**Příloha č. 4 Minimální technické podmínky**

## Monitoring síťového provozu

Zadavatel požaduje dodávku dvou systémů

1. Systém pro monitorování síťového (datového) provozu
2. Systém pro monitoring aktivit privilegovaných uživatelů

### **Systém pro monitorování síťového (datového) provozu**

Předmětem veřejné zakázky je dodávka systému pro monitoring a vyhodnocování anomálií síťového provozu (dále jen „systém“) ve vnitřní síti zadavatele. Dodávka systému představuje nákup a implementaci systému (v rozsahu min 5 člověkodnů práce certifikovaného technika), tedy bezpečnostního a technologického řešení pro:

* zajištění automatizace monitoringu síťového provozu na bázi datových toků,
* včasnou detekci případných kybernetických útoků v rámci síťové infrastruktury zadavatele,
* včasnou detekci provozních anomálií v rámci síťové infrastruktury zadavatele.

 Další požadavky na technické řešení:

* statistiky získané z dlouhodobého detailního monitoringu provozu síťové infrastruktury umožní sledování a vyhodnocení objemů a struktury dat v reálném čase,
* analytická funkce zjištění příčiny provozních anebo výkonnostních problémů včetně odhalování bezpečnostních hrozeb,
* systém založený na pokročilých metodách tzv. behaviorální analýzy umožňující odhalování hrozeb a incidentů, které překonají zabezpečení na perimetru datové sítě nebo bezpečnostní ochranu koncových stanic, pro které není dostupná signatura pro antivirové nebo IPS (Intrusion Prevention Systems – systém prevence průniků) řešení,
* funkce včasné detekce a reakce na bezpečností incidenty vhodně doplňující stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům, které jsou v perimetru sítě zajištěny především firewallem typu NGFW a na koncových stanicích antivirovým řešením s integrovaným personálním firewallem,
* funkce další možné analýzy, vizualizace a automatických reportů detekovaných událostí,
* úplná nezávislost systému na použité síťové infrastruktuře a podmínka, aby systém svou funkcí monitorovanou síť neovlivňoval,
* ze strany sledované sítě nesmí být systém detekovatelný,
* automatické vyhodnocování IP toků musí umožňovat automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí.

#### **Minimální technické parametry systému**

##### Požadavky na monitorovací systém

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Uložení a zpracování statistik musí být zajištěno na k tomu určeném specializovaném zařízení – kolektor. Ten musí být vybaven SW či HW RAIDem, Kolektor musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat probíhá kontinuálně s dostupností bez jakékoliv ztrátové agregace. Požadována je plná customizace způsobu prezentace dat a reportů na základě cílového prostředí. Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow).

Součástí dodávky monitorovacího systému musí být i pěti letá záruční podpora zahrnující všechny updaty i upgrady, přístup k webovému zákaznickému centru, podporu telefonem a emailem v českém jazyce v pracovní době (8x5), vzdálenou podporu přes SSH, konzultace síťového a bezpečnostního technika a NBD (Next Bussines Day) hardwarovou záruku v místě instalace.

Monitorovací systém bude kompatibilní a v případě budoucí potřeby rozšířitelný o systém na monitorování výkonu aplikací, který bude umožňovat transparentně (bez vlivu na aplikaci a infrastrukturu) a bez instalace softwarových agentů monitorovat provoz aplikace, vyhodnocovat její výkon a reportovat/notifikovat o stavu aplikace.

Požadavky na monitorovací systém musí splňovat požadavky uvedené v tabulce.

|  |  |
| --- | --- |
| **POŽADAVEK** | **POPIS** |
| Ucelený, škálovatelný NetFlow/IPFIX monitorovací systém | Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflowd, NetStream). |
| Podpora infrastruktury | Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s. |
| Decentralizovaný monitoring lokalit s centrální správou | Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému. |
| Nezávislost na stávající infrastruktuře | Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce). |
| Zdroje NetFlow statistik (sondy) | Specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5,v9, IPFIX) |
| Bezeztrátový sběr flow statistik z více zdrojů | Bezeztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlowv v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream). |
| Ukládání statistik a vyhodnocování bezpečnostních hrozeb | Ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. |
| Rozhraní pro integraci nástrojů třetích stran | Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran. |

