POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 2019-09

Poskytovatel služby	StorageOne a.s.
Správce IS	SZR
Objednatel	ČESKÁ REPUBLIKA - SPRÁVA ZÁKLADNÍCH REGISTRŮ
Smlouva	Č. SZR-3149-17/Ř-2017
Číslo RFC SZR	RFC 530
Název RFC SZR	Bezpečnostní monitoring - analýza
Číslo tiketu (Service Desk)	39769 , 41869
Katalogový list	SZR14-02 (na objednávku)
Typ odstávky	

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServisDesk.

2. Zadání požadované změny

Žádáme o nacenění (PnČ) zajištění bezpečnostního monitoringu v rámci interních systémů SZR (CLOUDIE) Na straně SZR vedeno jako RFC 530

3. Popis zajištění realizace změny

3.1 Předpoklady

Vzhledem k současnému stavu, kdy nejsou v rámci infrastruktury splněny základní podmínky nutné pro vlastní realizaci a spuštění bezpečnostního monitoringu je nutné jako první krok provést analýzu a naplánování nezbytných kroků, po jejichž realizaci bude možné zahájit vlastní nasazení systému pro bezpečnostní monitoring.

Pro zajištění bezpečnostního monitoringu systémů je nutné:

- Definovat bezpečnostní domény systému
- Definovat minimální seznam zaznamenávaných událostí pro každý ze zdrojových systémů/komponent
- Definovat požadavky pro sběr a uchovávání zaznamenaných událostí
- Definovat požadavky pro detekci bezpečnostních událostí

3.2 Činnosti a výstup

Výstupem analytické fáze bude dokument popisující:

1. Zaznamenávání událostí
   a. Požadavky na zaznamenávání událostí pro jednotlivé druhy komponent v souladu s Vyhláškou č. 82/2018 Sb.
   b. Zohlednění případných omezení pro zaznamenávání událostí jednotlivých komponent
   c. Definice minimálního seznamu údajů pro zaznamenávané události
   d. Návrh principů pro dočasné uchovávání záznamů v rámci zdrojových komponent
   e. Návrh pravidel pro řízení přístupů k záznamům o událostech, zamezení pokusům o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí
2. Uchovávání a sběr zaznamenaných událostí – centrální log management
   a. Definice požadavků na centrální log management – základní vlastnosti, sizing
   b. Návrh mechanismů pro zajištění bezpečnosti a integrity log záznamů (ochrana před zneužitím, změněním nebo vymazáním) napříč celým log management systémem
3. Detekce kybernetických bezpečnostních událostí – bezpečnostní monitoring
   a. Definice požadavků na bezpečnostní monitoring – základní vlastnosti, sizing
   b. Návrh základní/startovní sady pravidel – detekovaných bezpečnostních incidentů, jejich hladin a dotčených systémových komponent
4. Plán realizace – harmonogram
   a. Plán jednotlivých kroků
   b. Definice zodpovědností za jednotlivé úkoly

4. Odhad pracnosti

Činnost	Pracnost MD
1. Zaznamenávání událostí	
Definice požadavků na zaznamenávání událostí, definice minimálního seznamu údajů pro zaznamenávané události po jednotlivých komponentách systému	
Návrh uchovávání záznamů v rámci zdrojových komponent, návrh pravidel pro řízení přístupů k záznamům, zamezení pokusům o manipulaci a změnám nastavení nástrojů pro zaznamenávání událostí	
2. Uchovávání a sběr zaznamenaných událostí – centrální log management	
Definice požadavků na centrální log management – základní vlastnosti, sizing	
Návrh mechanismů pro zajištění bezpečnosti a integrity log záznamů (ochrana před zneužitím, změněním nebo vymazáním) napříč celým log management systémem	
3. Detekce kybernetických bezpečnostních událostí – bezpečnostní monitoring	
Definice požadavků na bezpečnostní monitoring – základní vlastnosti, sizing	
Návrh základní/startovní sady pravidel – detekovaných bezpečnostních incidentů, jejich hladin a dotčených systémových komponent	
4. Plán realizace – harmonogram	
Plán realizace - podklady pro volbu koncepce řešení (on premis, DCeGOV..)	

Návrh harmonogramu	
Celkem	[redacted]

Celková cena: 364.650,00 Kč bez DPH, tj. 441.226,5 Kč s DPH.

5. **Návrh harmonogramu změnového požadavku**

   Odevzdání výstupu do 6 týdnů od objednání.

6. **Návrh testovacího scénáře**

   Akceptace předaného výstupu.

7. **Výstupy změnového požadavku**

   Dokument řešení požadavků bezpečnostního monitoringu.

8. **Akceptační kritéria, způsob ověření na produkci**

   Akceptace předaného výstupu.

9. **Požadavky na součinnosti**

   - Poskytnutí relevantní technické a bezpečnostní dokumentace
   - Účast vytipovaných zaměstnanců SZR na pracovních schůzkách
   - Účast vytipovaných správců IS na pracovních schůzkách

10. **Dopady do provozu / dopady do provozní dokumentace**

    Žádné.

	Schválil (dodavatel)	Schválil (zákazník)
Jméno	[redacted]	
Datum		
Podpis		