DataCentrum
medzi Vami a financiami

Cintorínska 5
814 88 B r a t i s l a v a

INFORMÁCIA O VÝSLEDKU VYHODNOTENIA PONÚK A PORADIE UCHÁDZAČOV

podľa § 55 ods. 2 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“)

Názov predmetu zákazky:
Systém na monitorovanie a analytiku siete, bezpečnostný sieťový monitoring (NDR)

Postup vo verejnom obstarávaní:
Zákazka zadávaná v rámci nadlimitného dynamického nákupného systému na predmet *Nákup hardvéru a/alebo podpory hardvérových produktov* (identifikátor zákazky v dynamickom nákupnom systéme: DNS096/HW)

Vyhlásenie verejného obstarávania:
Oznámenie o vyhlásení verejného obstarávania k zriadeniu predmetného dynamického nákupného systému bolo uverejnené v Úradnom vestníku EÚ dňa 17.04.2023 pod zn. 2023/S 075-227231 a vo Vestníku verejného obstarávania č. 77/2023 dňa 18.04.2023 pod zn. 14482 – MUT.

Poradie uchádzačov:

PČ uchádzača	Uchádzač	Kritérium na vyhodnotenie ponúk: **Najnižšia celková cena v EUR s DPH** Návrh na plnenie kritérií	Poradie uchádzača
1	**AUREUS + a. s.** Tomášikova 19081/28D Bratislava - mestská časť Ružinov 821 01 IČO: 50854402	391 755,00	1.
2	**XXX** XXX XXX IČO: XXX	393 089,88	2.

Identifikácia úspešného uchádzača:
AUREUS + a. s.
Tomášikova 19081/28D
Bratislava - mestská časť Ružinov 821 01
IČO: 50854402
(ďalej len „úspešný uchádzač“)

Dôvod úspešnosti ponuky:
Verejný obstarávateľ určil poradie uchádzačov na základe kritéria na vyhodnotenie ponúk určeného vo výzve, ktoré je objektívne, nediskriminačné, podporujúce čestnú hospodársku súťaž a na základe

predložených ponúk. Verejný obstarávateľ vyhodnotil ponuku predloženú úspešným uchádzačom z hľadiska jej súladu so všetkými požiadavkami verejného obstarávateľa určenými v oznámení o vyhlásení verejného obstarávania, v súťažných podkladoch, vo výzve a v iných dokumentoch potrebných na vypracovanie ponuky ako celku a z pohľadu splnenia všetkých požiadaviek verejného obstarávateľa obsiahnutých vo vyššie uvedených dokumentoch, a to všetko vo vzťahu a v záujme naplnenia základného cieľa verejného obstarávania – získať za vynaložené prostriedky najlepšiu a najvýhodnejšiu ponuku.

Ponuka úspešného uchádzača bola predložená v súlade so všetkými požiadavkami verejného obstarávateľa a splnila všetky požiadavky verejného obstarávateľa určené v oznámení o vyhlásení verejného obstarávania, v súťažných podkladoch, vo výzve a v iných dokumentoch potrebných na vypracovanie ponuky. Verejný obstarávateľ pri vyhodnocovaní ponúk dodržal všetky princípy verejného obstarávania, najmä princíp nediskriminácie hospodárskych subjektov, rovnakého zaobchádzania, hospodárnosti a transparentnosti a prijatím ponuky úspešného uchádzača získa verejný obstarávateľ za vynaložené prostriedky najlepšiu ponuku. Ponuka úspešného uchádzača je v súlade so všetkými požiadavkami, kvalitatívnymi a kvantitatívnymi parametrami a náležitosťami uvedenými vo výzve.

