TECHNICKÁ SPECIFIKACE

Název veřejné zakázky	**Software pro síťový monitoring a detekci anomálií**
Zadavatel	Zdravotnická záchranná služba Královéhradeckého kraje, Hradecká 1690/2A, 500 12 Hradec Králové, IČ: 48145122
Druh řízení	Veřejná zakázka malého rozsahu II. kategorie - na dodávky

Základní technické parametry:

Řešení musí zahrnovat funkce pro automatické detekce útoků, hrozeb a síťových anomálií. Systém musí umět pracovat s technologií NetFlow ve verzi 5, 9 a IPFIX.

1) Sondy (generátory flow) – pro 2 lokality s infrastrukturou VMware á 2 ESX uzly:

- 100% přesný nezávislý autonomní zdroj NetFlow a IPFIX statistik s podporou IPv4, IPv6, VLAN, MPLS, GRE, ERSPAN, VxLAN, ESP a VoIP,
- 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, MySQL, PostgeSQL, klientského TLS, certifikátů TLS,
- pasivní zapojení bez vlivu na monitorovanou síť (prostřednictvím SPAN portu aktivních zařízení),
- podpora filtrování dat na základě IP prefixů a VLAN,
- podpora vzorkování na úrovni paketů,
- podpora vzorkování na úrovni toků,
- podpora pro nastavení časů u aktivní a neaktivní expirace toků,
- podpora vyplňování AS na základě vestavěného či dodaného seznamu,
- podpora filtrování a export datových toků na základě AS,
- snadná instalace do stávající síťové infrastruktury,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232),
- dva administrativní porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu,
- podpora autentizace vůči LDAP (Active Directory),
- správa uživatelů a přístupových práv na zařízení,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména,
- časová synchronizace zařízení proti centrálnímu zdroji času na síti.

2) Kolektor (společný pro obě lokality):

- zabezpečený kolektor NetFlow statistik s databází pro plné uložení síťových statistik o velikosti minimálně 500 GB,
- možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru,
- drill-down – možnost dohledat každý jednotlivý zaznamenaný tok,
- schopnost ukládání síťových statistik bez jakékoliv redukce,
- 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, MSSQL, MySQL, PostgreSQL, včetně obsahu daného dotazu a IOT (Internet of thinks) jako jsou např. goos, mms, dlms a coap,
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD,
- podpora geolokace na základě IP adresy,
- integrace dohledového systému pro kontrolu dostupnosti (SNMP),
- otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh,
- snadná instalace do stávající síťové infrastruktury,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232),

- dva administrativní porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- podpora autentizace vůči LDAP (Active Directory),
- víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména,
- časová synchronizace zařízení proti centrálnímu zdroji času na síti.

3) Bezpečnostní analýza:

Součástí kolektoru musí být také nástroj pro automatickou detekci anomálií na základě behaviorální analýzy, který bude sledovat a vyhodnocovat nestandardní chování a anomálie na úrovni datové sítě a to zejména:

- útoky na síťové služby s cílem získat neoprávněný přístup k zařízení nebo službě,
- podpora pro jednu instanci vyhodnocování dat a výkon pro analýzu alespoň 5000 toků za vteřinu,
- komunikaci s potenciálně nežádoucími IP adresami, mezi které patří stanice šířící malware, botnet comman & control centra, známí útočníci nebo systémy šířící nevyžádanou poštu,
- anomálie DNS provozu indikující infikované stanice, nežádoucí software nebo chybné konfigurace,
- anomálie DHCP provozu indikující stanice pokoušející se o odposlech síťové komunikace nebo chybné konfigurace,
- skenování portů a další projevy infikovaných stanic nebo nežádoucího software,
- potenciálně nežádoucí síťové aplikace jako jsou P2P sítě nebo on-line komunikátory,
- anonymizační služby jako např. TOR (The Onion Router) s cílem obcházet bezpečnostní opatření a přistupovat na zablokované webové stránky, obcházení PROXY serveru,
- výpadky síťových služeb a špatné konfigurace síťových služeb,
- pohyb dat z interní sítě do internetu, tj. potenciální únik dat a využívání služeb pro výměnu dat na internetu (webová úložiště apod.),
- útoky na internetovou telefonii, ústředny a přístroje připojené do IP sítě,
- nestandardní poštovní komunikace a síření nevyžádané pošty.

4) Podpora:

Součástí dodávky řešení musí být garantovaná podpora ze strany výrobce či dodavatele zejména:

- dostupnost vzdálené pomoci (např. telefon, e-mail) v rozsahu minimálně 5x8 hodin,
- aktualizace reputační databáze pro přesnější detekci infikovaných stanic nebo odhalení nežádoucí komunikace s o hledem na nejnovější hrozby,
- možnost získání Updatu či Upgradu řešení bez dalších nákladů po celou dobu podpory,
- doba trvání podpory minimálně 3 roky.

5) Instalace, konfigurace a dokumentace:

Součástí dodávky musí být provedení instalace a konfigurace řešení v místě instalace a také alespoň stručná písemná dokumentace, zahrnující minimálně záznam o konfigurovaných parametrech a uživatelských účtech pro přístup k nastavení.