

**Klasifikace: Veřejný dokument**



Technická specifikace

Příloha č. 1 zadávací dokumentace pro zadávací řízení „Log management a SIEM“

Obsah

[1 Seznam zkratek 3](#_Toc142379757)

[2 Úvod 5](#_Toc142379758)

[2.1 Záměr SŽ v oblasti systému Log management a SIEM 5](#_Toc142379759)

[2.2 Předmět plnění veřejné zakázky 6](#_Toc142379760)

[2.3 Etapy a výstupy aktivity 7](#_Toc142379761)

[2.3.1 Etapa 1 7](#_Toc142379762)

[2.3.2 Etapa 2 8](#_Toc142379763)

[2.3.3 Etapa 3 8](#_Toc142379764)

[2.3.4 Etapa 4 9](#_Toc142379765)

[2.3.5 Etapa 5 10](#_Toc142379766)

[2.3.6 Etapa 6 10](#_Toc142379767)

[2.4 Parametry poptávaného řešení 11](#_Toc142379768)

[2.4.1 Testovací prostředí 12](#_Toc142379769)

[2.4.2 Infrastruktura pro přenos logů 12](#_Toc142379770)

[2.4.3 Řešení vysoké dostupnosti 13](#_Toc142379771)

[2.4.4 Zálohování 14](#_Toc142379772)

[2.4.5 Architektura úložišť 14](#_Toc142379773)

[2.4.6 Provozní monitoring 15](#_Toc142379774)

[2.4.7 Zabezpečení 15](#_Toc142379775)

[2.4.8 Log management 15](#_Toc142379776)

[2.4.9 SIEM 16](#_Toc142379777)

[2.4.10 Lokality určené k provozu komponent Log management a SIEM 18](#_Toc142379778)

[2.4.11 Požadavky na technické funkcionality řešení 18](#_Toc142379779)

[2.4.12 Požadavky na specifikaci virtualizačních prostředků Zadavatele 19](#_Toc142379780)

[2.4.13 Dodávka hardwarových a softwarových prostředků 20](#_Toc142379781)

[2.5 Oblasti, které nejsou předmětem plnění veřejné zakázky 20](#_Toc142379782)

[3 Současný stav a popis prostředí 22](#_Toc142379783)

[4 Požadavky na plnění 23](#_Toc142379784)

[4.1 Jednorázové projektové činnosti 23](#_Toc142379785)

[4.1.1 Před-implementační analýza 23](#_Toc142379786)

[4.1.2 Instalace a konfigurace řešení 24](#_Toc142379787)

[4.1.3 Napojení určených zdrojů logů 24](#_Toc142379788)

[4.1.4 Tvorba a optimalizace bezpečnostní / detekční politiky řešení 25](#_Toc142379789)

[4.1.5 Školení 26](#_Toc142379790)

[4.2 Průběžné služby dodavatele řešení 26](#_Toc142379791)

[4.2.1 Technická podpora servisního týmu SŽ 26](#_Toc142379792)

[4.2.2 Údržba řešení 27](#_Toc142379793)

[4.2.3 Konzultace a rozvojové aktivity 28](#_Toc142379794)

[5 Akceptační milníky 29](#_Toc142379795)

# Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

|  |  |
| --- | --- |
| Zkratka | Popis |
| API | Rozhraní pro programování aplikací (Application Programming Interface) |
| CDP | Centrální dispečerské pracoviště |
| DNS | Systém správy doménových jmen, slouží k převodu jmenných záznamů na adresy informačních systémů a evidenci dalších podpůrných informací |
| EPS | Jednotka určující objem logů za sekundu v počtu událostí |
| GB/d | Jednotka určující objem logů za den v Giga Byte |
| GDPR | Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) |
| HA | Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance |
| HTTP | HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro komunikaci s WWW servery |
| IOC | Indikátor kompromitace (Indicator of Compromise, IOC) je ve forenzním světě důkaz, který v kybernetickém prostředí naznačuje, že došlo k narušení kybernetické bezpečnosti |
| IS/ICT | Informační systémy a informační a komunikační technologie. |
| JSON | JavaScript Object Notation je způsob zápisu dat nezávislý na počítačové platformě, určený pro přenos dat, která mohou být organizována v polích nebo agregována v objektech |
| LM | Log management |
| MD | Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day) |
| On-premise | On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá |
| OS | Operační Systém |
| OT | Operational technology (OT) je hardware a software, který zjišťuje nebo způsobuje změny prostřednictvím přímého monitorování a/nebo řízení průmyslových zařízení, prostředků, procesů a událostí. |
| RAT | Remote Access Tool – druh škodlivého kódu, který umožňuje vzdálené ovládání napadeného systému |
| SATA | Počítačová sběrnice, která využívá datové rozhraní pro připojení velkokapacitních paměťových zařízení (např. pevných disků) |
| SIEM | Security Information and Event Management je systém pro správu bezpečnostních informací a událostí. |
| SLA | Dohoda o úrovni poskytovaných služeb (Service Level Agreement) |
| SOC | Kybernetické bezpečnostní dohledové centrum. |
| SSD | Solid-State Drive |
| SW | Software |
| SŽ | Správa železnic, státní organizace |
| SŽT | Správy železniční telematiky |
| Účastník | Subjekt, který se v rámci tohoto zadávacího řízení uchází o realizaci veřejné zakázky |
| URL | Uniform Resource Locator (URL), označovaný jako webová adresa, je odkaz na webový zdroj, který určuje jeho umístění v počítačové síti a mechanismus jeho vyhledávání |
| USB | Univerzální sériové rozhraní informačního systému |
| VoKB | Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| WAN | Wide Area Network je v informatice počítačová síť, která pokrývá rozlehlé geografické území |
| XML | Extensible Markup Language je obecný značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C |
| ZoKB | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů |

# Úvod

Tento dokument je přílohou a nedílnou součástí zadávacího řízení pro výběr dodavatele veřejné zakázky „Log management a SIEM“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

## Záměr SŽ v oblasti systému Log management a SIEM

Jedním z požadavků vyplývajících z § 22 VoKB (*Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů*) je požadavek na sběr informací o provozních a bezpečnostních činnostech a jejich ochranu před neoprávněným přístupem nebo změnou. V současné době jsou informace o provozních a bezpečnostních událostech (logy) zaznamenávány převážně jen na lokální úrovni, kde není vždy možné zaručit jejich integritu a bezpečí.

Cílem aktivity je zavést kompletní řešení pro centrální sběr a uchovávání informací o provozních a bezpečnostních událostech (logů), zaručujícím jejich integritu i všechny další požadavky kladené výše uvedenou VoKB. Toho by mělo být dosaženo nasazením centrálního log management řešení a zapojením potřebných zdrojů logů ze systémů a sítě SŽ do tohoto řešení.

Aktivita definuje implementaci systému správy logů a SIEM jako jeden z kroků zaměřujících se na zlepšení celkového stavu zabezpečení organizace (SŽ). Jedním z hlavních očekávání je zlepšit detekci hrozeb a čas potřebný k reakci tím, že se umožní monitorování a analýza logů z různých systémů v téměř reálném čase. To povede nejen ke zlepšení detekce hrozeb, ale také k rychlejší reakci v případě bezpečnostního incidentu.

Klíčovým cílem je také zajištění souladu s příslušnými bezpečnostními standardy, které se v organizaci (SŽ) uplatňují. Zavedením systému pro správu logů a SIEM chce organizace (SŽ) sledovat a vykazovat bezpečnostní události, a tím zajistit soulad s takovými normami.

Zavedení systému správy logů a SIEM také zefektivní vyšetřování incidentů. Centralizované úložiště logů, které požadované řešení poskytne, umožní bezpečnostním týmům rychle a efektivně vyšetřovat zachycené bezpečnostní i provozní incidenty.

Dalším cílem implementace systému správy logů a SIEM je snížení provozních nákladů a požadavků na součinnosti. Automatizovaný sběr a analýza logů sníží manuální úsilí potřebné k vyšetřování a hlášení bezpečnostních incidentů, čímž se sníží provozní náklady. Kombinace těchto cílů umožní organizaci (SŽ) posílit její bezpečnostní pozici, zvýšit efektivitu a snížit náklady, čímž se systém správy logů a SIEM stane důležitou součástí komplexní strategie kybernetické bezpečnosti.