Verejný obstarávateľ skonštatoval, že ponuka úspešného uchádzača spĺňa požiadavky na predmet zákazky, nakoľko úspešný uchádzač ako plnenie zodpovedajúce predmetu zákazky predložil tovary spĺňajúce definované parametre nasledovne:

Parameter	Popis parametru (vlastnosti)	Vlastný návrh plnenia
Názov	**Systém na monitorovanie a analytiku siete, bezpečnostný sieťový monitoring (NDR)**	
Funkcia	Ucelené škálovateľné riešenie na dlhodobé monitorovanie siete. Monitorovací systém musí umožňovať dlhodobé detailné monitorovanie všetkej prevádzky na počítačovej sieti. Získané štatistiky o prevádzke dátovej siete musí umožniť v reálnom čase sledovať a vyhodnocovať objemy a štruktúru prevádzky, analyzovať príčiny prevádzkových alebo výkonnostných problémov na strane siete až po používateľov a jednotlivé aplikácie, odhaľovať vnútorné a vonkajšie neznáme bezpečnostné hrozby a anomálie na základe analýzy chovania siete. Je nevyhnutné, aby monitorovací systém bol úplne nezávislý od použitej sieťovej infraštruktúry a svojou funkciou monitorovanú sieť neovplyvňoval. Zo strany sledovanej siete nesmie byť monitorovací systém detekovateľný.	Ponúkané riešenie predstavuje ucelený, škálovateľný systém na dlhodobé monitorovanie sieťovej prevádzky a bezpečnostnú analytiku (NDR). Systém umožňuje pasívny zber sieťovej prevádzky, generovanie a analýzu dátových tokov (NetFlow/IPFIX), vizualizáciu, koreláciu prevádzkových a bezpečnostných udalostí, analýzu výkonnostných problémov až na úroveň používateľov a aplikácií a detekciu vnútorných aj vonkajších neznámych bezpečnostných hrozieb na základe správania siete. Riešenie je úplne nezávislé od sieťovej infraštruktúry, pracuje výhradne s kopírovanou prevádzkou (SPAN/mirror porty), monitorovanú sieť neovplyvňuje a zo strany siete nie je detekovateľné. https://www.progress.com/flowmon
Sieťový senzor/sonda	3 x senzor/sonda s pasívnym zapojením bez vplyvu na monitorovanie sieť (SPAN / mirror portami) v HW prevedení 1U	Ponúkané riešenie obsahuje 3 hardvérové sieťové senzory v 1U prevedení, zapojené pasívne prostredníctvom SPAN / mirror portov: 1× Progress Flowmon Probe 20000 PRO SFP+, PN: FM-PRB-HW-PRO-20000-SFP+

		2× Progress Flowmon Probe 4000, PN: FM-PRB-HW-STD-4000-CU https://www.progress.com/docs/default-source/flowmon-resources/2025-11-flowmon_probe_specification.pdf?sfvrsn=b7d1fab4_112
	Manažment rozhranie: min. 1 x (administratívne) porty 10/100 / 1000Mb / s pre zabezpečenú vzdialenú správu a prenos NetFlow dát dohľad a konfigurácia - SSH, HTTPS pre každý senzor/sondu	Každý senzor disponuje samostatným manažment rozhraním 10/100/1000 Mb/s pre zabezpečenú vzdialenú správu, dohľad a konfiguráciu. Podporované protokoly: SSH, HTTPS, prenos NetFlow/IPFIX dát.
	1 x senzor/sonda s 2x10/25Gbps optickým monitorovacím portom , výkon min. 14,48 Mp/s (milión paketov za sekundu) na monitorovací port (vrátane 2x 10Gb/2x25Gb baseSFP+ transceiver fiber multimode, 850nm, 300m), spracovanie min.50.000 Fps (dátových tokov za sekundu), kapacita interného NetFlow úložiska min. 1TB	Požiadavka je splnená zariadením Progress Flowmon Probe 20000 PRO SFP+, PN: FM-PRB-HW-PRO-20000-SFP+. 2× SFP+/SFP28 monitorovací port (10Gb/25Gb) Výkon: ≥ 14,48 mil. paketov/s na port Spracovanie: ≥ 50 000 flow/s Interné NetFlow úložisko: ≥ 1 TB Dodané transceivery: 2× 10GBase-SR SFP+, MM, 850 nm, PN: FM-ACC-HW-10G-SFP-SR 2× 25GBase-SR SFP28, MM, 850 nm, PN: FM-ACC-HW-25G-SFP28-SR
	2 x senzor/sonda s 4x1Gbps monitorovacím metalickým portom , výkon min. 1,48 Mp/s (milión paketov za sekundu) na monitorovací port, spracovanie min.50.000 Fps (dátových tokov za sekundu), kapacita interného NetFlow úložiska min. 1TB	Požiadavka je splnená zariadeniami 2× Progress Flowmon Probe 4000, PN: FM-PRB-HW-STD-4000-CU. 4× 1GbE metalický monitorovací port Výkon: ≥ 1,48 mil. paketov/s na port Spracovanie: ≥ 50 000 flow/s Interné NetFlow úložisko: ≥ 1 TB
	Senzory musia spracovávať kopírovanú sieťovú prevádzku a následne generovať informácie o dátových tokoch v rozsahu min NetFlow v5, NetFlow v9 a IPFIX	Senzory spracovávajú kopírovanú sieťovú prevádzku a generujú dátové toky v rozsahu NetFlow v5, NetFlow v9 a IPFIX.
	Senzory musia umožňovať integráciu do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov pomocou SNMP	Senzory umožňujú integráciu do dohľadových systémov prostredníctvom SNMP pre kontrolu dostupnosti a vyťaženia zdrojov.
	Senzory musia umožňovať vzorkovanie na úrovni paketov a na úrovni dátových tokov	Senzory umožňujú vzorkovanie: • na úrovni paketov, na úrovni dátových tokov.
Monitoring a uchovávanie dátových tokov	Systém musí podporovať vizualizáciu a spracovanie dátových tokov / paketov v 5-minútových, 1-minútových alebo 30-sekundových intervaloch	Systém podporuje vizualizáciu a spracovanie dát v intervaloch 30 sekúnd, 1 minúta a 5 minút.