##### Požadavky na zdroje NetFlow/IPFIX dat (sondy)

Pro zajištění komplexního přehledu a detailních informací o dění v síti bude využito výkonné autonomní zařízení/sondy – zdroje flow dat (NetFlow/IPFIX), které monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data musí obsahovat informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvy OSI modelu. Zařízení/sondy rovněž musí umožňovat analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. http, DNS, DHCP). Mimo objemových charakteristik provozu budou rovněž sledovat výkonové parametry datové sítě (např. RTT, SRT, iter) pro analýzu zpoždění na síti.

Zařízení/sondy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňovat sledovanou síť. K síti mohou být připojeny pasivně prostřednictvím SPAN/mirroring portu nebo pomocí TAPu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné.

Specifikace zdrojů NetFlow/IPFIX dat (sondy):

* **1 ks – virtuální zařízení pro prostředí Vmware s 2 monitorovacími porty**

Zařízení/sondy musí splňovat požadavky uvedené v tabulce níže

|  |  |
| --- | --- |
| **POŽADAVEK** | **POPIS** |
| **Požadavky na zdroje NetFlow/IPFIX dat (sondy)** |
| Pasivní zapojení | Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). |
| Instalace | Snadná instalace do stávající síťové infrastruktury – šablony pro nasazení virtuálního stroje. |
| Zabezpečená vzdálená správa  | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. |
| Dohled | Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. |
| Minimální výkon | Minimální výkon 1 milion paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed s garancí zpracování všech paketů. |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+ |
| Podpora protokolů pro výměnu dat | Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX. |
| Podpora spolehlivého a šifrovaného exportu toků dle standardu | Zařízení umožňuje exportovat statistiky o síťovém provoze (toky) pomocí spolehlivého a zabezpečeného komunikačního kanálu dle standardu RFC 5153. |
| Zpracování datového provozu | Zpracování datového provozu Ipv4 a Ipv6, VLAN, MPLS a jejich reportování na kolektor. |
| Analýza tunelovaného provozu | Monitorování provozu v tunelu (deenkapsulace) GRE, ESP a OTV. |
| Uživatelsky definované šablony | Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. |
| Monitorování MAC adres | Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. |
| Detekce aplikací | Detekce aplikací dle standardu NBAR2. |
| Analýza zpoždění na síti | Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování a analýza http provozu | Monitorování a analýza http provozu – včetně položek typu URL, hostname, stavový kód http, dotazovací metoda. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Profilování zařízení v síti | Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování VoIP | Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, iter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování DNS provozu | Monitorování a analýza DNS provozu – položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování SMB/CIFS provozu | Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování DHCP provozu | Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování e-mailového provozu | Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování MS SQL (TDS protokolu) provozu | Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování rozšířených L3/L4 informací | Monitorování rozšířených L3/L4 informací – TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.  |
| Kapacita paměti současných toků | Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port. |
| Nastavení času pro expiraci toků | Podpora pro nastavení časů u aktivní a neaktivní expirace toků. |
| Vzorkování | Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. |
| Simultánní export NetFlow statistik | Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX). |
| Export na základě filtrování dat na sondě | Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). |
| Vyplňování identifikace AS | Podpora vyplňování AS na základě vestavěného či dodaného seznamu. |
| Vyplňování čísla interface | Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. |
| Záchyt provozu v plném rozsahu | Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu.  |

##### Požadavky na kolektor pro ukládání NetFlow/IPFIX dat

Pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat bude využitý hardwarový kolektor (dále jen „kolektor“) s minimální diskovou kapacitou dle níže uvedené specifikace. Kolektor bude podporovat flow data ve formátech jFlow, sFlow, NetStream a další kompatibilní s NetFlow a tudíž na něj bude možné exportovat flow data z různých zdrojů (routery, switche, firewally, apod.). Zobrazení uložených flow dat a jejich analýza (vyhledávání, agregace, výpisy aj.) bude probíhat na kolektoru prostřednictvím zabezpečeného webového rozhraní. Uložená data a výsledky analýz budou dostupná ve formě dlouhodobých grafů a top statistik s možností zobrazení dat až na úrovni jednotlivých komunikací (jednotlivé NetFlow/IPFIX záznamy). Kolektor musí také poskytovat funkce reportování statistik o síťovém provozu a systém notifikací v případě výskytu definované události/anomálie.

