Příloha č. 4 Podrobná specifikace položek

Položka	Předmět	Ks
1A	**Kolektor logů síťových sond pro analýzu bezpečnostních vzorů a indcidentů v předmětu Bezpečnosti technologie**	**1**

F	**Kolektor logů síťových sond pro analýzu bezpečnostních vzorů a indcidentů v předmětu Bezpečnosti technologie**		Flowmon colector IFP-R5 1000
Počet kusů:	1		
Minimální konfigurace:	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. Minimální kapacita systému 900 GB. 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. 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. Podpora LDAP a TACACS+. Podpora HOT SWAP a RAID. 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 flow standardů: Cisco AVC, 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. Přeposílání flow vč. možnosti samplingu a převodu formátu: Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik. Spolehlivý a šifrovaný přenos IPFIX dat: Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 5153 Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. 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. 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). 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 v grafech provozu. 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. 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). 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). 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. 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.). Možnost dohledat každý jednotlivý datový tok (flow záznam). 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. Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). Monitorování dostupnosti zdroje flow dat pomocí SNMP.		Dodávané řešení splňuje veškeré požadované technické specifikace
	Kompatibilita:	s majetkem UJEP ev. číslo: 1002909 (FLOWMON Probe 400 CU)	Dodávané zařízení je s uvedeným zařízením kompatibilní
	Záruka:	min. 24 měsíců zásahem technika u zákazníka	Dodávané zařízení tuto podmínku splňuje