## Předmět plnění veřejné zakázky

Předmětem aktivity je řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky (zejména s požadavky dle § 22 VoKB). Součást SIEM, která je bezpečnostní nadstavbou nad systémem Log management, bude zajišťovat detekci provozních a bezpečnostních událostí, které je možné odvodit od struktury, posloupnosti a významu zaznamenaných logů, nebo na základě předem definovaných symptomatických pravidel.

Řešení je požadováno realizovat v režimu „centralizovaném“, tedy všechny logy budou přenášeny infrastrukturou SŽ na jedno centrální místo. Přenos bude realizován soustavou log kolektorů, které budou zajišťovat sběr logů od zdrojů logů a dle definovaných pravidel je předají do centrálního úložiště. Přenos logů musí být realizován spolehlivým způsobem, tedy bez ztrát logů, jejich nechtěné modifikace nebo vyzrazení.

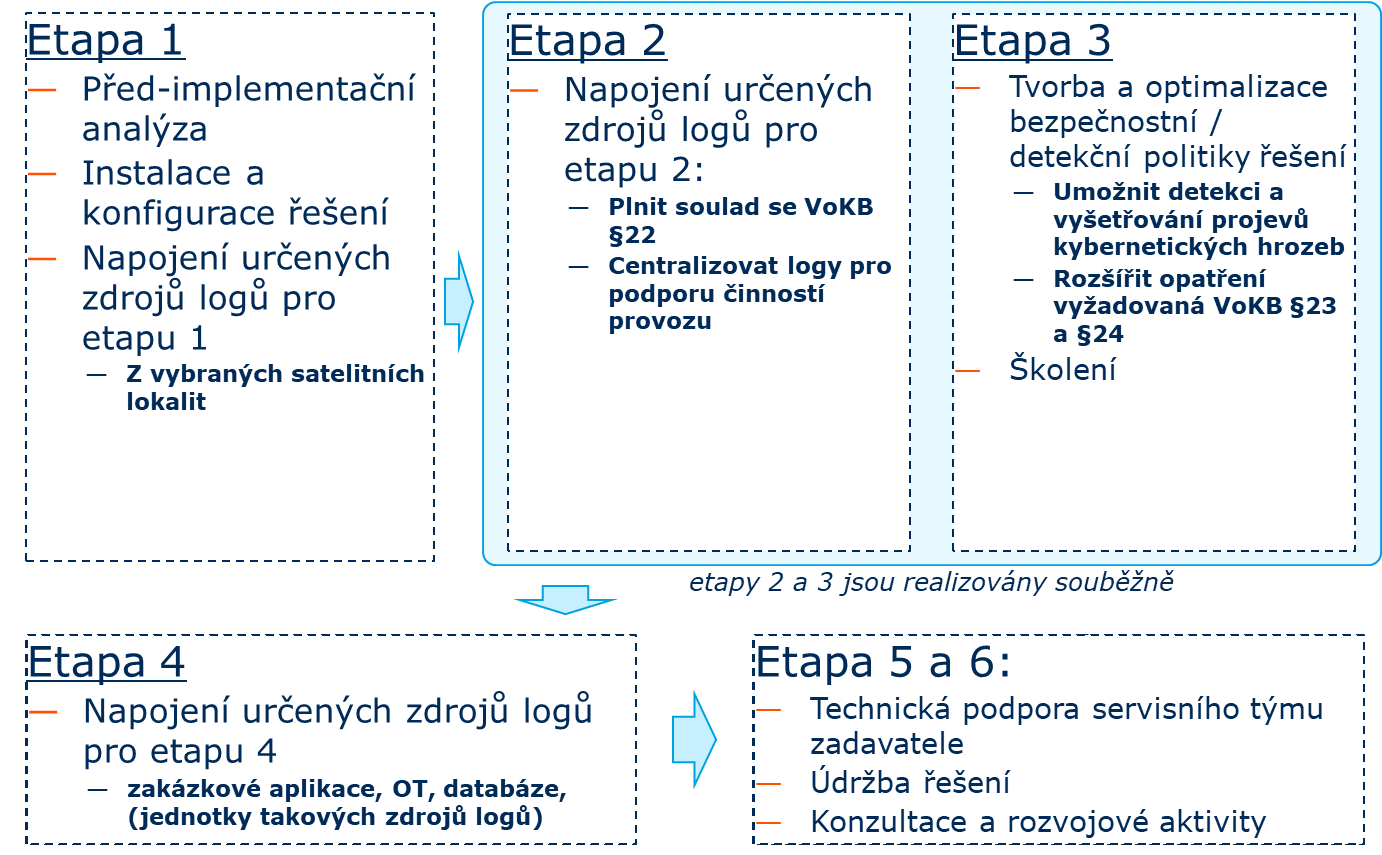
Obsah obrázku text, snímek obrazovky, design

