POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 29-2025

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 1662**
Název RFC	ISZR - Rozšíření stávajícího řešení pro zajištění multitenantního provozu SIEM prostřednictvím domén
Kategorie RFC	**Change**
Číslo tiketu (ServisDesk)	RITM0147556 / 217044
Katalogový list	**ISZR05_objednávka**
Investice	**Ano**
Typ odstávky	

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServiceDesk – viz tiket RITM0147556 / 217044 ze dne 6.8.2025

2. Zadání požadované změny

V návaznosti na nákup licencí QRadar, které mají sloužit i pro účely rozšíření stávajícího řešení SIEM QRadar aktuálně sloužícího pouze pro jeden systém základních registrů, prosíme o nacenění dalších souvisejících prací s rozšířením tohoto systému tak, aby fungoval v doménovém (multitenantním) prostředí, tj. mohla se nezávisle evidovat data z bezpečnostního monitoringu systémů ISSS, ISZR, a tato data nezávisle pro každý jednotlivý systém mohla být zpracovávána různými zpracovateli.

3. Popis zajištění realizace změny

3.1 Aktuální stav

DIA nemá k dispozici bezpečnostní řešení doménového (multitenantního) přístupu pro prostředí SIEM. Pro zvýšení úrovně kybernetické bezpečnosti je třeba provést implementaci tohoto řešení. 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 zavedení doménového modelu s využitím QRadar SIEM domén. Cílem je oddělit v systému SIEM bezpečnostní data a oprávnění na úrovni jednotlivých systémů (ISZR a ISSS), ale zároveň udržet centrální správu nad celým prostředím.

Daná změna zahrnuje:

a) Zavedení doménového modelu
   - Definice domén Default, ISZR a ISSS
   - Nastavení domén v infrastruktuře QRadar Deploymentu

- Nastavení domén pro všechny relevantní objekty v SIEM
- Nastavení domén pro všechny zdroje logů
- Definice uživatelských rolí a profilů v systému
- Přiřazení roli uživatelům

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	**122**

Celková cena činí 1 827 650,00 Kč bez DPH, tj. 2 211 456,50 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 31. prosince 2025.

6. Návrh testovacího scénáře

A) Doménový režim
- V systému jsou nadefinovány Domény
- Na domény jsou navázány zdroje logů
- Na domény je navázán systém oprávnění
- Uživatel v rámci domény vidí jen své logy
- Nad přijímanými událostmi funguje systém pravidel
- Na systém pravidel jsou navázány notifikace
- Z logů je možné provádět Reporting nástroji QRadar

7. Výstupy změnového požadavku

QRadar SIEM pracuje v multitenantním režimu na základě QRadar domén. Všechny události z logů a sítě jsou centrálně vyhodnocovány systémem pravidel a zároveň bezpečně uloženy v auditním úložišti SIEM s definovanou retencí vyhovující legislativě. Přístup k systému se řídí na globální nebo doménové úrovni. Systém je připraven na další modulární 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) V systému jsou definovány domény – ověření screenshotem z konfigurace domén
b) Objekty v QRadar, např. zdroje logů používají doménovou notaci – ověření screenshotem z LogSources App
c) V systému jsou definovány globální a doménové účty. Doménové účty vidí pouze zdroje dané domény – ověřeno screenshotem nastavení uživatelských rolí
d) V systému je aktivní systém pravidel, na základě kterého vznikají Offense (bezpečnostní události).
e) Z logů je možné provádět Reporting nástroji QRadar – ověření exportem vybraného logů (skupiny logů) nebo compliance reportem v PDF

9. Požadavky na součinnosti

Realizace je paralelní k, nebo navazující na PnČ 31-2025 RFC 1664 ISZR (ISZR - log management – implementace logovacího nástroje)

9.1 DIA – HW zdroje

V souladu se zpracovanou analýzou upřednostňujeme fyzický HW následujících parametrů:

a) Centrální dvojici serverů, které budou sloužit jako QRadar SIEM All-in-One Cluster.
Fyzický HW - 2U server (DELL, LENOVO, HPe, Cisco)

- [redacted]

Alternativně lze využít zdroje v rámci Hyper-V Sizing dle:
https://www.ibm.com/docs/en/qsip/7.5?topic=planning-system-requirements-virtual-appliances

[redacted]

9.2 DIA

- Koordinační práce ze strany DIA
- Součinnost ohledně síťové konektivity
- Předávání kontaktních informací mezi zúčastněnými stranami
- Předání relevantní dokumentace nebo informací nutných k nastavení SIEM
- Otestování přístupů k systému SIEM
- Seznámení s předanou dokumentací
- 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