SYSTÉM PRO MONITOROVÁNÍ SÍŤOVÉHO PROVOZU
- technická specifikace

ZÁKLADNÍ POŽADAVKY NA DODÁVKU A IMPLEMENTACI

Předmětem plnění veřejné zakázky (VZ) je dodávka a implementace Systém pro monitorování síťového provozu VŠPJ, spočívající v nasazení řešení pro provozní, výkonnostní a bezpečnostní monitoring síťového provozu v hybridním prostředí s pokročilými analytickými funkcemi.

Plnění VZ bude obsahovat tyto základní komponenty a parametry:

1) 1 ks monitorovací sonda s kapacitou 2x10Gbps (rozhraní SFP+) ve formě hardware appliance
2) 1 ks kolektor s výkonem až 75 000 flows/s a kapacitou úložiště až 1TB ve formě virtuální appliance
3) Systém pro automatické vyhodnocování a bezpečnostní analýzu síťového provozu

- Všechny dodávané komponenty budou dodány včetně veškerého software a licencí potřebných k jejich provozu
- Součástí dodávky bude kompletní nastavení, implementace a instalace dodávaných komponent a software do stávající infrastruktury zadavatele (nutná kompatibilita se stávajícím řešením Progress Flowmon), včetně zaškolení obsluhy
- Součástí dodávaného řešení bude záruka a podpora výrobce na všechny dodávané komponenty, včetně veškerého dodávaného potřebného software, po dobu minimálně 60 měsíců.
- Podléhají-li některé z dodávaných komponent či software časově omezenému licencování, musí být dodáno jeho předplatné v délce trvání min. 60 měsíců

Pro jednotlivé části nabízeného plnění požaduje zadavatel doložení příslušných dokumentů (technická specifikace, datový list, uživatelská dokumentace) pro ověření požadovaných funkčních vlastností a technických parametrů.

Uchazeč předloží **jako součást nabídky** tuto dokumentaci ve formátu PDF v českém nebo anglickém jazyce.

MINIMÁLNÍ TECHNICKÉ POŽADAVKY KOMPONENT SYSTÉMU

1) Monitorovací sonda (generátor flow)

- rack mount zařízení – max. velikost 1RU
- 2× 10 GbE monitorovací port typu SFP+, včetně osazených SFP+ modulů SM
- minimální výkon 1,5M paket/s na každém portu
- nezávislý autonomní zdroj NetFlow (v5, v9) a IPFIX statistických dat s podporou IPv4, IPv6, VLAN, MPLS, GRE, VxLAN, ESP
- detekce aplikací dle standardu NBAR2, monitorování a analýza MAC adres, HTTP provozu (včetně položek URL, hostname), VoIP statistik (jiter, zpoždění, ztráta paketů), DNS provozu, DHCP, HTTP, SMTP, Samba a MSSQL
- pasivní zapojení bez vlivu na monitorovanou síť (prostřednictvím SPAN portu aktivních zařízení)
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS
- správa uživatelů a přístupových práv na zařízení
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- instalace a nastavení zařízení prostřednictvím příkazové řádky
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména
- podpora autentizace vůči LDAP (Active Directory)
- podpora pro nastavení časů u aktivní a neaktivní expirace toků
- podpora vzorkování na úrovni paketů
- podpora vzorkování na úrovni toků
- podpora filtrování dat na základě IP prefixů a VLAN
- podpora vyplňování AS na základě vestavěného či dodaného seznamu
- podpora filtrování a export datových toků na základě AS

2) Kolektor

- kolektor NetFlow statistických dat ve formě virtuální appliance (Vmware/Hyper-V) pro ukládání síťových statistik
- Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite
- podpora úložiště o velikosti minimálně 1 TB
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS
- víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup
- podpora autentizace vůči LDAP (Active Directory)
- integrace dohledového systému pro kontrolu dostupnosti (SNMP)
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- instalace a nastavení zařízení prostřednictvím příkazové řádky
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména
- ukládání síťových statistik bez jakékoliv redukce
- 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, rozšiřitelnost o pluginy na míru
- analýza HTTP provozu - včetně položek typu URL, hostname

- analýza VoIP statistik (jitter, latence, ztrátovost), podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace DNS provozu, DHCP, HTTP, SMTP, Samba a MSSQL včetně obsahu daného dotazu
- drill-down – možnost dohledat každý jednotlivý zaznamenaný tok
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD
- podpora geolokace na základě IP adresy
- otevřené API rozhraní s možnostmi skriptování a zpracování dávkových úloh
- webové uživatelské rozhraní v českém jazyce

3) Systém pro vyhodnocení a bezpečnostní analýzu

Systém pro automatické vyhodnocování IP toků a detekci anomálií na základě behaviorální analýzy, aby bylo sledováno a vyhodnocováno nestandardní chování a anomálie na úrovni datové sítě:

- zpracovávání flow dat minimálně 1000 toků za vteřinu
- otevřené API rozhraní pro získávání a zpracování událostí. Prostřednictvím API je možné systém též konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).
- systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií.
- detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.
- detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.
- identifikace 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 24hodin. možnost zapojit další zdroje IP a host reputačních dat pro automatickou detekci.
- detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti.
- 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.).
- veškerá funkcionalita detekce anomálií musí být založena na vyhodnocování flow dat bez nutnosti paketové analýzy, např. nasazení speciálních senzorů výrobce, systém nevyžaduje viditelnost na úrovni zrcadlení provozu.
- zobrazení informace o identitě uživatelů obsaženou ve flow datech jako součást události.
- podpora persistence doménových jmen, tedy uložení doménového jména původce události v okamžiku zaznamenání výskytu této události.
- správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí.