

Projektová dokumentace

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU
KOLÍN - zpracování projektové dokumentace“***

TECHNOLOGICKÁ ČÁST JCE IB

D.1.4.9. Technologie a řešení JCE IB

***D.1.4.9.08. ANALÝZA DATOVÝCH TOKŮ V SÍTI (NDR)
NA ZÁKLADĚ MONITORINGU ZALOŽENÉM NA
ANALÝZE NETFLOW-IPFIX - ŠKOLA***

Zpracoval:

Petr Lacina

8 ANALÝZA DATOVÝCH TOKŮ (NDR) - ŠKOLA

8.1 POPIS

NDR je určena pro zvýšení schopností detekce a ochrany před kybernetickými útoky v rámci sítě a analýzu datových toků. Jedná se o sofistikovaný nástroj pro zaznamenání síťového provozu a detekci útočníka v síti s možností automatické reakce na vzniklý bezpečnostní incident.

V rámci provozního prostředí Školy s ohledem na MBS (minimální bezpečnostní standard) bude provedena implementace NDR pro zajištění schopnosti detekce hrozeb v rámci sítě a reakce na ně.

V rámci realizačního projektu je nutné dané řešení vybírat s ohledem na vzájemnou propojitelnost jednotlivých technologií. V rámci Školy se jedná doporučený o sběr a archivaci logů v rámci LM.

V rámci provozního prostředí bude řešení využito pro zaznamenání síťového provozu (síťová sonda) a pro uchování a analýzu dat (kolektor).

Vzhledem ke zdrojům virtualizačních serverů a předpokládanému objemu dat na 10Gbps linkách je požadováno využití hardware. Předpokládaná potřebná úložná kapacita na kolektoru je 3 TB při uchování obohacených dat po dobu 6 měsíců. Odhad reflektuje předpokládaný rozvoj v rámci Školy a její infrastruktury.

Řešení monitoringu a analýzy datových toků bude tedy jednotným celkem (složeným z dílčích HW a SW prvků) určeným pro zvýšení síťové bezpečnosti v provozním prostředí hlavní serverovny a zároveň celé školy. Monitoring a analýza datových toků bude probíhat v produkčním prostředí odděleně od CYLAB.

8.2 OBECNÉ VLASTNOSTI ŘEŠENÍ

Komplexní škálovatelné řešení umožňující monitorování sítě jako systém pro monitorování výkonu, provozu a bezpečnosti počítačových sítí. Monitorovací systém musí umožňovat dlouhodobé podrobné monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit sledovat a vyhodnocovat objemy a strukturu provozu v reálném čase, analyzovat příčiny provozních nebo výkonnostních problémů na straně sítě až po uživatele a jednotlivé aplikace, odhalovat vnitřní a vnější neznámé bezpečnostní hrozby a anomálie na základě analýzy chování sítě, uživatelů a zařízení. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí nenarušoval sledovanou síť. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Pro uložení a zpracování statistik bude využito specializovaného zařízení – kolektor. Pro účely výuky opět ve formě virtuální appliance.

Kolektory 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 po dobu několika měsíců. Samozřejmostí je plná customizace způsobu prezentace dat a reportů na základě cílového prostředí.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow). Tato technologie představuje nejmodernějším prostředek pro monitorování sítě a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní síť nebo specializovaná prostředí průmyslových sítí.

Obecné vlastnosti řešení:

- Řešení musí umět identifikovat zero-day útoky (např. na základě behaviorální analýzy).
- Řešení poskytuje detekci anomálií na síti s podporou deduplikace, vzorkování na úrovni toků, identifikace uživatelů, persistencí doménových jmen.
- Minimální detekční mechanismy zahrnují detekci skenování portů, slovníkové útoky, útoky typu DoS (odmítnutí služby), útoky na síťové protokoly SSH, RDP, Telnet.
- Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikaci.
- Detekce P2P sítí a anonymizačních služeb (např. TOR).
- Detekce událostí na základě "Threat Intelligence" dat (komunikace s botnet C&C), detekce nadměrného zatížení sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti.
- Detekce NAT.
- Řešení musí být schopné analyzovat a vyhodnocovat události nejen na základě porovnání signatur, ale také na základě behaviorální analýzy.
- Řešení nesmí omezovat funkčnost, kvalitu ani narušovat bezpečnost ostatních zařízení/systémů v síti.
- Systém musí podporovat čtení a vyhodnocování informací z síťového provozu, zejména na aplikační úrovni ISO/OSI modelu resp. TCP/IP, s ohledem na možnost odhalení pokročilých útoků.

