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 na k tomu určeném specializovaném dedikovaném zařízení. To musí být vybaveno HW RAIDem a musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice. Dále pak musí poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat musí probíhat kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců.

Požadavek	Popis
Ucelený, škálovatelný monitorovací systém	Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, sFlow).
Podpora infrastruktury	Podpora IPv4, IPv6, VLAN, MPLS, Ethernet až 10Gb/s.
Nezávislost na stávající infrastruktuře	Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce).
Zdroje NetFlow statistik	Specializovaná dedikovaná zařízení 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 ÚLOŽIŠTÍCH 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	Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů.
Zákaznická podpora	Plná zákaznická podpora v českém jazyce.
Reference	Systém ověřený instalacemi v rozsáhlé síťové infrastruktuře (datové linky 10 Gbps a výše).
Rozhraní pro integraci nástrojů třetích stran	Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran.
Přizpůsobení vzhledu (branding)	Možnost přizpůsobit vzhled uživatelského rozhraní a vložit vlastní logo.
Instalace	Instalace bude provedena v sídle zadavatele.
Aktualizace nastavení	Nejdříve po 14 dnech zkušebního provozu bude v sídle zadavatele provedena úprava konfigurace podle zjištěných a naměřených hodnot.
Školení správců	Součástí bude školení správců v délce minimálně 4 hodiny v sídle zadavatele.
Dokumentace	Součástí předání bude dokumentace k systému a jeho nastavení.

Zdroje dat

Zdroje flow (NetFlow/IPFIX) dat musí být výkonná autonomní zařízení, která monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na samostatné dedikované zařízení 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. Tyto zdroje rovněž musí umožnit analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu musí poskytovat rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti.

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

Název požadavku	Popis požadavku
Pasivní zapojení	Pasivní zapojení bez vlivu na monitorovanou síť prostřednictvím SPAN/mirror portu.
Instalace	Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje.
Management rozhraní	Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s 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.
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 0,5 milion paketů za sekundu na každém portu
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.
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 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 úložiště.
Analýza tunelovaného provozu	Monitorování provozu v tunelu 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, jitter, 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).
Monitoring (SSL) šifrovaného provozu	Schopnost monitorování a reportování různých charakteristik provozu šifrovaného pomocí SSL/TLS. To zahrnuje verzi protokolu, šifrovací algoritmus, cipher suite, detaily certifikátu a další.
Monitorování IOT/ICS sítí	Podpora monitoringu nativních IoT a ICS/SCADA prostředí včetně protokolů IEC 61850 (Goose, MMS), DLMS, CoAP a IEC 104. Tyto statistiky jsou monitorovány pomocí standardní IPFIX technologie.
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 zařízení 2 miliony toků na 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. 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.
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. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace.

Požadavky na zdroje dat

Název požadavku	Popis požadavku
Typ	1ks samostatná HW appliance do racku 19 palců
Velikost	1 RU.
Monitorovací porty	Minimálně 1x 10Gbps port SFP+.
Management rozhraní	Dva plnohodnotné management (administrativní) porty RJ45.
Vzdálená správa	Dedikovaný port RJ45 pro monitoring hardware a vzdálené vypnutí/zapnutí.
Příslušenství monitoring	Včetně potřebných optických SFP+ modulů pro vlastní appliance a pro aktivní prvky řady Cisco Catalyst 9400, včetně propojovacího kabelu délky 2m.
Příslušenství management	Včetně 2 ks metalických propojovacích kabelů RJ45 min. Cat5e délky 2m pro management.
Podpora	Podpora poskytovaná výrobcem v délce 12 měsíců.

Požadavky na úložiště NetFlow dat

Musí je jednat o zařízení (datové úložiště) s vysokou diskovou kapacitou určené pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. Úložiště musí podporovat i flow data ve formátech jFlow, sFlow, NetStream a další kompatibilní s NetFlow a tudíž je na něj možné exportovat flow data z různých zdrojů (routery, switche, firewally, apod.). Zobrazení uložených flow dat a jejich analýza (vyhledávání, agregace, výpisy aj.) musí probíhat prostřednictvím zabezpečeného webového rozhraní. Uložená data a výsledky analýz musí být dostupná ve formě dlouhodobých grafů a top statistik s možností zobrazení dat až na úrovni jednotlivých komunikací (jednotlivé NetFlow/IPFIX záznamy). Úložiště dále musí poskytovat funkce reportování statistik o síťovém provozu a obsahovat systém notifikací

v případě výskytu definované události/anomálie. Úložiště také musí přinášet kompletní přehled o dění v síti a umožňovat operátorům přesně, rychle a efektivně řešit problémy v síti, zvýšit jejich bezpečnost díky detekci analýze provozu, optimalizovat síť, plánovat budoucí rozvoj a kapacitní požadavky a snížit provozní náklady.

Název požadavku	Popis požadavku
Ukládání flow statistik	Zabezpečené ukládání flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce.
Granularita vizualizace	Úložiště umožní zpracování a vizualizaci flow záznamů volitelně v 5-minutových nebo 30-sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků.
Podpora standardů datových toků	Podpora standardů 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	Snadná 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 RAID	Hardwarová podpora RAID, zapojení minimálně RAID5
Dohled	Úložiště 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.
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, Gigamon a Ixia IPFIX Extensions.
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.
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 zařízení 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	Systém 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 úložiště, kde je možné tyto statistiky analyzovat standardními prostředky.
Podpora pro uživatelské identity	Úložiště umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity musí být možné získávat ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení musí být 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	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.
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	Úložiště poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné úložiště rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).
Monitorování dostupnosti zdroje flow dat	Monitorování dostupnosti zdroje flow dat pomocí SNMP.