Specifikace kolektoru NetFlow dat

* **1 ks – fyzické (hardwarové) zařízení/kolektor o výkonu min. 150 000 toků/s, úložné kapacitě min. 3TB, RAM min. 64 GB**

Kolektor musí splňovat požadavky uvedené v tabulce níže.

|  |  |
| --- | --- |
| **POŽADAVEK** | **POPIS** |
| **Požadavky na kolektory NetFlow dat** |
| Ukládání flow statistik | Zabezpečené ukládání flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce. |
| Granularita vizualizace | Kolektor umožní zpracování a vizualizaci flow záznamů volitelně min. v 5minutových nebo 30sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků.  |
| Podpora standardů datových toků | Podpora standardů v rozsahu: NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. |
| Hlavní funkcionalita | Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení. |
| Instalace | Instalace do stávající síťové infrastruktury – racková montáž. |
| Management rozhraní | Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. |
| Zabezpečená vzdálená správa  | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+. |
| Podpora HOT SWAP a RAID  | Kolektor musí být vybaven HOT SWAP disky s podporou RAID včetně SMART detekce. |
| Dohled | Kolektor musí být možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. |
| Sériová linka pro konfiguraci zařízení | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. |
| Podpora Cisco AVC | Podpora standardu Cisco AVC vč. položek HTTP hostname a URL. |
| Podpora dalších flow standardů | Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2. |
| Podpora položek proměnlivé délky | Podpora IPFIX položek proměnlivé délky.  |
| Podpora IPFIX rozšíření jiných výrobců | Podpora rozšíření VMware NSX. |
| Monitoring výkonu sítě | Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety. |
| Monitoring informací z aplikační vrstvy  | Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS). |
| Monitorování rozšířených L3/L4 informací | Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů.  |
| Kapacita datového úložiště | Systém musí být schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště o velikosti minimálně 3 TB musí umožnit záznamy statistik bez jakékoliv redukce. |
| Rozlišování rozdílných samplovacích poměrů pro každé rozhraní zdroje flow dat | Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat. |
| Přeposílání flow vč. možnosti samplingu a převodu formátu | Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik. |
| Spolehlivý a šifrovaný přenos IPFIX dat | Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 5153 |
| Automatická identifikace zdroje flow statistik | Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. |
| Zálohování a obnova flow statistik | Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky. |
| Podpora pro uživatelské identity | Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele). |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). |
| Vizualizace statistických dat | Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem. |
| Vizualizace výkonnostních metrik sítě | Vizualizace výkonnostních metrik sítě v grafech provozu. |
| Vizualizace výkonnostních metrik sítě | Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru. |
| Analýza dat a ad hoc výstupy | Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. |
| Řízení uživatelského přístupu | Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). |
| Top N statistiky | Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků, nejvyšší hodnoty RTT, průmětné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. |
| Filtrování a přizpůsobení výstupů | Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). |
| Uživatelsky definovatelné alerty | Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu. |
| Uživatelsky definované pohledy na datový provoz | Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.). |
| Drill-down | Možnost dohledat každý jednotlivý datový tok (flow záznam). |
| Monitoring aktivních zařízení na sítí | Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení. |
| Automatická podpora geolokace | Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). |
| Otevřené rozhraní | Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). |
| Aplikace pro mobilní zařízení | Aplikace pro mobilní zařízení platformy Android a iOS, pro zobrazování základních informací v podobě grafů a statistik per jednotlivý uživatel.  |
| Monitorování dostupnosti zdroje flow dat | Monitorování dostupnosti zdroje flow dat pomocí SNMP. |

##### Požadavky na automatické vyhodnocování NetFlow/IPFIX dat

Systém pro automatické vyhodnocování IP toků musí umožňovat automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách tzv. behaviorální analýze a umožňovat tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura pro AV nebo IPS řešení. Musí se tak jednat o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události musí být dále možné analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM.

