POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 19-2025

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 1621**
Název RFC	**ISZR: Vytvoření úložiště bezpečnostních logů pro ROS a IAIS v prostředí qRadar SIEM ISZR**
Kategorie RFC	**Konfigurace**
Číslo tiketu (ServisDesk)	RITM0143011 / 211597
Katalogový list	**ISZR KL05 - objednávka**
Typ odstávky	bez odstávky

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServiceDesk – viz tiket RITM0143011 / 211597 ze dne 4.6.2025

2. Zadání požadované změny

Vytvoření úložiště pro bezpečnostní logy z IS ROS a IAIS a jeho dočasné umístění v rámci SIEM QRadar prostředí ISZR do doby vytvoření centrálního řešení SIEM.

Toto řešení bude zajišťovat bezpečnostní dohled nad systémem ROS mezi ukončením služeb Českým statistickým úřadem a vytvořením trvalého řešení prostřednictvím SIEM QRadar ISZR. V rámci tohoto požadavku bude provedena konfigurace SIEM prostředí pro ROS, která bude připravena pro trvalé řešení.

3. Popis zajištění realizace změny

3.1 Aktuální stav

V roce 2024 došlo k převodu role správce IS ROS z ČSÚ na DIA. Pro bezpečnostní dohled využívá ČSÚ vlastní SIEM QRadar, jehož služby umožnila využívat do 30.6. 2025 novému správci. Stejný nástroj využívá pro bezpečnostní dohled i IS ISZR.

3.2. Popis změny

V rámci změnového řízení dojde k přesměrování zdrojů logů z ROS a IAIS v obou datových centrech (NDC Vápenka) a (DC Malešice) do QRadar provozovaného v DIA. Daná změna zahrnuje

a) Zajištění nezbytných prostupů mezi ROS, IAIS a QRadar Procesorem (VIP) v DIA. Prostupy ROS, ISZR, DIA (příprava podkladů GOV/NAKIT)

b) Vložení nových licenčních klíčů, které zvyšují EPS a FPM propustnost QRadar SIEM v DIA

c) Přesměrování zdrojů logů, formou rekonfigurace IP destinací na QRadar Procesorem (VIP) v DIA, zavedení logSources pro non-syslog zdroje logů v QRadar DIA

d) Přenesení nezbytné konfigurace QRadar ČSÚ, která byla využívána k obsluze logů ROS a IAIS (logsources, parsery, custom properties, reporty, use-cases, retenční politiky, přístupové role, skripty).

e) Provedení specifických nastavení pro ukládání logů ROS a IAIS na straně QRadar DIA (jmenné konvence pro logsources ROS a ROS.IAIS, parsery, custom properties, reporty, use-cases, retenční politiky, přístupové role, skripty)

f) Nastavení oprávnění pro vybrané pracovníky pro přístup k logům ROS a IAIS.

g) Filtrace reportingu ISZR (nesmí reagovat na log ROS a IAIS)

h) Provedení testů/akceptace a aktualizace dokumentace

i) Převzetí QRadar do provozu (AMS)

j) Pozn.: vlastní logy ROS a IAIS se z ČSU migrovat nebudou a budou v tomto QRadaru do okamžiku jejich expirace.

4. Odhad pracnosti

Činnost	Pracnost MD
Administrátor	[illegible]
Analytik	[illegible]
Architekt	[illegible]
Bezpečnostní architekt	[illegible]
Bezpečnostní specialista	[illegible]
Tester	[illegible]
Projektový manažer	[illegible]
celkem	**41**

Celková cena činí 620 950 Kč bez DPH, tj. 751 350 Kč včetně DPH.

5. Návrh harmonogramu změnového požadavku

Harmonogram realizace požadavku se bude řídit datem objednání. Harmonogram má dva hlavní milníky:

A) Přesměrování příjmu a vyčítání logů do QRadar DIA s termínem 30.6.2025

B) Dokončení konfiguračních prací na QRadar SIEM s termínem do 30.8.2025

Celkově dokončení realizace do 30.8.2025

Termín dodání může být prodloužen v případě neposkytnutí nezbytné součinnosti dle bodu 9. tohoto PnČ, nebo z dalších důvodů na straně objednatele. Nejzazší termín dodání je však 31.12.2025.

6. Návrh testovacího scénáře

Součástí budou následující scénáře:

A) Dochází k příjmu a parsování logů z ROS a IAIS

B) Logy je možné prohledávat formou QRadar „searches“

C) Z logů je možné provádět Reporting nástroji QRadar

D) Testovací uživatel má přístup pouze na logy ROS a IAIS.

E) Logy z ROS a IAIS negenerují aletry do ISZR a ServiceNow.

7. Výstupy změnového požadavku

Logy ROS a logy aplikace IAIS jsou napojeny na úložiště bezpečnostních logů QRadar v DIA, kde jsou náležitě parsovány a vyhodnocovány systémem pravidel.

8. Akceptační kritéria, způsob ověření na produkci

Součástí budou následující testy:

a) V konfiguraci QRadar SIEM je alokována agregovaná kapacita všech zakoupených klíčů (pořízená v rámcové smlouvě MV) – ověření screenshotem ze SIEM admin GUI

b) Seznam všech relevantních zdrojů logů je definován a navázán na parser v QRadar DIA – ověření screenshotem ze SIEM LogSources App

c) Zdroje logů ROS a ROS.IAIS jsou v QRadar uvedeny s touto jmennou konvencí – ověření screenshotem ze SIEM LogSources App

d) Logy jsou ukládány s požadovanou retencí do vlastní retenční skupiny – ověření screenshotem ze SIEM Retention Policy

e) Z logů je možné provádět Reporting nástroji QRadar – ověření exportem vybraného logů (skupiny logů) nebo compliance repotem v PDF

f) V QRadar jsou zkonfigurovány pro přístup k logům ROS a IAIS odpovídající přístupové role a oprávnění pro vybrané uživatele – ověření screenshotem z konfigurace uživatelských přístupů

g) logy z ROS a IAIS negenerují aletry do ISZR a ServiceNow.

9. Požadavky na součinnosti

9.1 DIA

- Koordinační práce ze strany DIA,
- Předávání kontaktních informací mezi zúčastněnými stranami
- Součinnost při akceptaci.
- Zajištění součinností současného provozovatele a správce ROS (přesměrování logových souborů a zajištění přeposílání logů)
- Zajištění prostupů ROS – ISZR (nová GOV)

9.2 Správce ROS a IAIS (ICZ) – zajišťuje DIA

- Rekonfigurace zdrojů logů typu Syslog
- Součinnost při nastavení vyčítání non-syslog logů a případných QR agentů
- Nastavení prostupů v síti na straně ROS a IAIS
- Poskytnutí seznamu zdrojových IP adres pro zasílání logů
- Předání seznamu uživatelů přistupujících do QR DIA k logům ROS a IAIS
- Otestování přístupu a visibilita logů

9.3 ČSU – zajišťuje DIA

- Přístup nebo zajištění exportu vybraných konfigurací z QRadar souvisejících se zpracováním logů ROS a IAIS.

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		