Popis byl vytvořen automaticky

Jednotlivé komponenty řešení budou muset umožňovat a dle požadovaných parametrů také poskytovat vysokou dostupnost. Očekáváním od vysoké dostupnosti je, že nebudou narušeny nezbytné funkcionality řešení a tím omezena možnost užívání řešení nebo porušeny zákonné a regulatorní povinnosti.

## Etapy a výstupy aktivity

Aktivita Log management a SIEM bude rozdělena do jednotlivých etap, které zajistí postupnou realizovatelnost, specifikaci dílčích milníků a finanční plnění vůči dodavateli. Všechny etapy budou součástí jediné veřejné zakázky a budou jen dílčím rozdělením činností.



### Etapa 1

V první části bude zajištěna realizace řešení pro přenos, uložení a interpretaci logů z provozní a bezpečnostní infrastruktury SŽ. Dále bude provedena instalace komponenty SIEM a všech vyžadovaných prvků vysoké dostupnosti. Pro potvrzení funkcionality první etapy, bude požadováno napojení vzorových zdrojů logů, které budou vybrány jako reprezentativní z vybraných satelitních lokalit (Brno, Plzeň) i centrální lokality (Praha U2 / CDP Praha). Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ a označeny ve sloupci „Priorita napojení“ příslušnou etapou, během níž bude vyžadováno jejich napojení.

|  |  |
| --- | --- |
| Aktivita | Popis aktivity |
| Před-implementační analýza | *Popisuje způsob a podmínky nasazení technologie Log management a SIEM do prostředí SŽ.* |
| Instalace a konfigurace řešení | *Budou dodány všechny nezbytné softwarové komponenty řešení, potřebný hardware a licence výrobců software.*  *Funkční řešení pro sběr, ukládání, vyhodnocování logů. Funkční systém pro řešení garantovaného přenosu logů infrastrukturou SŽ. Funkční rozhraní pro práci s nástrojem, vyhledávání logů a jejich interpretaci.* |
| Napojení určených zdrojů logů pro etapu 1 | *Napojení logů z vybraných satelitních lokalit pro ověření funkční přenosové trasy od zdroje logu k systému Log management.*  *Napojení logů z vybraných zdrojů k ověření výkonnostních parametrů a schopnosti řešení užívat a ovládat.* |

### Etapa 2

Tato etapa bude zaměřena na napojování všech zdrojů logů, které budou uvedeny jako zdroje logů podmiňující akceptaci díla. Tyto logy dodavatel napojí na připravené kolektory logů, zajistí jejich transport do centrálních komponent řešení Log management, připraví a nasadí všechny parsovací a normalizační politiky, aby logy byly uloženy v požadovaném formátu umožňujícím jejich další využití. Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ a označeny ve sloupci „Priorita napojení“ příslušnou etapou, během níž bude vyžadováno jejich napojení.

|  |  |
| --- | --- |
| Aktivita | Popis aktivity |
| Napojení určených zdrojů logů pro etapu 2 | *Dodavatel, se součinností SŽ, zajistí napojení všech určených zdrojů logů, čímž prokáže schopnost nástroje zpracovat všechny druhy logů, které SŽ pro tuto etapu specifikovala.* |