	Systém musí podporovať spracovanie štandardov dátových tokov v rozsahu min. NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite a ich zber z desiatok zdrojov v sieti	Systém podporuje spracovanie NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite a zber z desiatok zdrojov.
	Systém musí umožniť dohľadanie ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty, databázy aktívnych zariadení na sieti vr. identifikácii zariadení.	Systém umožňuje dohľadanie ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty a databázu aktívnych zariadení vrátane ich identifikácie.
	Systém musí umožniť konfiguráciu pomocou dostupných konfiguračných šablón a ich aplikáciou vytvárať profily, kapitoly, reporty, widgety a dashboardy bez nutnosti manuálnej konfigurácie.	Systém umožňuje konfiguráciu pomocou preddefinovaných šablón a vytváranie profilov, reportov, widgetov a dashboardov bez nutnosti manuálnej konfigurácie.
	Systém na uchovávanie a monitoring dátových tokov musí mať kapacitu dátového úložiska: Min 12TB pre uchovávanie štatistík o sieti v rozsahu min 6 mesiacov a musí byť schopný spracovať min. 200.000 dátových tokov za sekundu o virtuálnom prevedení ako šablóna do VmWare, Hyper-V alebo KVM	Požiadavka je splnená zariadením Progress Flowmon Collector 12000 VA, PN: FM-COL-VA-12000. Kapacita úložiska: ≥ 12 TB Retencia: ≥ 6 mesiacov Výkon: ≥ 200 000 flow/s Virtuálne prevedenie: VMware, Hyper-V, KVM https://www.progress.com/docs/default-source/flowmon-resources/2025-11-flowmon_collector_specification.pdf
	Zariadenie musí umožňovať integráciu do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov pomocou SNMP	Collector umožňuje integráciu do dohľadového systému prostredníctvom SNMP.
	Systém musí poskytovať manažment rozhranie min. 1 x (administratívne) port 10/100 / 1000Mb / s pre zabezpečenú vzdialenú správu a prenos a preposielani Flow/IPFIX dát, a to aj v šifrovanej forme pri podpore protokolu TLS podľa štandardu RFC 7011 a vzdialenou správou prostredníctvom SSH a HTTPS	Systém poskytuje manažment rozhranie 10/100/1000 Mb/s, podporuje šifrovaný prenos Flow/IPFIX dát pomocou TLS (RFC 7011) a vzdialenú správu cez SSH a HTTPS.
	Systém musí vizualizovať štatistické údaje podľa objemu (min . počet prenesených bytov, tokov, paketov), IP prevádzky (min. TCP, UDP, ICMP, ostatné) alebo protokolu (min. HTTP, IMAP, SSH), vrátane plnej konfigurácie grafov a pohľadov užívateľom	Systém vizualizuje štatistiky podľa objemu, IP prevádzky, protokolov a umožňuje plnú konfiguráciu grafov a pohľadov používateľom.
	Systém musí umožňovať autentizáciu voči LDAP (Active Directory) a časovú synchronizáciu zariadenia proti centrálnemu zdroju času na sieti.	Systém podporuje autentizáciu voči LDAP / Active Directory a synchronizáciu času s centrálnym časovým zdrojom.
	Systém by mal mať možnosť využitia DNS cache na zariadení pre rýchlejší preklad IP adries na doménové mená.	Systém podporuje využitie DNS cache pre rýchlejší preklad IP adries.