8.3 POPIS POŽADOVANÝCH TECHNOLOGIÍ

Všechny níže zmíněné technologie budou provozovány v prostředí ŠKOLY. V rámci ŠKOLY a v souladu s jejími potřebami a udržitelnosti je zamýšleno pořízení technologie včetně hardware.

- *NetFlow/IPFIX dat (sondy) – 1 kus:*

Zdroje flow (NetFlow/IPFIX) dat (sondy) jsou výkonné autonomní zařízení, 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 obsahují 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. Soudy musí rovněž umožnit analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu poskytnout sondy rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti. Sonda tak musí přinést komplexní přehled a detailní informace o dění v síti a usnadnit řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Soudy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivnit sledovanou síť. K síti budou připojeny pasivně prostřednictvím SPAN/mirroring portu nebo pomocí TAPu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Sonda bude navíc vybavená vlastní kolektorovou aplikací umožňující lokální ukládání a analýzu vlastních NetFlow/IPFIX dat.

- *Vlastnosti kolektoru NetFlow dat – 1kus:*

Kolektory jsou zařízení (datová úložiště) s vysokou diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. Kolektor dále podporuje 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, firewallly, 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 bude dále poskytovat funkce reportování statistik o síťovém provozu a systém notifikací v případě výskytu definované události/anomálie. Kolektor tak přinese kompletní přehled o dění v síti a umožní operátorům přesně, rychle a efektivně řešit problémy v síti, zvýšit jejich bezpečnost díky detekci a analýze provozu, optimalizovat síť, plánovat budoucí rozvoj a kapacitní požadavky a snížit provozní náklady.

Funkčnost kolektoru musí být možné dále rozšířit o systémy pro automatické vyhodnocování NetFlow/IPFIX dat, záchyt síťového provozu, monitorování výkonu aplikací a systémem pro ochranu proti DoS/DDoS útokům.

- *Automatické vyhodnocování NetFlow dat:*

Systém pro automatické vyhodnocování IP toků musí umožňovat automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém bude založen na pokročilých metodách tzv. behaviorální analýzy a umožní tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostní ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečnostní incidenty, který vhodným způsobem doplní další nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události bude 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 výrazně zjednoduší správu datové sítě, zvýší její bezpečnost a umožní proaktivně identifikovat příčiny problémů.

8.4 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

8.4.1 Obecné požadavky na monitorovací systém

Požadovaná funkcionalita	Specifikace minimálních požadavků
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 (NetFlow 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.
Rozhraní pro integraci nástrojů třetích stran	Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran.
Podpora Microsoft Azure	Podpora pro nativní nasazení v prostředí Microsoft Azure. Podpora pro zpracování dat zrcadleného provozu v Microsoft Azure. Schopnost sbírat, zpracovávat a vizualizovat Azure NSG flow logs, které obsahují informace o provozu zachyceném v Microsoft Azure cloudu.
Multitenance	Jedna instance systému může být nakonfigurována tak, aby monitorovala provoz vícero zákazníků (tenantů) nezávisle. Tenant má definovanou viditelnost na výčet zdrojů flow dat a profilů. Tenant administrator spravuje uživatele a role v rámci tenantu.

8.4.2 Požadavky na zdroje NetFlow/IPFIX dat (sondy) – 1 kus

Požadovaná funkcionální	Specifikace minimálních požadavků
Provedení sondy	Sonda musí být provedena formou hardware appliance, nebo dodávky HW a SW.
Pasivní zapojení	Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty).
Aktivní zapojení	Možnost zachytávat provoz přes ERSPAN nebo GRE tunel, který je zakončen na monitorovacím portu sondy.
Instalace	Snadná instalace do stávající síťové infrastruktury – montáž do standardního rack s vyčleněným prostorem 1U.
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 vyřízení zdrojů technologií SNMP.
Vestavěný kolektor	Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionální flow kolektoru.
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.
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 verzí 5 a 9, IPFIX.
Podpora spolehlivého a šifrovaného exportu toků dle standardu	Zařízení umožňuje exportovat statistiky o síťovém provozu (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.
Deduplikace paketů	Zařízení je schopné detekovat a odstranit duplikované pakety.
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/CIFS 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. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace.
Podpora vysokorychlostních sítí	Řešení podporuje síť s rychlostmi 1/10/40/100GbE (Gigabit Ethernet).
Monitorovací porty sond	Sonda musí obsahovat minimálně 2x 10 GbE optických monitorovacích portů SFP+ na zařízení. Dodávka je počítána včetně optických modulů.
Výkon sond s 10 GbE monitorovacími porty	Sonda musí být schopná zpracovávat minimálně 1,5Mp/s (pakety za sekundu)
Záruka a servisní podpora	Požadujeme dodání hardware sondy vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.