**Systém musí splňovat požadavky uvedené v tabulce níže**

|  |  |
| --- | --- |
| **POŽADAVEK** | **POPIS** |
| **Požadavky na automatické vyhodnocování NetFlow dat** |
| Podpora flow standardů | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. |
| Výkon | Minimálně 5000 toků/s |
| Deduplikace | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. |
| Vzorkování na úrovni toků | Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. |
| Správa zdrojů síťových toků | Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků. |
| Identita uživatelů | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. |
| Persistence doménových jmen | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. |
| Detekční pravidla a algoritmy | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. |
| Detekce síťových útoků | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. |
| Detekce anomálií v síťovém provozu | Detekce anomálií v DNS, DHCP, SMTP, VoIP/SIP, multicast provozu a nestandardní komunikace. |
| Detekce nežádoucích aplikací | Detekce P2P sítí, a anonymizačních služeb (např. TOR) |
| Detekce událostí na základě „Threat intelligence“ dat | Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. |
| Detekce provozních problémů | Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. |
| Detekce síťových anomálií | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. |
| Vytváření událostí | Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí. |
| Přímý přístup k události přes unikátní URL s využitím ID události | Systém je schopen poskytnout přímý přístup k evidované události za pomoci ID události z externích systémů za pomoci unikátního URL, které je možné sestavit v externím systému při znalosti ID události. |
| Konfigurační průvodce | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. |
| Konfigurace detekčních schopností | Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). |
| Definice vlastních detekčních metod | Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.). |
| Detekce NATů | Detekce NATů v síti s využitím rozšířených informací z L3/L4. |
| Správa filtrů | Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. |
| Správa falešných poplachů | Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. |
| Definice závažnosti událostí | Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. |
| Různé pohledy na události podle uživatelských rolí | Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí. |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. |
| CEF export | Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu log management. |
| SNMP Trap | Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. |
| E-mailové notifikace | Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu. |
| Záchyt provozu v plném rozsahu | Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu.  |
| Spuštění skriptu | Na výskytu události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů. |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. |
| Integrace informací z jiných služeb | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP. |
| Získávání doplňujících informací z adresářových služeb | Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP. |
| Kategorie a komentáře | Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. |
| Vyhledávání událostí | Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). |
| Interaktivní vizualizace událostí | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých, byla událost rozpoznána. |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF, včetně automatické distribuce reportů e-mailem. |
| CSV export | Události je možné exportovat do formátu CSV pro další zpracování. |
| Otevřené rozhraní | Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). |
| Sledování změn konfigurace | Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace musí být možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu log management. |
| Škálovatelnost řešení | Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí. |

**Požadavky na záruční podporu:**

Záruční podpora bude poskytována na veškeré dodané zboží po dobu 60 měsíců, bude ověřitelná na webu výrobce a bude zahrnovat následující služby minimálně v níže uvedené specifikaci:

* zákaznická podpora v českém jazyce dodavatele (přístup k webovému zákaznickému centru, telefonická a e-mailová podpora, vzdálená podpora přes SSH a konzultace technika v režimu 8x5),
* pravidelná aktualizace a upgrade SW včetně firmware dodaného zboží a aktualizace reputačních databází,
* záruka na dodané zboží po celou dobu trvání záruční podpory (60 měsíců),
* servis certifikovaným technikem v místě instalace systému s garantovanou dobou nástupu následující pracovní den a odstraněním vady nejpozději do 5 pracovních dnů od nahlášení vady.

### **Monitoring aktivit privilegovaných účtů**

Zadavatel požaduje dodávku a nasazení systému pro kompletní dohled nad veškerými dodavatelskými (ale nejen jimi) aktivitami umožňující nahrávání všech vzdálených připojení včetně záznamu textu pro rychlejší orientaci v nahrávkách. Z výše uvedeného požaduje přehledné chronologické reporty s podrobným seznamem provedených akcí včetně odkazů pro přehrání videa.