	Systém musí byť schopný monitoringu rozšírených L3 / L4 informácií - TTL (Time to live), TCP Window size, TCP SYN, MAC adries vo flow štatistikách, spracovať dátovú prevádzku min.v rozsahu IPv4 a IPv6, VLAN, MPLS, AS, HTTP, HTTPS (SNI) VoIP,DNS, DHCP,SMB / CIFS a emailovej komunikácie	Systém monitoruje TTL, TCP Window size, TCP SYN, MAC adresy, IPv4/IPv6, VLAN, MPLS, AS, HTTP/HTTPS (SNI), VoIP, DNS, DHCP, SMB/CIFS a e-mailovú komunikáciu.
	Systém musí umožňovať analýzu dát oneskorenia na sieti v rozsahu min. RTT, SRT, delay, jitter, retransmisiu, out-of-order pakety ako súčasť flow štatistík a zároveň podporovať analýzu CISCO AVC	Systém podporuje analýzu RTT, SRT, delay, jitter, retransmisie, out-of-order pakety a Cisco AVC.
	Systém musí umožňovať monitoring aktívnych zariadení na sieti a viditeľnosť do šifrovanej komunikácie SSL/TLS bez nutnosti jej dekryptovania	Systém poskytuje viditeľnosť do SSL/TLS komunikácie bez nutnosti dekryptovania.
	Systém musí byť schopný monitoringu možných využívaných externých cloudových služieb (MS Azure, AWS, GPC) s podporou end-to-end visibility dátovej komunikácie	Systém monitoruje komunikáciu s cloudovými službami Microsoft Azure, AWS, Google Cloud s end-to-end viditeľnosťou.
	Systém musí obsahovať centrálny dashboard s možnosťou zdieľania vybraných widgetov, preddefinovaných widgetov pre rôzne náhľady a možnosti tvorby vlastných widgetov a prístup do systému musí byť realizovaný HTTPS webovou aplikáciou (GUI)	Systém obsahuje centrálny dashboard s možnosťou zdieľania widgetov, tvorby vlastných pohľadov a prístupom cez HTTPS GUI.
	Systém musí podporovať multitenancie pre správu systému internými, ale aj externými používateľmi s oddelenými rolami a prístupom do systému	Systém podporuje multitenantné prostredie s oddelenými rolami a prístupmi.
	Systém musí umožnovať vizualizáciu monitorovaných liniek a prepojov a sieťovej topológie	Systém umožňuje vizualizáciu monitorovaných liniek, prepojov a sieťovej topológie.
Automatizované spracovávanie a detekciu anomálií a hrozieb na sieti	Systém musí automatizovane vyhodnocovať dátové toky a detegovať anomálie na sieti s podporou deduplikácie, vzorkovania na úrovni tokov, identity používateľov a persistencii doménových mien	Požiadavky sú splnené modulom Progress Flowmon ADS Corporate, PN: FM-ADS-SW-C-SUB (3 roky). Systém automatizovane vyhodnocuje dátové toky, deteguje anomálie, interpretuje ich formou udalostí s mapovaním na MITRE ATT&CK, podporuje strojové učenie, heuristiku a streamové spracovanie dátových tokov. https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf Flowmon APM Corporate, PN: FM-APM-SW-C-SUB – aplikačný monitoring, SLA, HTTP/HTTPS, SQL https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf

		Flowmon Packet Investigator Business, PN: FM-FPI-SW-B-SUB – forenzná analýza, PCAP https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí interpretovať anomálie vo forme udalostí s detailnými informáciami pre analytikov až do úrovne jednotlivých spojení dátových tokov s vizualizácie v min. rozsahu podľa MITTRE ATT&CK techník a taktík, podľa zariadení a v agregovanom časovom pohľade	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Architektúra systému musí umožňovať streamové spracovávanie dátových tokov v min. rozsahu 20000 dátových tokov za sekundu pre rýchlu detekciu bezpečnostných alebo prevádzkových anomálií.	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí obsahovať minimálne túto sadu detekčných metód v prednastavenom režime s podporou využitia princípov strojového učenia, heuristiky, porovnávania vzorcov správania sa zariadení, používateľov a sieťovej komunikácie na sieti a heuristiky: Detekcia skenovanie portov, slovníkové útoky, útoky odopretia služieb (DoS), supply chain útoky, malware, ransomware a cryptojacking. Detekcia útokov na sieťové protokoly SSH, RDP, Telnet. Detekcia anomálií v DNS vrátane DoH, DHCP, SMTP a neštandardnej komunikácie. Detekcia P2P sietí, podvrhnutých doménových mien, VPN služieb a anonymizačných služieb (napr. TOR nódy). Detekcia nadmernej záťaže siete, nových a cudzích zariadení pripojených k sieti, výpadkov služieb, chýbajúcich reverzných DNS záznamov. Detekcia NAT.	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43

	Systém musí poskytovať tzv. Threat Inteligence napojenie a obohatienie detekovaných anomálií - identifikácia bezpečnostných udalostí (napr. komunikáciu s botnet command & control centrom, prístup na phishingové servery, apod.) využívaním zdrojov IP a host reputačných databáz poskytovaných výrobcom a aktualizovaných najmenej každých 6 hodín. Systém musí umožniť zapojiť ďalšie zdroje IP a host reputačných dát pre automatickú detekciu z CSV alebo MISP	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí umožňovať automatizované plnenie feedov zo správ na internete ohľadom spravodajstva o externých hrozbách a to vo forme prehľadného dashboardu a zároveň konvertovať IoC z týchto správ na jednotlivé detekčné metódy	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém monitoruje aplikácie bez nutnosti inštalovať akýkoľvek SW na servery alebo klientské stanice v úrovni min. 500 aplikačných transakcií za sekundu.	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém umožňuje monitorovať komunikáciu medzi klientmi aplikácie a aplikačné serverom na báze protokolu HTTP a HTTPS a komunikáciu medzi aplikačnými servermi a databázovými servermi Oracle alebo MSSQL a zároveň tiet oinformácie korelovať v rozsahu oneskorenia na úrovni užívateľské transakcie na aplikačnom serveri a transakcie medzi aplikačným a databázovým serverom. Pre každú používateľskú transakciu je možné zobraziť SQL transakcie, ktoré boli v rámci užívateľskej transakcie vykonané.	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém umožňuje pre každú aplikáciu, resp. aj jej časť definovať SLA pre dobu odozvy. Systém kontinuálne vyhodnocuje všetky transakcie a stanovuje celkový index výkonu aplikácie na základe	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-

	plnenia SLA.	source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Pre každú transakciu aplikácie sú dostupné detaily minimálne v rozsahu URL, parametre, user agentov, objem prenesených dát, návratová hodnota, cookie, SQL dotazu v plnom rozsahu, veľkosť dotazu a odpovede, typ SQL dotazu, čas vzniku dopytu i odpovede a doba odozvy.	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí obsahovať funkcionalitu IDS (Intrusion Detection System) agregovanú pre každú detekovanú anomáliu s interpretáciou signatúr v rámci danej udalosti pre identifikáciu známeho škodlivého kódu, alebo zraniteľnosti systému (CVE)	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí umožňovať vizualizáciu priebehu sieťovej prevádzky s vyznačením detegovaných udalostí v závislosti od nastavenej závažnosti udalostí (severity) v čase a to aj sútne do minulosti v rozsahu min 6 mesiacov	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí umožniť SOC operátorovi vytvárať vlastné aplikovateľné detekčné metódy nad rámec vstavaných metód napr. na báze jednoduchého SQL syntaxu a musí umožniť konfigurovať citlivosť detekčných metód až do úrovne jednotlivých inštancií v rámci rôznych segmentov siete	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-

