POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 30-2025

Poskytovatel	Aricoma Systems a.s.
Správce IS	Digitální a informační agentura
Objednatel	Digitální a informační agentura, Na Vápence 915/14, 130 00 Praha 3
Smlouva	SZR- 4231-15/Ř-2020
Číslo RFC	**RFC 1663**
Název RFC	ISZR - Síťový monitoring – pořízení řešení umožňujícího monitoring síťového provozu s možností jeho vyhodnocování
Kategorie RFC	**Change**
Číslo tiketu (ServisDesk)	RITM0147557 / 217045
Katalogový list	**ISZR05_objednávka**
Investice	Ano
Typ odstávky	

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServiceDesk – viz tiket RITM0147557 / 217045 ze dne 6.8.2025

2. Zadání požadované změny

V návaznosti na nákup licencí QRadar, které mohou sloužit také pro účely síťového monitoringu, prosíme o nacenění dalších prací spojených s realizací implementace řešení síťového monitoringu, které umožní monitoring síťového provozu. Cílem je dohled a řízení komunikačního provozu mj. na síťových prvcích.

V rámci změnového řízení dojde k implementaci síťových sond technologie QRadar QFlow/VFlow pro příjem flow nebo přímý odposlech sítě.

3. Popis zajištění realizace změny

3.1 Aktuální stav

DIA nemá k dispozici bezpečnostní řešení pro monitorování síťového provozu. Proběhl nákup licencí IBM QRADAR, které umožňují nasazení tohoto řešení, je třeba provést jeho implementaci. Bez realizace této akce hrozí riziko snížené schopnosti detekovat a reagovat na bezpečnostní incidenty. To může vést k prodloužení doby reakce a zvýšenému riziku bezpečnostních hrozeb.

3.2 Popis změny

V rámci změnového řízení dojde k implementaci řešení síťových sond technologie QRadar QFlow/VFlow pro příjem flow nebo přímý odposlech sítě. Daná změna zahrnuje:

a) Nasazení síťových sond SIEM
   - Instalace FLOW sondy (*.vhdx) v DIA na každého Hyper-V HOSTA (viz kap. 9.1 součinnost)
   - Napojení FLOW do QRADAR SIEM
   - Aktivace pravidel, úvodní ladění pravidel

b) Vyhotovení testovacího protokolu.

- Provedení testovacích scénářů a splnění akceptačních kritérií

4. Odhad pracnosti

Činnost	Pracnost MD
Administrátor	[redacted]
Analytik	
Architekt	
Bezpečnostní architekt	
Bezpečnostní specialista	
Tester	
Projektový manažer	
CELKEM	**39**

Celková cena činí 583 000,00 Kč bez DPH, tj. 705 430,00 Kč včetně DPH.

Poskytovatel služby (dále jen „Aricoma“) bere na vědomí, že Realizace tohoto požadavku souvisí s dosažením cílů uvedených v projektu „Zvýšení úrovně kybernetické bezpečnosti informačních systémů SZR“ s registračním číslem projektu: CZ.31.2.0/0.0/0.0/22_028/0007969, který je financovaný z Národního plánu obnovy (NPO). Aricoma v této souvislosti bere na vědomí, že je povinna plnit některé další povinnosti vyplývající z podmínek realizace projektu, a to uchovávat veškerou dokumentaci související s realizací poskytnutého plnění dle tohoto PnČ, včetně všech účetních dokladů, nejméně po dobu 10 let ode dne schválení závěrečné zprávy o projektu, s tím, že o datu jejího schválení bude Aricoma ze strany DIA informována po skončení projektu. Faktura za plnění dle tohoto PnČ bude obsahovat údaje o názvu projektu a registrační číslo projektu, viz identifikace výše.

5. Návrh harmonogramu změnového požadavku

Termín dodání je do 31. prosince 2025.

6. Návrh testovacího scénáře

A) Realizace implementace řešení síťového monitoringu prostřednictvím QRadar sond
- QRadar sonda je nainstalována v prostředí ISZR a je součástí QRadar Deploymentu
- Sonda zpracovává příchozí data o síťovém provozu a předává je v normalizovaném tvaru na QRadar SIEM
- Na informace o síťovém provozu jsou aplikována pravidla
- Na systém pravidel jsou navázány notifikace
- Ze síťových Flow je možné provádět Reporting nástroji QRadar

7. Výstupy změnového požadavku

Systém SIEM sbírá i informace o komunikaci v síti pomocí dedikovaných sond. Všechny události z logů a sítě jsou centrálně vyhodnocovány systémem pravidel a zároveň bezpečně uloženy v auditním úložišti SIEM s definovanou retencí vyhovující legislativě. Systém je připraven na další rozšíření směrem k ostatním registrům nebo centrální infrastruktuře CMS.

8. Akceptační kritéria, způsob ověření na produkci

Cílem prováděných změn je zvýšení kybernetické bezpečnosti informačního systému v souladu s požadavky zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

Součástí budou následující testy:

a) Seznam všech relevantních zdrojů Flow dohledatelný v QRadar DIA – ověření screenshotem ze SIEM Admin rozhraní
b) Síťová Flow jsou ukládány s požadovanou retencí do vlastní retenční skupiny – ověření screenshotem ze SIEM Retention Policy
c) Síťové sondy zachycují síťovou komunikaci předanou buď flow (IPFIX) protokolem nebo získanou odposlechem sítě (mirror port, TAP port)
d) V systému je aktivní systém pravidel využívajících Flow, na základě kterého vznikají Offense (bezpečnostní události).
e) Z Flow je možné provádět Reporting nástroji QRadar – ověření exportem vybraného logů (skupiny logů) nebo compliance repotem v PDF

9. Požadavky na součinnosti

9.1 DIA – HW sondy

V souladu se zpracovanou analýzou bude třeba zajistit virtuální sondy.

Virtuální flow sonda – optimálně na každém Hyper-V hostu. Sizing dle:
https://www.ibm.com/docs/en/qsip/7.5?topic=planning-system-requirements-virtual-appliances

- 

9.2 DIA – služby

a) Koordinační práce ze strany DIA
b) Součinnost ohledně síťové konektivity nebo nastavení síťových flow nebo odposlechu sítě.
c) Zajištění virtualizovaný HW pro QRadar sondy
d) Předávání kontaktních informací mezi zúčastněnými stranami
e) Předání relevantní dokumentace nebo informaci nutných k nastavení SIEM a Flow Management
f) Otestování přístupů k systému SIEM
g) Seznámení s předanou dokumentací
h) Součinnost při akceptaci.

10. Dopady do provozu / dopady do provozní dokumentace / dopady na finanční prostředky na podporu provozu daného IS

- Aktualizace provozní dokumentace QRadar (CIT/AMS)
- Aktualizace síťové dokumentace (AMS)

10.1 Náklady na podporu provozu IS

Úpravy definované v čl. 3. „Popis zajištění realizace změny“ tohoto PnČ nebudou vyžadovat další dodatečné finanční prostředky na podporu provozu daného IS.

11. Dopady na bezpečnost IS / dopady do bezpečnostní dokumentace

- Bez dopadu.

	Schválil (poskytovatel)	Schválil (objednatel)
Jméno		
Datum		
Podpis