### Etapa 3

V této etapě bude vytvořena konfigurace pro vyhodnocování logů v komponentě SIEM, pravidla pro detekce symptomů v lozích a korelační pravidla. Výstupní generované události budou předávány na určené odběratele, kteří budou specifikováni v rámci přípravy před-implementační analýzy. Tato etapa bude realizována souběžně s etapou 2 a nebude se vyčkávat na dokončení napojení všech zdrojů logů definovaných pro celé dílo.

|  |  |  |
| --- | --- | --- |
| Aktivita | Popis aktivity | |
| Tvorba a optimalizace bezpečnostní / detekční politiky řešení | *Dodané komponentě SIEM bude definován způsob nakládání s logy – tento způsob bude dodavatelem nastaven a bude ověřena jeho funkčnost.*  *Nad logy, které jsou již zasílány do systému Log managementu, bude dodavatelem vytvořena sada detekčních a korelačních pravidel, kterými budou naplněny požadavky na USE-CASES SŽ, které jsou uvedeny na listu „USE-CASES“ v příloze č. 21 zadávací dokumentace.*  *Nad nastavenými detekcemi budou vytvořena pravidla pro integraci se systémy SŽ, jako např. JIRA, MS Teams. Důležité je, aby byla naplněna potřeba SŽ o předávání detekovaných událostí jejich zamýšleným odběratelům, tedy útvarům SOC a provoz SŽT.* | |
| Školení pracovníků SŽ | | *Pracovní týmy SŽ budou vyškoleny v:*   * *administraci řešení* * *technické podpoře řešení* * *napojování zdrojů logů* * *práci s logy (hledání, třídění, interpretaci)* * *práci v nástroji SIEM* * *tvorbě detekčních a korelačních politik.* |

### Etapa 4

Etapa bude obsahovat připojování specifických vzorových zdrojů logů (jednotky množství zdrojů) u nichž je očekávána potřeba specifické úpravy nastavení komponent řešení. Mezi taková specifika patří zejména vybraná aktiva z technologických částí sítí, specifické aplikační zdroje logů a podobné. Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ a označeny ve sloupci „Priorita napojení“ příslušnou etapou, během níž bude vyžadováno jejich napojení.

|  |  |
| --- | --- |
| Aktivita | Popis aktivity |
| Napojení určených zdrojů logů pro etapu 4 | *SŽ vybere specifické zdroje logů, které dodavatel v této etapě připojí. Bude se jednat o napojení logů zakázkových aplikací, vybraných zařízení z prostředí OT a databázových systémů.*  *Bude se jednat o jednotky takových systémů, jejichž napojením dodavatel prokáže flexibilitu řešení a možnosti, jak řešit napojení nestandardních zdrojů logů.*  *SŽ bude schopno další zdroje logů napojovat ve vlastní režii, jen s možností čerpání technické podpory dodavatele řešení.* |

### Etapa 5

|  |  |
| --- | --- |
| Aktivita | Popis aktivity |
| Technická podpora servisního týmu SŽ | *Technická podpora dodaného řešení a provoz Help Desku dodavatele.* |
| Údržba řešení | *Zajištění pravidelné údržby všech komponent dodaného řešení, a to včetně bezpečnostní údržby.* |

### Etapa 6

|  |  |
| --- | --- |
| Aktivita | Popis aktivity |
| Konzultace a rozvojové aktivity | *Rozvojové aktivity, které budou souviset především ve změnami v prostředí SŽ, které mohou mít dopad na provoz řešení Log management a SIEM.* |

## Parametry poptávaného řešení

Všechny komponenty řešení požaduje SŽ provozovat v režimu on-premise (tedy výhradně na zařízení v infrastruktuře SŽ). Přípustná integrace s online / CLOUD službami je pouze pro aktualizační služby a získávání informací o hrozbách. Není přípustné předávat data z prostředí SŽ ke zpracování k výrobci nabízeného řešení, pokud tuto aktivitu manuálně (a pouze pro konkrétní vyšetřování) neiniciuje pracovník SŽ.

Řešení Log management a SIEM je poptáváno jako ucelené softwarové řešení, které obsahuje veškeré potřebné licence k naplnění poptávaných parametrů řešení, včetně technické podpory (maintenance nebo subscripce) výrobce nabízených komponent řešení a technické podpory dodavatele řešení, a to na dobu 5 let.

