POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 31-2025

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 1664**
Název RFC	ISZR - Log management – implementace jednotného logovacího nástroje
Kategorie RFC	**Change**
Číslo tiketu (ServisDesk)	RITM0147558 / 217046
Katalogový list	**ISZR05_objednávka**
Investice	Ano
Typ odstávky	

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServiceDesk – viz tiket RITM0147558 / 217046 ze dne 6.8.2025

2. Zadání požadované změny

V návaznosti na nákup licencí QRadar, které mají sloužit mimo jiné pro účely logovacího systému, prosíme o nacenění dalších souvisejících prací spojených s vytvořením log managementu umožňujícího sběr logů z aplikačních, síťových a bezpečnostních systémů a jejich bezpečné a centralizované uložení pro auditní záznamy.

3. Popis zajištění realizace změny

3.1 Aktuální stav

DIA nemá k dispozici bezpečnostní řešení Log managementu. Proběhl nákup licencí IBM QRADAR, které umožňují nasazení tohoto řešení. Je třeba provést implementaci výše uvedeného 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 nasazení log managementu, a to formou transformace současné implementace IBM QRadar na nové umístění z hlediska síťové topologie. Následně budou zajištěny i veškeré funkce log managementu. Tato změna zahrnuje:

a) Vytvoření Log Managementu spojeného s migrací mezi Hyper-V clustery
   - příprava stávajícího QRadar na migraci
   - konfigurace stávajícího deploymentu
   - migrace AiO Clusteru na nový HW (*.vhdx).
   - nastavení nových IP na AiO

- napojení na stávající infrastrukturu ISZR
- otestování a úprava schématu

b) Vyhotovení testovacího protokolu
- Provedení testovacích scénářů a splnění akceptačních kritérií
- Ověření nasazených změn
- Revize aktivních Log Sources
- Revize nastavení retenční politiky a dlouhodobého využití a trendu alokovaných HW zdrojů
- Popis základních pracovních postupů při kontrole funkcí log managementu a validity příjmu logů (kontrola SIM Generic Log DSM)

4. Odhad pracnosti

Činnost	Pracnost MD
Administrátor	[redacted]
Analytik	
Architekt	
Bezpečnostní architekt	
Bezpečnostní specialista	
Tester	
Projektový manažer	
CELKEM	**28**

Celková cena činí 415 250,00 Kč bez DPH, tj. 502 452,50 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 do 31. prosince 2025.

6. Návrh testovacího scénáře

A) Zajištění Log Managementu
- Deployment SIEM je úplný a všechny jeho komponenty jsou vzájemné propojeny
- SIEM v rámci Log Managementu zajišťuje i příjem logů

- Dochází k parsování logů
- 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 zajišťuje funkce log managementu. Všechny události z logů a sítě jsou centrálně vyhodnocovány systémem pravidel a zároveň bezpečně uloženy na 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

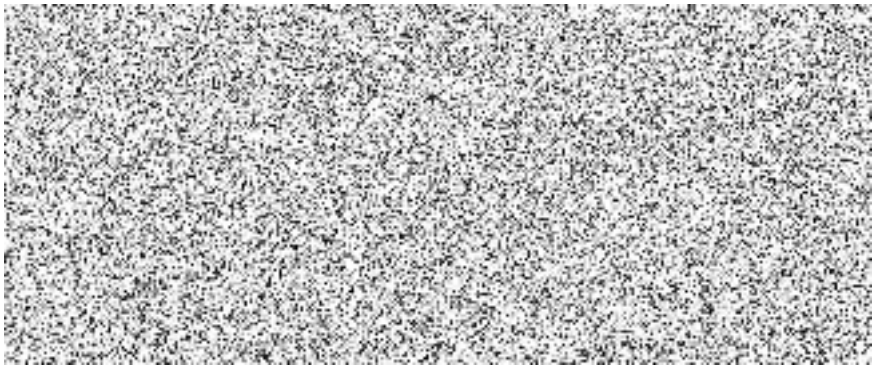
Cílem prováděných změn je zvýšení kybernetické bezpečnosti informačního systému v souladu s požadavky zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

Součástí budou následující testy:

a) Seznam všech relevantních zdrojů logů je definován a navázán na parser v QRadar DIA – ověření screenshotem ze SIEM LogSources App
b) Logy jsou ukládány s požadovanou retencí do vlastních retenčních skupin – ověření screenshotem ze SIEM Retention Policy
c) V systému je aktivní systém pravidel, na základě kterého vznikají Offense (bezpečnostní události).
d) Z logů je možné provádět Reporting nástroji QRadar – ověření exportem vybraného logů (skupiny logů) nebo compliance reportem v PDF

9. Požadavky na součinnosti

a) Centrální dvojici serverů, které budou sloužit jako QRadar SIEM Processor Cluster pro Log Management.
Doporučen fyzický HW - 2U server (DELL, LENOVO, HPe, Cisco)



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

9.1 DIA – služby

- Koordinační práce ze strany DIA
- Součinnost ohledně síťové konektivity
- Zajištění virtualizovaného HW pro QRadar Cluster
- Předávání kontaktních informací mezi zúčastněnými stranami
- Předání relevantní dokumentace nebo informací nutných k nastavení Log Management
- 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