Navrhované řešení musí monitorovat aktivity privilegovaných uživatelů, a tím minimalizovat bezpečnostní rizika spojená s přístupem ke zdrojům příslušných systémů. Privilegované účty umožňují přístup ke zdrojům příslušných systémů včetně manipulace s nimi, a proto jsou významným bezpečnostním rizikem. Dále znalost přihlašovacích údajů může být sdílena mezi více uživateli, tudíž odpovědnost za případné zneužití by mohla být velice těžko dohledatelná. Tato rizika se vztahují na všechny systémy, počínaje operačními systémy, databázemi, síťovými prvky, komplexními informačními systémy distribuovanými jako produkt, nebo vyvinutými na míru. Z tohoto důvodu vznikla potřeba zadavatele zavést monitoring veškeré aktivity privilegovaných účtů s vazbou na konkrétní osobu, která jím právě disponuje, a to jak zaměstnance organizace, tak i externích dodavatelů. Důležitou oblastí je detailní audit aktivity privilegovaných účtů. To bude zajištěno nahráváním uživatelských relací – snímáním obrazovky a logování uživatelského vstupu (key-logging). Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu bude nahrávána a bude jednoznačně přiřazena konkrétní osobě. Nahrávky budou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou následně dlouhodobě uchovávány. Takové nahrávky jsou klíčovým důkazem, kterým bude možné uživateli jednoznačně prokázat veškeré jeho aktivity.

|  |
| --- |
| **Monitoring aktivit privilegovaných účtů** |
| Parametr | Popis povinného parametru | Účastník ZŘ popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek | Účastník ZŘ uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru |
|
| Autentizace | Autentizace přístupu ke všem komponentám je řízena adresářem LDAP nebo Active Directory. |   |   |
| Správa rolí | Aplikace musí umožnit správu rolí (auditor, správce, apod.) |  |  |
| Záznam uživatelských vstupů a výstupů | V rámci nahrávky jsou zaznamenávány uživatelské vstupy (key-logging) a výstupy na obrazovku. |  |  |
| Upozornění uživatelů | Uživatelé jsou upozorněni na skutečnost, že jejich aktivita je nahrávána. |  |  |
| Auditováni administrátorů | Auditováni, monitoring a nahrávání aktivit administrátorů na serverech při vzdáleném i lokálním přihlášení. |  |  |
| Auditovániexterních uživatelů | Auditování, monitoring a nahrávání aktivit externích uživatelů vykonávající vzdálenou správu v LAN Zadavatele, pomocí předřazené virtuální administrační stanice nebo terminálového serveru. |  |  |
| Auditovániinterních zaměstnanců s VD | Auditování, monitoring a nahrávání aktivit vybraných interních zaměstnanců vyžívajících virtuální desktopy. |  |  |
| Auditovániinterních zaměstnanců | Auditování, monitoring a nahrávání aktivit vybraných interních zaměstnanců vyžívajících počítače nebo notebooky. |  |  |
| Podpora platforem | Podporované platformy pro auditování, monitoring a nahrávání aktivit uživatelů, včetně vynucení definovaných prevenčních pravidel: Windows Desktop (7-10)/Windows Server (2008-2016)/Linux (RHEL, SLES SuSe, Debian, Ubuntu). |  |  |
| Indexace / Metadata | Každá z nahraných uživatelských relací je indexována pomocí textových metadat (názvy oken, textové řetězce, názvy stisknutých tlačítek, …), tak aby bylo zřejmé, k jakým aktivitám během relace došlo, aniž by bylo nutné shlédnout nahranou videosekvenci. |  |  |
| Vyhledávání | V metadatech je možné fulltextově vyhledávat. |  |  |
| Přehrávání relace | Schopnost zpětně přehrávat uživatelské relace ve formě videosekvence. |  |  |
| Kvalita snímků  | Snímek v barevné škále 24 bitů 1 za 3 sekundy. |  |  |
| Export dat | Schopnost exportu nahraných uživatelských relací (včetně snímků obrazovek a metadat) pro tvorbu dokumentace, nebo prokazování incidentů. |  |  |
| Alerting | Integrovaný alerting na základě definovaného nestandardního chování uživatelů (identifikace netypické/nestandardní aktivity uživatele, například spuštění editoru registrů). |  |  |
| Upozornění | Předdefinovaná upozornění, možnost tvorby vlastních upozornění. |  |  |
| Přehrávaní dle metadat | Možnost spustit přehrávání videosekvence přímo z přehledu o aktivitách uživatelů a to včetně konkrétní části dle metadat. |  |  |
| Integrace | Možnost integrace se SIEM nástroji pomocí přímého napojení do databáze pro vyčítání informací v reálném čase. |  |  |
| Reporting | Integrovaný reporting, s možností tvorby vlastních reportů o aktivitách uživatelů, vč. Exportu do XLS/XML/HTML pro následné analýzy. |  |  |
| Politika nahrávání uživatelů | Politikou je možné definovat uživatele, kteří budou, nebo naopak nebudou nahrávání. |  |  |
| Politika nahrávání aplikací | Politikou je možné definovat aplikace, které budou, nebo naopak nebudou nahrávány. |  |  |
| Funkce zamezení ztráty dat při výpadku nahrávacího serveru | Nahrávání uživatelských relací, i v případě nedostupnosti serverové části navrhovaného řešení, bez ztráty nahraných dat. Po obnovení funkčnosti serverové části jsou nahraná data automaticky odeslána. |  |  |
| Podpora standardů | PCI, HIPAA, ISO 27001, GDPR |  |  |
| Podpora virtualizačních platforem | Podpora celého řešení i pro provoz ve virtualizovaném prostředí (VMWare). |  |  |
| Instalace | Instalace do virtuálního prostředí objednatele VMWare 6.x platforma.  |  |  |