Technická podpora dodavatele bude řízena dle parametrů uvedených ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT Zadavatele (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně ustanovením kapitoly „12. SERVISNÍ MODELY“. SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný“.

SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT Zadavatele (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně ustanovením kapitoly „10. HELPDESK“. SŽ požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“.

|  |  |  |
| --- | --- | --- |
| Parametr | Jednotka | Hodnota |
| Celkem událostí za vteřinu | EPS | 40000 |
| Celkový denní objem logů | GB/d | 1000 |
| Počet lokalit pro umístění log kolektorů | počet | 16 |
| Celkový počet lokalit pro umístění centrálních komponent:   * Jedná se o dvě pracoviště v rámci Prahy * Lokality jsou propojeny silným datovým propojem * SŽ chce využít lokalit pro geo-redundanci centrálních komponent řešení | počet | 2 |
| Minimální doba, po kterou budou logy v systému Log management uloženy | měsíců | 18 |

### Testovací prostředí

SŽ požaduje dodání řešení včetně testovacího prostředí, které bude obsahovat všechny komponenty řešení, licencované na nejmenší dostupné objemy, popřípadě opatřené přímo licencí pro testovací účely. Testovací prostředí musí disponovat prvky režimu vysoké dostupnosti, z důvodu možnosti jejich testování, bude však provozováno pouze v centrálním datovém centru. Testovací prostředí bude sloužit zejména k ověřování nových konfigurací, testování procesů aktualizace SW, řešení chybových stavů apod.

Pro napojení na testovací prostředí jsou vybrány jednotky zdrojů logů, které jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ vyplněním údaje „ANO“ ve sloupci „Testovací prostředí“.

### Infrastruktura pro přenos logů

SŽ požaduje, aby přenos logů od jednotlivých zdrojů logů do centrálních komponent řešení Log management a SIEM, bylo řiditelné, zajištěno bezpečným způsobem a řešení bylo otevřené případnému napojování jiných centrálních komponent řešení.

#### Podpora zdrojů logů

Přenosovou infrastrukturu požaduje SŽ realizovat takovým nástrojem, který umožní integraci se zdroji logů, které jsou uvedeny v příloze č. 21 zadávací dokumentace „Zdroje logů – 2023-05“, a to formou:

1. Pasivního příjmu logů, kdy log odesílá zdroj logu a využívá komunikačních protokolů:
   1. SYSLOG (TCP/UDP)
   2. HTTP/HTTPS
   3. SNMP Trap
   4. TCP
   5. UDP
   6. WEF (Windows Event Forwarder)
2. Aktivního vyčítání logů ze zdrojového systému:
   1. Office 365 Services
   2. Office 365 Activity
   3. Office 365 Message Trace
   4. Kafka
   5. Azure Event Hubs
   6. Azure Blob Storage
   7. Soubor na lokální / vzdáleném souborovém systému
   8. Databázový systém (SQL)

Zdroje logů z prostředí Microsoft systémů, které umožní předávání prostřednictvím Windows Event Forwarder, budou tento způsob využívat. Prostředí Windows Event Forwarder bude ve správě SŽ.

#### Dostupné parametry nastavení řešení

Řešení pro přenos logů musí umožnit nastavení filtračních pravidel, kterými bude možné již před přenosem logů do centrálních komponent řešení, nastavit filtrační pravidla pro redukci objemů přenášených logů (např. odfiltrování logů nepodstatných pro kybernetickou bezpečnost) dle jejich typu, kategorie nebo klíčových slov.

Dalším požadavkem na konfiguraci řešení je možnost upravovat parametry dočasné paměti (cache / buffer), kterou bude možné využívat k uložení logů od zdrojových systémů v případě nedostupnosti cílových centrálních komponent řešení. Požadavek na kapacitu této dočasné paměti je 5 dnů, pokud nebude v před-implemenatační analýze rozhodnuto o snížení této hodnoty. Po obnovení dostupnosti centrálních komponent řešení budou uložené logy odeslány spolehlivým a bezpečným způsobem, tedy tak, že přenos bude šifrovaný a uložení logů do centrálních komponent řešení bude potvrzováno (k vyprázdnění dočasné paměti dojde až po potvrzení uložení na centrálním úložišti).

