# 9 Implementace nástroje pro monitorování toků

Cílem implementace technického opatření je dodávka systému, který zajistí detekci nestandartního chování uživatelů a aplikací, které komunikují na síťové úrovni. Smyslem je detekce nevhodně se chovajících aplikací a uživatelů a zejména pokročilého malware, který by mohl ohrozit privátnost, dostupnost a integritu aplikací Významného informačního systému, případně dalších informačních a komunikačních systémů.

## Schéma zapojení kolektoru a sond



## Požadavky na kolektor

| *Požadavek na funkcionalitu* | *Popis* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- | --- |
| Počet kusů | Je požadován jeden kus. | ANO |  |
| Kapacita úložiště | Je možné uložit až 12TB dat. | ANO |  |
| Ucelený, škálovatelný NetFlow/IPFIX monitorovací systém | Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků. | ANO |  |
| Podpora infrastruktury | Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s. | ANO |  |
| 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. | ANO |  |
| Nezávislost na stávající infrastruktuře | Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce). | ANO |  |
| 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) | ANO |  |
| 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). | ANO |  |
| Ukládání statistik a vyhodnocování bezpečnostních hrozeb | Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. | ANO |  |
| Zákaznická podpora | Plná zákaznická podpora v českém jazyce. | ANO |  |
| Rozhraní pro integraci nástrojů třetích stran | Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran. | ANO |  |
| Granularita vizualizace | Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v min. dvou časových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků. | ANO |  |
| 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. | ANO |  |
| Instalace | Snadná instalace do stávající síťové infrastruktury – racková montáž | ANO |  |
| Management rozhraní | Plnohodnotný fyzicky vyhrazený management (administrativní) port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. | ANO |  |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | ANO |  |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele, napojení na PIM/PAM systém. | ANO |  |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+. | ANO |  |
| Podpora HOT SWAP a RAID | Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce. | ANO |  |
| Dohled | Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP Součástí implementace bude zapojení do stávajícího PRTG monitorovacího systému. | ANO |  |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | ANO |  |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. | ANO |  |
| Sériová linka pro konfiguraci zařízení | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). | ANO |  |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | ANO |  |
| Podpora Cisco AVC | Podpora standardu Cisco AVC vč. položek HTTP hostname a URL. | ANO |  |
| Podpora dalších flow standardů | Podpora pro Cisco NSEL, Cisco NBAR2. | ANO |  |
| Podpora položek proměnlivé délky | Podpora IPFIX položek proměnlivé délky. | ANO |  |
| Podpora IPFIX rozšíření jiných výrobců | Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions. | ANO |  |
| Monitoring informací z aplikační vrstvy | Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS). | ANO |  |
| 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. | ANO |  |
| 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. | ANO |  |
| Přeposílání flow vč. převodu formátu | Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik. | ANO |  |
| 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. | ANO |  |
| 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). | ANO |  |
| 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). | ANO |  |
| Analýza dat a ad hoc výstupy | Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. | ANO |  |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. | ANO |  |
| Top N statistiky | Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. | ANO |  |
| 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). | ANO |  |
| 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. | ANO |  |
| Drill-down | Možnost dohledat každý jednotlivý datový tok (flow záznam). | ANO |  |
| Monitoring aktivních zařízení na sítí | Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, přihlášeného uživatele na daném zařízení. | ANO |  |
| Automatická podpora geolokace | Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). | ANO |  |
| Otevřené rozhraní | Kolektor poskytuje dokumentované API pro získávání a zpracování dat. | ANO |  |
| Monitorování dostupnosti zdroje flow dat | Monitorování dostupnosti zdroje flow dat pomocí SNMP. | ANO |  |

