SPRÁVA ŽELEZNIC

Příloha č. 1 Smlouvy - Bližší specifikace

Technická specifikace

Součástí Předmětu Díla jsou práce zajišťující detailní architektonický návrh, instalace jednotlivých komponent řešení v určené lokalitě, integrace řešení, parametrizace jednotlivých komponent, testování a napojení na službu SOC. Předmětem Díla není dodávka hardware, v rámci smlouvu bude primárně užíván hardware Objednatele, není-li z povahy věci zřejmé, že má být užíván hardware Zhotovitele. Zhotovitel po dobu trvání Smlouvy poskytne Objednateli veškeré licence nezbytné pro provedení a kontrolu Díla.

Dílo je členěno do následujících částí:

1. Vstupní před-implementační analýza, která bude obsahovat následující oblasti:
   a. Detailní návrh architektury řešení.
      - Parametrizace jednotlivých technických oblastí se zohledněním, jejich specifik.
      - Identifikace a návrh import vstupních dat (asset-management, definice sítí, technická definice KII, seznam služeb a jejich priorit, definice služeb klíčových pro detekční pravidla atp.).
      - Definice kritických zdrojů informací (síťové segmenty zdroje logů, podpůrné informační systémy pro vyšetřování kybernetických incidentů).
      - Definice uživatelský rolí a oprávnění uživatelů
      - Napojení na existující služby a prvky
        - Systém pro zálohování dat
        - Systém pro sledování stavu jednotlivých komponent (systémový monitoring)
        - Způsob autentizace uživatelů
        - Elektronická pošta
        - Perimetr sítě
        - Systém EPP

   b. Harmonogram implementace řešení, primárně vychází z výstupů a zjištění v rámci před-implementační analýzy.

   c. Požadavky na součinnosti Objednatele (technické, organizační, procesní).

   d. Návrh akceptačních testů pro jednotlivé oblasti technického řešení (Centrální konzole, Systém APT). Rozsah akceptačních testů je rozdělen na oblasti testování vstupně výstupních vlastností řešení a vybrané klíčové vlastnosti jednotlivých částí řešení.

   e. Součástí analýzy bude seznámení s procesem Incident response Zákazníka. Zavedení revidovaného procesu není součástí dodávky a Objednatel zajistí interně nebo samostatným projektem.

   f. Návrh způsobu napojení pracoviště SOC.

   Výstupem bude technická dokumentace projektu, která bude sloužit jako vstup do realizačních fází implementačního projektu.

2. Implementace a parametrizace řešení na základě informací uvedených v před-implementační analýzy a následné uvedení řešení do provozu.
   a. Instalace software v místě jejího určení ve spolupráci se Objednatelem.
   b. Aktivace potřebných licencí a služeb výrobce zajišťující podporu po dobu trvání Smlouvy.

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

3. Napojení technického řešení na externí SOC pracoviště dodavatele.
   a. Nastavení vstupních dat do SOC.
   b. Technická integrace detekčních nástrojů SOC do vzdáleného pracoviště SOC
4. Ostatní služby spojené s Dílem (onboarding SOC)
   a. Integrace SOC týmu Dodavatele do incident response procesu Zákazníka
   b. Definice alertů na které je požadováno provést různé činnosti dle incident response procesu.
      i. triáž
      ii. reakci
   c. Inicializační ladění detekčních pravidel na základě charakteristik a specifik jednotlivý lokalit.
   d. Nastavení parametrů pro externí skenování zranitelností.
      i. Definice cílů skenování
      ii. Inicializační sken (optimalizace skenovací politiky).
      iii. Spuštění pravidelného skenování.
   e. Provozní deník změn.
5. Dodávka a realizace školení pracovníků Objednatele.
   a. Základní zaškolení pracovníků Objednatele. Školení seznamuje účastníky, jakým způsobem bylo řešení implementováno a ukazuje základní možnosti a vlastnosti celku i jednotlivých technických komponent.
   b. Specializované zaškolení pracovníků Objednatele v následujícím rozsahu. Školení bude probíhat v prostředí zákazníka.

Typ školení	Název – obsah školení	Počet osob	Rozsah (v MD)
Administrace nástrojů SOC	Školení zaměřená na základní správu nástroje bezpečnostního dohledu. Seznámení se hlavními funkcemi nástroje a vysvětlení principů jeho fungování.	max 8	2
Analytik SOC	Praktické procvičování dovedností pracovníka bezpečnostního dohledu z pohledu detekce, analýzy a reakce na kybernetické události a incidenty v nástrojích dodaných v rámci zakázky v prostředí Zákazníka.	max 8	3

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Doložka číslo: 2862541

Původní datový formát: application/pdf

UUID původní komponenty: ab309f53-8d97-4765-85c4-2d9413de9cae

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:

Systém ERMS (zpracovatel dokumentu Miriam HEMZOVÁ)

Subjekt, který změnu formátu provedl: Správa železnic, státní organizace

Datum vyhotovení ověřovací doložky: 18.07.2022 10:32:07