Počet monitorovaných zařízení

|  |  |
| --- | --- |
| Typ zařízení | Sdružené zdravotnické zařízení Krnov, příspěvková organizace |
| Windows Server  | 7 |
| Windows Desktop (WIN 7 Pro CZ, WIN 10 Pro CZ) | 3 |
| Linux Server | 1 |
| Instalace monitorovacího systému bude provedena vždy na jedeno zařízení z celkového počtu daného typu zařízení v dané organizaci. Instalaci klientů na další zařízení daného typu provedou po zaškolení správci jednotlivých organizací. |

### **Společná část pro systémy A a B**

#### Školení

Školení obsluhy (IT správců) pro zdravotnické zařízení v rozsahu min. 1 x 8 hod. v prostorách sídla zadavatele.

#### Podpora a servis

Min. 60 měsíců na HW zařízení a na veškerý SW, který je neoddělitelnou součástí HW zařízení, včetně práva na nové verze.

Min. 60 měsíců za jakost od instalace a zprovoznění díla jako celku, tj. aktualizace programového a technického vybavení (Update Service, maintenance) např. předání nových verzí SW modulů programového vybavení s vylepšenými funkcemi tak, jak je výrobce dává k dispozici, řešení vad apod.

#### Licence

Dodané řešení nesmí být řešeno formou pronájmu, po skončení technické podpory musí být dále schopno pracovat. Řešení musí pokrývat veškeré výrobcem technologie garantované SW licence a HW komponenty s jeho podporou na celou dobu požadovanou v této technické specifikaci.

Řešení musí zahrnovat v ceně dodávky všechny náklady na provoz řešení, tedy včetně licence na operační systémy pro nabízené řešení, databázi, middleware apod.

#### Testovací provoz (akceptační testy)

Dodavatel ve spolupráci se Zadavatelem na základě jeho požadavků (v rámci realizace předmětu smlouvy) vypracuje návrh testovacích postupů pro ověření funkčnosti díla během testovacího provozu a vypracuje jednotlivé akceptační protokoly. Návrh testovacích postupů bude předložen Zadavateli (objednateli) a po jeho schválení a doplnění bude Zadavatelem (objednatelem) akceptován.

Testovací postupy se musí týkat minimálně těchto oblastí:

* Funkční testy

Funkční testy ověří, že implementované řešení poskytuje bezchybně vybrané požadované funkcionality uvedené v Technické specifikaci.

Testovací provoz bude probíhat v sídle Zadavatele (objednatele) na stanovených systémech zadavatelem minimálně v délce 30 dní.