## Požadavky na sondu

| *Požadavek na funkcionalitu* | *Popis* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- | --- |
| Počet kusů | Jsou požadovány dva kusy hw sondy a osm virtuálních sond do vmware host prostředí. | ANO |  |
| Pasivní zapojení | Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). | ANO |  |
| Instalace | Snadná instalace do stávající síťové infrastruktury – racková montáž pro fyzické zařízení nebo šablony pro nasazení virtuálního stroje. | ANO |  |
| Management rozhraní | Plnohodnotný management (administrativní) port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. | ANO |  |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | ANO |  |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. | ANO |  |
| Dohled | Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. | ANO |  |
| Vestavěný kolektor | Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru. | ANO |  |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | ANO |  |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. | ANO |  |
| Sériová linka pro konfiguraci zařízení | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). | ANO |  |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | ANO |  |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+ | ANO |  |
| Podpora protokolů pro výměnu dat | Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX. | ANO |  |
| Zpracování datového provozu | Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. | ANO |  |
| Analýza tunelovaného provozu | Monitorování provozu v tunelu (deenkapsulace) GRE, ESP a OTV. | ANO |  |
| Monitorování MAC adres | Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. | ANO |  |
| Detekce aplikací | Detekce aplikací dle standardu NBAR2. | ANO |  |
| 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). | ANO |  |
| Profilování zařízení v síti | Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | ANO |  |
| 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). | ANO |  |
| Monitorování SMB/CIFS provozu | Monitorování a analýza SMB/CIFS. | ANO |  |
| 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). | ANO |  |
| Monitorování e-mailového provozu | Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP. | ANO |  |
| Monitorování MS SQL (TDS protokolu) provozu | Monitorování Microsoft SQL provozu (TDS protokolu). | ANO |  |
| Monitorování rozšířených L3/L4 informací | Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. | ANO |  |
| Nastavení času pro expiraci toků | Podpora pro nastavení časů u aktivní a neaktivní expirace toků. | ANO |  |
| Vzorkování | Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. | ANO |  |
| Vyplňování čísla interface | Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. | ANO |  |
| 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. | ANO |  |
| Monitorovací porty sond | HW sondy obsahujíminimálně 4x 10GbE optické monitorovací porty na zařízení. Virtuální sondy obsahují minimálně jedno 1GbE rozhranní. Optické SMFtransceivery pro obě strany připojení jsou součástí dodávky (za dvě sondy tedy 16x SFP+ SM). | ANO |  |

## Požadavky na systém automatického vyhodnocování NetFlow dat

| *Požadavek na funkcionalitu* | *Popis* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- | --- |
| Počet kusů | Je požadován jeden kus – minimální počet zpracování - 4000 toků za sekundu | ANO |  |
| Podpora flow standardů | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, | ANO |  |
| Deduplikace | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. | ANO |  |
| 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. | ANO |  |
| Identita uživatelů | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. | ANO |  |
| Persistence doménových jmen | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. | ANO |  |
| Detekční pravidla a algoritmy | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. | ANO |  |
| Detekce síťových útoků | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. | ANO |  |
| Detekce anomálií v síťovém provozu | Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. | ANO |  |
| Detekce nežádoucích aplikací | Detekce P2P sítí, a anonymizačních služeb (např. TOR) | ANO |  |
| 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. | ANO |  |
| Detekce provozních problémů | Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. | ANO |  |
| Detekce síťových anomálií | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. | ANO |  |
| Konfigurační průvodce | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. | ANO |  |
| 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). | ANO |  |
| 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.). | ANO |  |
| 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. | ANO |  |
| 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. | ANO |  |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. | ANO |  |
| SNMP Trap | Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. | ANO |  |
| 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. | ANO |  |
| Záchyt provozu v plném rozsahu | Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. | ANO |  |
| Uživatelské rozhraní | Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. | ANO |  |
| Integrace informací z jiných služeb | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP. | ANO |  |
| 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.). | ANO |  |
| Interaktivní vizualizace událostí | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. | ANO |  |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní. Automatická distribuce reportů e-mailem. | ANO |  |
| CSV export | Události je možné exportovat do formátu CSV pro další zpracování. | ANO |  |
| 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.). | ANO |  |
| 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. | ANO |  |

