 13 Gbps
* SSL-VPN priepustnosť min. 35 Mbps
* Súbežný SSL-VPN uživatelia (dopručené max.) 500
* IPS priepustnosť min. 5 Mbps
* NGFW priepustnosť min. 3,5 Gbps
* Threat Protection priepustnosť min. 3Gbps
* Virtuálne domény min. 10
* Konfigurácia vysokej dostupnosti aktívne/aktívne, aktívne/pasívne, klástrovanie
* Rozmery 1U
* Forma rack mount
* vyžarovanie tepla max 430 BTU/h
* Certifikácie ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6
* Podpora 24x7x365 plný prístup k online portálu, plný prístup k SW fixom a novým vydaniam SW.

**Záruka a podpora**:

* Podpora od výrobcu s dostupnosťou 7/24/365 po dobu 24 mesiacov.
* Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou vadného komponentu do 24h, po dobu trvania 2 roky.

1. **Všeobecné požiadavky na dodávku a implementáciu systému na centralizovanú správu logov a iných strojových dát z ľubovoľných zdrojov**

* Centrálne riadený klient na zber logov
* Neobmedzený počet zdrojov - Žiadne licencie.
* Integrácia so SIEM, Syslog-Out, REST-API.
* Vysoká dostupnosť v aktív/aktív režime
* Trvalý príjem minimálne 5000 udalostí za sekundu. (EPS) Špičkové EPS min. 10 000, Možnosť navýšenia výkonu.
* V základe Kapacita DB min. 40TB, Možnosť navýšenia min do 100TB
* Úložisko dát s integrovanou kompresiou a možnosťou šifrovania AES-256.
* Retencia logov minimálne 3 000 EPS - 275 (5502 )dní
* Integrované diskové pole typu RAID 6 s ochranou proti výpadku diskov.

**Podporované zariadenia min. v rozsahu:**

* Networking - Cisco, HP, Huawei, Aruba, Dell, H3C, Extreme Networks, Brocade SAN, Mikrotik, Juniper
* Firewally - Fortinet, Juniper, Checkpoint, Kernum, Cisco ASA, Dell SonicWall, H3C, Hillstone, Sophos, Huawei USG, Palo Alto Networks
* Windows servery, stanice a aplikácie - Hyper-V, DHCP, Firewall, IIS, SharePoint, Exchange....
* Linux servery - Apache httpd, Tomcat, Nginx
* VMWare - ESX, Vcenter, FlowMon
* WiFi - FortiNet, Aruba, HP, Cisco, H3C, Trapeze/Juniper, UBNT, Dell, Ruckus
* Antiviry - Avast, AVG, ESET, Kaspersky, Microsoft Defender
* Adresárové služby - MS ActiveDirectory, Novell eDirectory
* Databázy - Oracle, MS SQL, MySQL, PostgreSQL, SAP
* Systémy pre riadenie 802.1x - Addnet, GAMA

**Užívateľsky definované zdroje min. v rozsahu:**

* JavaScript Object Notation (JSON), Common Event Formátu (CEF), Log Event Extended Formátu (LEEF), WebTrends Enhanced Log Formátu (WELF) a strukturovaného Syslog Formátu (RFC5424)
* Priama technická podpora výrobcom a testovanie
* Rozhranie a kompletná dokumentácia v slovenskom , českom alebo anglickom jazyku
* Rozmery 1U alebo 2U
* Forma rack mount
* Certifikácia (STN/ISO 27001:2013) alebo jej ekvivalent

**Záruka a podpora**:

* Podpora od výrobcu s dostupnosťou 7/24/365 po dobu 24 mesiacov
* Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou vadného komponentu do 24h, po dobu trvania 2 roky

1. **Všeobecné požiadavky na vybavenie pracovných staníc a zobrazovacích zariadení pre zamestnancov centra pre bezpečnostný monitoring, detekciu bezpečnostných incidentov a riešenie kybernetických bezpečnostných incidentov, tzv. Security Operations Centra**

**Pracovná Stanica:** 2ks

**Minimálne technické parametre:**

**Procesor :** Procesor 8 jadier, 16MB cache s priemerným skóre min. 19 350 PassMark CPU Benchmark

**Pamäť :** min. 16 GB, DDR4 SDRAM, 2666 Hz, Non-ECC (s možnosťou rozšírenia do 128 GB)

**Operačný systém :** Windows 10 Pro (64Bit) s možnosťou upgrade na Windows 11.

**Optická mechanika** : áno

**Kapacita disku:** min. 1x 512GB PCIe NVMe M.2 SSD + 2TB SATA HDD

**Grafická karta:** Nvidia Quadro P2000 alebo ekvivalent, min. 5GB GDDR5, min. 4x Displayport, PCI Express x16 3.0

**Pripojenie**: min. 10/100/1 000 Mb/s

**Konektivita (minimálny počet portov):**

vpredu

2x port USB 3.2, typ A (2. generácie, 10 Gb/s)

1x port USB 3.2, typ A [5 Gb] (Power share)

1x port USB 3.2 typu C Gen 2x2 [20 Gb/s]

1x univerzálna zvukový konektor typu Jack 3.5mm

vzadu

2x porty USB 3.2 Type-A Gen1 (5Gbps)

1x port USB 3.2 Type-A Gen2 (10Gbps)

2x porty USB 2.0 typu A

1x univerzálna zvukový konektor typu Jack 3.5mm

1x sieťový konektor RJ45 1Gb

1x port PS2 pre klávesnicu

1x port PS2 pre myš

2x DisplayPort 1.4

**Zobrazovacie zariadenie:** 4ks

**Minimálne technické parametre:**

**Uhlopriečka displeja:** min. 55“, LED podsvietenie, 16:9

**Rozlíšenie obrazovky:** min. 3840x2160 (60HZ)

**Kontrast:** min. 4000:1

**Jas:** min. 300cd/m2

**Typ povrchu displeja:** matné

**Konektivita (min. počet portov):**

1 x Audio line out port, 1 x Audio line in port, 1 x VGA port, 1 x DisplayPort version 1.2, 2 x HDMI port version 2.0, 1 x USB Dedicated charging port, 2 x USB 3.0 downstream ports, 1 x USB 3.0 upstream port, 1 x RS232, 1 x RJ-45, 1 x USB Dedicated charging port, 2 x USB 3.0 downstream ports, 1 x USB 3.0 upstream port

**Ostatné parametre:** ENERGY STAR certified monitor, TCO certified display, RoHS compliant, Držiak na stenu s montážnou sadou.

**Záruka a podpora**:

Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou vadného komponentu do 24h, po dobu trvania 2 roky.

1. **Všeobecné požiadavky na služby**

* Implementácia hardvéru a inštalácia softvéru.
* Implementácia, konfigurácia, integrácia, doladenie riešenia pre každý dodávaný systém v rozsahu definovanom v Prílohe č. 4 týchto súťažných podkladov - Návrh na plnenie kritérií.
* Zaškolenie pre každý dodávaný systém v rozsahu definovanom v Prílohe č. 4 týchto súťažných podkladov - Návrh na plnenie kritérií.
* Dokumentácia inštalácie a inštalačných postupov.
* Dokumentácia aktualizácie a aktivácie jednotlivých nástrojov.
* Otestovanie a ohodnotenie funkčnosti integrácií dodaných riešení.
* Podpora od výrobcu s dostupnosťou 7/24/365 po dobu 24 mesiacov.
* Hardvérová podpora s dostupnosťou 24 x 7, s garantovanou opravou/výmenou vadného komponentu do 24h, po dobu trvania 2 roky.