Přenášené logy budou komprimovány, aby byl optimalizován dopad na přenosovou infrastrukturu SŽ.

#### Bezpečnost řešení

SŽ vyžaduje, aby všechna spojení mezi satelitními kolektory a centrálními komponentami probíhalo zabezpečeně pomocí šifrování a ochrany integrity, přičemž kryptografické algoritmy budou zabezpečeny v souladu s aktuálními doporučeními NÚKIB dle článku 20.15. Zvláštních obchodních podmínek pro zakázky v oblasti ICT (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace).

#### Otevřenost řešení

Dodané řešení pro přenos logů od zdrojů logů do centrálních komponent řešení musí podporovat otevřené komunikační standardy (alespoň SYSLOG, SNMP Trap, Kafka, TCP JSON, ELASTICSEARCH, souborový systém), kterými bude zajišťováno spojení s nástrojem Log management a SIEM. SŽ nepřipouští, aby tato spojení byla realizovatelná pouze proprietárním komunikačním protokolem výrobce řešení Log management a SIEM.

### Řešení vysoké dostupnosti

Vysoká dostupnost je vyžadována u centrálních komponent Log management a SIEM, přičemž SŽ požaduje, aby dodavatel navrhl takové řešení, které splní minimálně následující podmínky:

1. Management rozhraní pro práci s logy a pro analýzu událostí bude provozováno v režimu vysoké dostupnosti Active-Standby nebo Active-Active a jednotlivé komponenty budou rozloženy mezi 2 datová centra SŽ, která jsou určena k provozu centrálních komponent řešení.
2. Úložiště logů a vygenerovaných událostí (alertů) bude provozováno v režimu vysoké dostupnosti Active-Standby nebo Active-Active, přičemž všechna data musejí vždy existovat alespoň ve dvou replikách, kdy každá z replik bude vždy jedna v každém ze 2 datových center SŽ, která jsou určena k provozu centrálních komponent řešení.

### Zálohování

SŽ požaduje dodání řešení včetně návrhu způsobu zálohování jednotlivých komponent řešení, přičemž minimálně budou požadovány následující parametry:

1. Konfigurace všech komponent řešení budou zálohovány v pravidelném cyklu minimálně 1 x denně.
2. Aplikační prostředí všech komponent řešení budou zálohována v pravidelném cyklu minimálně 1 x denně.
3. Bezpečnostní události (aletry a auditní logy Log management a SIEM), které vygenerují nástroje Log management a SIEM, budou zálohovány v pravidelném cyklu minimálně 1 x denně.
4. Data logů, která budou v nástroji Log management uloženy, nebudou podléhat potřebě zálohování – SŽ počítá s dostatečnou odolností dat v rámci jejich rozložení do úložišť ve 2 datových centrech SŽ. Řešení musí umožnit export vybraných logů (vybraných dle zdroje a typu logu) k provedení jejich zálohy na externí zálohovací zařízení SŽ.

### Architektura úložišť

Systém Log management musí podporovat rozklad diskové kapacity na různá úložiště s různou úrovní přístupnosti a rychlosti, která jsou známa jako úložiště HOT, WARM a COLD. Tento přístup, který se často nazývá víceúrovňová architektura úložiště (tiered storage architecture) a umožňuje efektivní správu a ukládání logů s ohledem na jejich důležitost a aktuálnost.

1. Úložiště HOT: Toto úložiště je určeno pro okamžité a intenzivní zápisy logů. Jedná se o nejrychlejší a nejdražší úložiště SSD (Solid-State Drive). Logy, které jsou často přístupné a které vyžadují rychlý přístup, budou ukládány na úložišti HOT.
2. Úložiště WARM: Úložiště WARM slouží pro ukládání logů, které již nejsou tak často přístupné jako na úložišti HOT, ale stále mají určitou důležitost a potřebují být uchovávány pro analýzu, výzkum nebo případnou kontrolu. Toto úložiště je provozováno na discích s nižší rychlostí přenosu dat, jako je SATA disk.
3. Úložiště COLD: Úložiště COLD je určeno pro ukládání starých a méně důležitých logů, které jsou přístupné jen zřídka. Tato data ukládáme na pomalejších a levnějších médiích, jako jsou pásková úložiště.