## Požadavky na systém pro záchyt síťového provozu

| *Požadavek na funkcionalitu* | *Popis* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- | --- |
| Počet kusů | Požadovány jsou dva kusy + centrální konzole | ANO |  |
| 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). | ANO |  |
| Architektura – distribuovaná | Systémem je možné rozšířit funkcionalitu sond. Systém se ovládá centrálně z kolektoru, který obsahuje webové rozhraní pro manuální zadávání požadavků na záchyt síťového provozu. Webové rozhraní kolektoru umožňuje definovat na jakých sondách a jejich monitorovacích rozhraních bude prováděn záchyt. | ANO |  |
| Architektura – all-in-one sonda | Systémem je možné rozšířit funkcionalitu sondy a zároveň ji vybavit webovým rozhraním pro manuální zadávání požadavků na záchyt síťového provozu. Webové rozhraní sondy umožňuje definovat, na jakých monitorovacích rozhraních sondy bude prováděn záchyt. | ANO |  |
| 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. | ANO |  |
| Filtrace a záchyt provozu podle parametrů linkové vrstvy (L2) | Systém umožňuje filtrovat síťový provoz podle VLAN tagu, MPLS značky. | ANO |  |
| Filtrace a záchyt provozu podle parametrů síťové vrstvy (L3) | Systém umožňuje filtrovat síťový provoz podle IPv4, IPv6 adresy, čísla sítě a masky. | ANO |  |
| Filtrace a záchyt provozu podle parametrů transportní vrstvy (L4) | Systém umožňuje filtrovat síťový provoz podle portů TCP, UDP a SCTP | ANO |  |
| Nahrávání VoIP provozu | Systém umožňuje filtrovat síťový provoz VoIP hovorů používající SIP a H.323 protokoly | ANO |  |
| Nastavení časového intervalu záchytu | Systém umožňuje pro jednotlivé záznamy definovat časový interval, ve kterém se bude síťový provoz zachytávat. | ANO |  |
| Správa přístupu k záznamům | Systém umožňuje při zadávání záznamu definovat skupinu uživatelů, která má přístup ke stažení záznamu. | ANO |  |
| Automatické spuštění záchytu provozu | Záchyt síťového provozu je možné spustit automaticky na základě detekce události systémem pro automatické vyhodnocování NetFlow dat. | ANO |  |
| Definice míst záchytu | Systém umožňuje definovat na jakých sondách a jejich monitorovacích rozhraních bude provádět záchyt síťového provozu. | ANO |  |
| 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. | ANO |  |
| Rotace dat | Automatická rotace starých dat pro uvolnění místa na disku pro nové záchyty síťového provozu. | ANO |  |