8.4.3 Požadavky na kolektor NetFlow dat – 1kus

Požadovaná funkcionality	Specifikace minimálních požadavků
Provedení kolektoru	Kolektor musí být proveden formou hardware appliance, nebo dodávky HW a SW.
Ukládání flow statistik	Zabezpečené kolektory 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 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 funkcionality	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. Vyčleněný prostor v rack 1U.
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	Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce.
Dohled	Kolektor 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.
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.
Automatická korekce časových známek	Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů.
Kapacita datového úložiště	Systém je schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně šesti měsíců.
Přeposílání flow vč. možnosti samplingu a převodu formátu	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti smplování 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 zaslá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.
Identifikace výpadku dat	Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat.
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).
Předdefinované dashboardy	Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů.
Sdílené dashboardy	Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat).
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, průměrné hodnoty SRT, atd.) umožňující vypsát neaktivnější 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.) prostřednictvím 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).
Síťová topologie	Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie.
Monitoring aktivních zařízení na síti	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.
Kapacita pro sběr dat	Tzv. kolektor musí splňovat kapacitu na sběr dat v minimální výši 3 TB s výkonem až 150 000 toků/s.
Záruka a servisní podpora	Požadujeme dodání hardware kolektoru vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.

8.4.4 Požadavky na automatické vyhodnocování NetFlow dat

Požadovaná funkcionalita	Specifikace minimálních požadavků
Podpora flow standardů	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Podpora VPC flow logů z AWS, Azure a GCP.
Streamové zpracovávání flow dat	Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií.
Otevřené rozhraní	Systém detekce anomálií poskytuje veřejně dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).
Deduplikace	Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.
Korelace před a za proxy	Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli.
Vzorkování na úrovni toků	Systém podporuje vzorkování na úrovni 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, multicast provozu a nestandardní komunikace.
Detekce nežádoucích aplikací	Detekce P2P sítí a VPN komunikace.
Detekce náhodných domén	Systém umožňuje detekovat závadnou komunikaci na základě rozlišení legitimních domén (druhé úrovně) od náhodně generovaných domén.

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 událostí	Detekované události musí být interpretovány v rámci MITRE ATT&CK taktik a technik.
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.
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.
Detekce TOR komunikace	Detekce použití TOR klientů v monitorované síti a detekce příchozí komunikace z TOR sítě na monitorované servery.
Analýza šifrovaného provozu použitím JA3 otisků	Systém umožňuje detekovat závadné komunikace monitorování JA3 otisků v síťovém provozu a jejich porovnáváním se seznamem známých závadných JA3 otisků.
Podpora MISP platformy	Systém lze napojit na MISP platformu a použít indikátory kompromitace (IoC) poskytované touto platformou k detekci závadných komunikací v monitorované síti.
Podpora MITRE ATT&CK frameworku a mapování na základě kontextu	Detekované události jsou mapovány na jednu nebo více MITRE ATT&CK taktik a technik pro poskytnutí širšího kontextu uživateli. Mapování je založeno na základě kontextové analýzy pro zajištění správného mapování taktiky a techniky na detekovanou událost. Stejný druh události tak může být mapován různě v závislosti na kontextu události nebo vývoji události v čase.

MITRE ATT&CK dashboard a vizualizace	Systém poskytuje dashboard pro vizualizaci MITRE ATT&CK matice, která zobrazuje počet událostí detekovaných v jednotlivých taktikách a technikách čímž umožňuje poskytnout přehled nad stávající bezpečností situací a zobrazit útoky v jejich různých fázích dle MITRE ATT&CK frameworku.
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.
Agregace událostí	Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.).
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.
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.

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.).
Výkon toků/s	Plugin pro automatické vyhodnocování netflow dat musí splňovat výkon minimálně 1000 toků/s
Záruka a servisní podpora	Požadujeme dodání pluginu pro automatické vyhodnocování vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.