		source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
	Systém musí umožňovať analýzu šifrovanej komunikácie pre potreby detekcie bezpečnostných hrozieb v šifrovanej prevádzke a podporu manažment politík používaných šifrovacích mechanizmov	https://www.progress.com/docs/default-source/flowmon-resources/flowmon-ads-cz.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_apm_specification.pdf https://www.progress.com/docs/default-source/flowmon-resources/2024-12-flowmon_packet_investigator_specification.pdf?sfvrsn=a74a8f26_43
Odozva na bezpečnostné udalosti na sieti	Prípadné udalosti, ktoré predstavujú falošné poplachy (false positives) je možné odstrániť prostredníctvom jednoduchej konfigurácie pravidiel vylúčenia falošných poplachov dostupné v používateľskom rozhraní.	Systém podporuje: • potláčanie false positives, • export udalostí cez Syslog (CEF), • SNMP trap, e-mail notifikácie, • REST API, on-demand PCAP záchyt spätne v čase.
	Udalosti je možné automaticky exportovať min. vo formáte Syslog (CEF) . Predpokladané využitie tejto funkcionality je integrácia so systémami typu SIEM, SOAR, EDR/XDR alebo LMS (log management system)	Systém podporuje: • potláčanie false positives, • export udalostí cez Syslog (CEF), • SNMP trap, e-mail notifikácie, • REST API, on-demand PCAP záchyt spätne v čase.
	Udalosti musí byť možné reportovať do dohľadových systémov prostredníctvom funkcionality SNMP trap	Systém podporuje: • potláčanie false positives, • export udalostí cez Syslog (CEF), • SNMP trap, e-mail notifikácie, • REST API, on-demand PCAP záchyt spätne v čase.
	Notifikácia o detekovaných udalostiach musí byť realizovaná min. prostredníctvom e-mailu s podporou rôznych formátov (HTML, incident handling systém, úsporný textový formát) a musí umožňovať pripojiť vzorku dátových tokov, na základe ktorých bola udalosť detekovaná k emailovému reportu	Systém podporuje: • potláčanie false positives, • export udalostí cez Syslog (CEF), • SNMP trap, e-mail notifikácie, • REST API, on-demand PCAP záchyt spätne v čase.
	Systém musí poskytovať dokumentované RestAPI pre získavanie, odosielanie a spracovanie udalostí. Prostredníctvom RestAPI je možné systém detekcie anomálií takisto konfigurovať (napr. vytvárať filtre, meniť nastavenia detekčných metód, apod.).	Systém podporuje: • potláčanie false positives, • export udalostí cez Syslog (CEF), • SNMP trap, e-mail notifikácie, • REST API, on-demand PCAP záchyt spätne v čase.

	Systém musí reagovať na výskyt anomálnej udalosti formou automatizovaného záchytu prevádzky v plnom rozsahu (on demand full packet capturing) vo formáte PCAP na základe užívateľom definovaného pravidla záchytu a musí tento záchyt vykonať v čase spätne podľa definovaných pravidiel, nie len v čase, kedy bola anomálna udalosť detegovaná	Systém podporuje: • potláčanie false positives, • export udalostí cez Syslog (CEF), • SNMP trap, e-mail notifikácie, • REST API, on-demand PCAP záchyt spätne v čase.
Služby spojené s inštaláciou	Požaduje sa v rámci inštalácie dodať zariadenia, umiestniť ich v mieste dodania, zrealizovať základné spustenie, otestovať funkčnosti komponentov	Inštalácia, konfigurácia, testovanie
Servisná podpora	Nepretržitá podpora v režime 24 hodín denne 7 dní v týždni s garantovanou dobou hardvérovej opravy do 24 hodín, po dobu 36 mesiacov od odovzdania, pričom oprava aj výjazd technika na opravu je pokrytý touto podporou. Oprava zariadenia musí byť realizovaná priamo výrobcom, alebo jeho lokálnym autorizovaným servisným partnerom (zastúpením). Počas doby podpory musí byť poskytnutý prístup k aktuálnym verziám strojových kódov a k aktuálnym verziám licenčného softvéru, ktorý tvorí neoddeliteľnú súčasť ponúkaných zariadení. Požaduje sa realizovať pravidelne 1 krát za kalendárny štvrťrok aktualizáciu strojového kódu a softvéru zariadení.	• Podpora 24×7, HW oprava do 24 hodín • Doba podpory: 36 mesiacov Pravidelné aktualizácie firmware a softvéru