POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 36-2023

Poskytovatel služby	AUTOCONT 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 1302**
Název RFC	**ISSS - Analýza napojení ISSS a dalších IS DIA na SIEM QRadar**
Kategorie RFC	**Dokument**
Číslo tiketu (Service Desk)	RITM0103720 / 150554
Katalogový list	ISRZ05 objednávka
Typ odstávky	Bez odstávky

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServiceDesk – viz tiket RITM0103720 / 150554 ze dne 20.11.2023.

2. Zadání požadované změny

Informační systémy provozované DIA nejsou napojeny na centrální SIEM řešení. Pouze ISZR je napojen na SIEM řešení QRadar dodaný společností AUTOCONT.

Úkolem je provedení analýzy napojení informačního systému ISSS a dalších IS DIA na stávající řešení SIEM QRadar, který je využíván pro informační systém ISZR. Následná analýza Tenant rozdělení stávajícího SIEM řešení pro možnost napojení dalších informačních systémů, definice jmenných konvencí a přístupů pro dodavatele pracovníky DIA. Specifikovat případné požadavky na doplnění licencí.

3. Popis zajištění realizace změny

Předpokládaná osnova analýzy:

- Doporučený obsah logovacích událostí a síťových toků
  - Posouzení vzorků logů systémů ISSS a ISRS (zvolené IS pro ověření doporučení)
  - Popis integrace globálních zdrojů (síťová infra)
  - Popis integrace zdrojů do tenantu
- ARCHITEKTURA pro nový SIEM tenant
  - Výběr vhodných komponent QRadar SIEM
  - Požadavky na nasazení a adresaci
  - HW sizing QRadar komponent a výpočet velikosti jejich úložišť
- Posouzení rozšíření QR SIEM licencí
- Požadavky na součinnost Zadavatele
- KONFIGURACE SYSTÉMU IBM SECURITY QRADAR SIEM
  - KLASIFIKACE ZDROJŮ (logsources) a jejich jmenné konvence a zatřídění do skupin

  - SÍŤOVÉ ROZSAHY a jejich granularita
  - KORELAČNÍ PRAVIDLA, BUILDING BLOCKS a jejich jmenné konvence
    - Výběr doporučených balíčků nových pravidel
  - REFERENČNÍ DATA návrh jejich využití
  - ASSETT DATABÁZE doporučení pro její naplňování
  - PROFILY A ROLE a jejich jmenné konvence s ohledem na multitanantnost
  - MOŽNOSTI INTEGRACE s externím skenerem zranitelností
  - AUTENTIZACE A AUTORIZACE UŽIVATELŮ
    - Doménově vs lokální účty
  - OFFENSE jmenné konvence a zásady pro jejich zpracování
  - REPORTING – výběr reportovacího standardu a plánování reportingu
- NOTIFIKACE a vazba na ticketovací systém v DIA
- RETENČNÍ POLITIKY (zásady nastavení dle požadavku vyhlášky ZoKB)
- INTEGRITA uložených logovacích událostí a flow
- Napojení na MONITORING
- Napojení na ZÁLOHOVÁNÍ
- Napojení na QRadar servisní dohled v AUTOCONT

4. Odhad pracnosti

Celková cena činí 649 000,00 Kč bez DPH, tj. 785 290,00 Kč včetně DPH.

Článek 4.1.2 Prováděcí smlouvy č. 3 o poskytování služeb podpory a rozvoje informačního systému základních registrů a informačního systému sdílené služby k Rámcové dohodě č.j. SZR-4231-4/Ř-2020 „Cena Služeb na objednávku“, Katalogový list ISZR05 „Další služby nad rámec paušálů“ – tento KL v rámci tohoto PnČ neslouží k pracím, které vedou k navýšení stávajících funkcionalit, a tedy k technickému zhodnocení IS ISZR dle vyhlášky č. 410/2009 Sb., k provedení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů pro vybrané jednotky. V rámci tohoto PnČ nebudou prováděny žádné rozvojové činnosti.

Poskytovatel služby (dále jen „Autocont“) bere na vědomí, že předmět plnění tohoto PnČ je spolufinancován z fondů Evropské unie, konkrétně z programu Národní plán obnovy (dále jen „NPO“), v rámci pilíře Digitální transformace, pro projekt, který byl zahrnut do projektu s názvem „Zvýšení úrovně kybernetické bezpečnosti informačních systémů SZR“ (dále jen „projekt“) s registračním číslem projektu: CZ.31.1.01/MV/22_19/0000019. Autocont v této souvislosti bere na vědomí, že je povinen 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 Autocont ze strany DIA informován 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

Dokument bude zpracován do 18 týdnů od objednání.

Kroky harmonogramu
Doporučený obsah logovacích událostí a síťových toků
Architektura pro nový SIEM tenant
Konfigurace systému IBM security QRadar SIEM • klasifikace zdrojů (logsources) a jejich jmenné konvence a zatřídění do skupin • notifikace a vazba na ticketovací systém v DIA • retenční politiky (zásady nastavení dle požadavku vyhlášky ZoKB) • integrita uložených logovacích událostí a flow
Napojení SIEM na ostatní systémy
Dokument k připomínkám
Připomínky
Finální verze dokumentu

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 31.12.2024.

6. Návrh testovacího scénáře

Není relevantní.

7. Výstupy změnového požadavku

Popis napojení informačního systému ISSS a dalších IS DIA na stávající SIEM řešení a příprava metodiky pro napojování ostatních informačních systému. Požadavky na rozvoj SIEM řešení. Specifikace případných požadavků na doplnění licencí.

8. Akceptační kritéria, způsob ověření na produkci

8.1 Akceptační kritéria

- Schválený výstupní dokument.

8.2 Způsob ověření na produkci

- Není relevantní.

9. Požadavky na součinnosti

9.1 DIA

- Koordinační práce ze strany DIA,
- Součinnost při akceptaci.

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

Bez dopadu.

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.