## Požadavky na systém pro monitorování výkonu aplikací

| *Požadavek na funkcionalitu* | *Popis* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- | --- |
| Počet kusů | Požadováno je osm kusů + centrální konzole | ANO |  |
| Uživatelské rozhraní | Vizualizuje stav aplikace pomocí indexu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožnuje analyzovat stav jednotlivých částí aplikace a transakcí. | ANO |  |
|  |  |  |  |
| Uživatelsky definovatelný dashboard | Uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů. Možnost přizpůsobení a vkládání vybraných widgetů uživatelem, např. index výkonu aplikace, 5 nejpomalejších transakcí, souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů). | ANO |  |
| Reporting odezvy aplikace | Systém reportuje pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací dobu odezvy aplikace a čas na transportní vrstvě. Díky tomu je možné odlišit zpoždění sítě od zpoždění aplikace. | ANO |  |
| Bez-agentní monitoring | Systém monitoruje aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice. | ANO |  |
| Transparentní monitoring | Systém monitoruje aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu. | ANO |  |
| Architektura systému | Systém je možné nasadit samostatně na jedné sondě, nebo na více sondách s centrální správou a webovým uživatelským rozhraním na kolektoru. | ANO |  |
| Monitoring na úrovni uživatel – aplikační server | Systém umožňuje monitorovat komunikaci mezi klienty aplikace a aplikační serverem na bázi protokolu HTTP a HTTPS. V případě použití protokolu HTTPS podporuje automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují. | ANO |  |
| Monitoring na úrovni aplikační server – databázový server | Systém umožňuje monitorovat komunikaci mezi aplikačními servery a databázovými servery Oracle , MSSQL, Postgre SQL, MySQL MariaDB. | ANO |  |
| Definice SLA a index výkonu aplikace | Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA. | ANO |  |
| Konfigurace aplikací | Systém nabízí flexibilní možnosti definice aplikace pro monitoring. | ANO |  |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Vizualizuje stav aplikace pomocí indexu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožnuje analyzovat stav jednotlivých částí aplikace a transakcí. | ANO |  |
| Uživatelsky definovatelný dashboard | Uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů. Možnost přizpůsobení a vkládání vybraných widgetů uživatelem, např. index výkonu aplikace, 5 nejpomalejších transakcí, souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů). | ANO |  |
| Reporting odezvy aplikace | Systém reportuje pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací dobu odezvy aplikace a čas na transportní vrstvě. Díky tomu je možné odlišit zpoždění sítě od zpoždění aplikace. | ANO |  |
| Bez-agentní monitoring | Systém monitoruje aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice. | ANO |  |
| Transparentní monitoring | Systém monitoruje aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu. | ANO |  |
| Architektura systému | Systém je možné nasadit samostatně na jedné sondě, nebo na více sondách s centrální správou a webovým uživatelským rozhraním na kolektoru. | ANO |  |
| Monitoring na úrovni uživatel – aplikační server | Systém umožňuje monitorovat komunikaci mezi klienty aplikace a aplikační serverem na bázi protokolu HTTP a HTTPS. V případě použití protokolu HTTPS podporuje automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují. | ANO |  |
| Definice SLA a index výkonu aplikace | Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA. | ANO |  |
| Konfigurace aplikací | Systém nabízí flexibilní možnosti definice aplikace pro monitoring. Minimálně v rozsahu IP adresy, porty, host, URL vč. regulárních výrazů pro jejich definici. | ANO |  |
| Korelace | Systém umožňuje korelovat zpoždění na úrovni uživatelské transakce na aplikačním serveru a transakce mezi aplikačním a databázovým serverem. Pro každou uživatelskou transakci je možné zobrazit SQL transakce, které byly v rámci uživatelské transakce vykonány. | ANO |  |
| Skupiny | Systém umožňuje definovat skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů). | ANO |  |
| Přepočítávání historických statistik | Systém přepočítává historické statistiky pro nově vytvořené skupiny. | ANO |  |
| Reporting | Systém umožňuje vytvářet reporty dostupné prostřednictvím webového GUI, ve formátu PDF. Reporty je možné automaticky odesílat e-mailem. | ANO |  |
| Notifikace | Jako reakci na snížení indexu výkonu aplikace, případně další metriky umožňuje systém odeslat e-mail, syslog zprávu, SNMP trap, nebo spustit skript. | ANO |  |
| Detaily HTTP transakcí | Pro každou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie. | ANO |  |
| Detaily databázových transakcí | Pro každou transakci jsou dostupné detaily minimálně v rozsahu SQL dotazu v plném rozsahu, velikost dotazu a odpovědi, typ SQL dotazu, čas vzniku dotazu i odpovědi a doba odezvy. | ANO |  |
| Filtrace agregovaných transakcí | Systém umožňuje filtrovat nad seznamem agregovaných transakcí pomocí kritérií (např. APM, index, počet chyb, celkový objem přenesených dat a další). Díky tomu lze získat informace o tom, jaké části aplikace jsou nejpomalejší, vykazují nejvíce chyb, atd. | ANO |  |
| Filtrace jednotlivých transakcí | Systém umožňuje filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu lze získat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná, atd. | ANO |  |
| CSV export | Systém umožňuje exportovat informace o transakcích ve formátu CSV. | ANO |  |
| Odvozené metriky | Systém sleduje další odvozené metriky jako je průměr, medián, 99-percentil a 95-percentil doby odezvy aplikace, zobrazuje přehled nejpomalejších transakcí, počet uživatelů souběžně pracujících s aplikací, počet transakcí dle splnění SLA, struktura chybových kódů. | ANO |  |