Požadavky na úložiště

Název požadavku	Popis požadavku
Typ	1ks samostatná HW appliance do racku 19 palců.
Velikost	1 RU.
Kapacita datového úložiště	Minimálně 2,5 TB.
Management rozhraní	Dva plnohodnotné management (administrativní) porty RJ45.
Vzdálená správa	Dedikovaný port RJ45 pro monitoring hardware a vzdálené vypnutí/zapnutí.
Příslušenství management	Včetně 2 ks metalických propojovacích kabelů RJ45 min. Cat5e délky 2m pro management.
Podpora	Podpora poskytovaná výrobcem v délce 12 měsíců.

Požadavky na automatické vyhodnocování NetFlow dat

Systém pro automatické vyhodnocování IP toků musí umožnit automatickou detekci bezpečnostních nebo provozních a anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách tzv. behaviorální analýzy a musí jak umožňovat tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Mělo by se tak jednat o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňí stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události musí být možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů má výrazně zjednodušit správu datové sítě, zvyšit její bezpečnost a umožnit proaktivně identifikovat příčiny problémů.

Název požadavku	Popis požadavku
Podpora flow standardů	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream.
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 doménová 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, multicast provozu a nestandardní komunikace.
Detekce nežádoucích aplikací	Detekce P2P sítí a VPN komunikace
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, 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).
Správa detekčních metod	Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry.
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. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu.
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.
Pozastavení platnosti pravidla falešných poplachů	Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu
Smazání falešných poplachů	Systém umožňuje při vytváření pravidel pro falešné poplachy smazat již detekované falešné události.
Dynamické definice falešných poplachů	Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu
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 SIEM nebo log management. Součástí exportu musí být event ID, které jednoznačně identifikuje danou událost.
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. Tyto záchyty je možné uživatelsky spravovat.
Spuštění skriptu	Na výskyt 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. Automatická 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 je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management.

Požadavky na automatické vyhodnocování

Název požadavku	Popis požadavku
Typ	Modul pro instalaci nad úložiště dat.
Výkon	Minimálně 3000 událostí za sekundu.
Podpora	Podpora poskytovaná výrobcem v délce 12 měsíců.

Požadavky na záchyt síťového provozu

Systém na záchyt síťového provozu musí umožnit záznam datového provozu včetně jeho obsahu. Na základě zadaných filtračních kritérií systém provede záchyt síťového provozu, který zpřístupní ve formátu PCAP pro jeho následnou analýzu v libovolných nástrojích třetích stran. Systém tak významně rozšíří možnosti v oblasti identifikace a řešení příčin provozních a komunikačních problémů, které jdou za hranici analytických možností IP toků.

Název požadavku	Popis požadavku
Záchyt síťového provozu	Systém zachycuje síťový provoz v plném rozsahu (vrstvy L2-L7) a záznamy zachyceného síťového provozu ukládá v souboru s formátem PCAP, který je možno stáhnout z webového uživatelského prostředí pro následnou analýzu v programu třetí strany (např. Wireshark).
Podpora vysokorychlostních sítí	Systém je schopný záchytu síťového provozu v sítích s rychlostmi až 10Gb/s.
Pravidla pro filtraci a záchyt provozu	Systém umožňuje pro jednotlivé záznamy definovat filtry a zachytávat tak část síťového provozu. Kritéria filtrace jsou parametry z vrstev L2-L4 a L7.
Filtrace a záchyt provozu podle parametrů linkové vrstvy (L2)	Systém umožňuje filtrovat síťový provoz podle VLAN tagu, MPLS značky.
Filtrace a záchyt provozu podle parametrů síťové vrstvy (L3)	Systém umožňuje filtrovat síťový provoz podle IPv4, IPv6 adresy, čísla sítě a masky.
Filtrace a záchyt provozu podle parametrů transportní vrstvy (L4)	Systém umožňuje filtrovat síťový provoz podle portů TCP, UDP a SCTP.
Nahrávání VoIP provozu	Systém umožňuje filtrovat síťový provoz VoIP hovorů používající SIP a H.323 protokoly .
Nastavení časového intervalu záchytu	Systém umožňuje pro jednotlivé záznamy definovat časový interval, ve kterém se bude síťový provoz zachytávat.
Správa přístupu k záznamům	Systém umožňuje při zadávání záznamu definovat skupinu uživatelů, která má přístup ke stažení záznamu.
Automatické spuštění záchytu provozu	Záchyt síťového provozu je možné spustit automaticky na základě detekce události systémem pro automatické vyhodnocování NetFlow dat.
Definice míst záchytu	Systém umožňuje definovat na jakých sondách a jejich monitorovacích rozhraních bude provádět záchyt síťového provozu.
Otevřené rozhraní	Systém poskytuje dokumentované API pro získávání záznamů zachyceného síťového provozu. Prostřednictvím API je možné v sytému zadávat požadavky na záchyty síťového provozu a definovat pro ně časový interval a filtrační kritéria.
Rotace dat	Automatická rotace starých dat pro uvolnění místa na disku pro nové záchyty síťového provozu.

Požadavky na záchyt síťového provozu

Název požadavku	Popis požadavku
Typ	Modul pro instalaci nad zdroje dat/úložiště dat.
Licence	Minimálně pro 1x port 10 Gbps.
Podpora	Podpora poskytovaná výrobcem v délce 12 měsíců.