Při využití víceúrovňové architektury úložiště se Log management systémy často spoléhají na různé mechanismy, jako je automatizované přesouvání logů mezi úložišti na základě jejich věku, důležitosti nebo jiných kritérií. To umožňuje optimalizaci využití diskové kapacity a uchování logů s ohledem na jejich hodnotu a přístupnost.

SŽ vyžaduje, aby nabízené řešení umožňovalo na aplikační úrovni rozlišování druhů úložišť pro:

1. HOT úložiště, která jsou specifická tím, že jejich stáří od doby uložení do Log management není delší než 3 měsíce
2. WARM úložiště budou všechna ostatní data až do požadovaného období pro uložení 18 měsíců.

Využití úložiště úrovně COLD bude sloužit pouze pro účely archivace / zálohování vybraných druhů logů (viz. kapitola „Zálohování“ této Technické specifikace) a bude dostupné pouze v lokalitách SŽ určených pro provoz centrálních komponent řešení.

### Provozní monitoring

SŽ provozuje nástroj provozního monitoringu ZABBIX a požaduje, aby součástí dodávky byl také soupis doporučených dohledovaných parametrů a hodnot nabízeného řešení pro zajištění monitoringu operačních systémů a aplikačního prostředí dodávaného řešení. Cílem je předcházet provozním incidentům na všech komponentách Log management a SIEM, včetně všech komponent dodaných pro přenos logů od zdroje logu až po centrální komponenty.

### Zabezpečení

Dodávané řešení a všechny jeho komponenty budou splňovat bezpečnostní doporučení výrobce (tzv. hardening) a svou vlastní konfigurací umožní dodržení souladu s požadavky ZoKB, resp. VoKB a jejích kapitol:

* § 18 Bezpečnost komunikačních sítí [písmena c) a d)]
* § 19 Správa a ověřování identit [odstavce 3, 5 písm. a) a 6 písm. a)]
* § 20 Řízení přístupových oprávnění
* § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů [odstavce 2 písm. d) a 2 písm. e)]
* § 26 Kryptografické prostředky [písmena a), c) a d)].

### Log management

Kybernetické bezpečnostní řešení Log management pro SŽ s centralizovanou architekturou by mělo splňovat následující požadavky:

1. Shromažďování logů: Řešení musí umožňovat shromažďování logovacích dat z různých zdrojů v organizaci (SŽ), včetně síťových prvků, serverů, aplikací a vybraných koncových zařízení.
2. Centralizace: Veškeré logy musí být sbírány a ukládány v centrálním datovém centru. Centralizovaná architektura umožňuje snadnou správu a analýzu dat a zajišťuje jednotný pohled na logovací informace z celé organizace.
3. Škálovatelnost: Řešení musí být schopné zvládat velké množství logovacích dat v rozsáhlé organizaci. Musí být navrženo tak, aby bylo schopné efektivně zpracovávat a ukládat logy ze všech specifikovaných satelitních lokalit (kapitola „2.4.10 Lokality určené k provozu komponent Log management a SIEM“ této Technické specifikace).
4. Bezpečnostní funkce: Log management řešení musí obsahovat bezpečnostní funkce, jako je šifrování dat při přenosu, ověřování identity uživatelů systému, kontrola a řízení přístupu. To zajistí ochranu logovacích dat proti neoprávněnému přístupu a manipulaci.
5. Real-time monitoring: Řešení musí poskytovat možnost sledování logovacích událostí v reálném čase. To umožní rychlou detekci a odpověď na bezpečnostní incidenty. Požadovaná vlastnost může být sdílenou součástí se SIEM vrstvou.
6. Vyhledávání a dotazování: Řešení musí poskytovat efektivní nástroje pro vyhledávání a dotazování logovaných dat. To umožní snadnou analýzu a vyhledávání specifických informací v rozsáhlých datových sadách.
7. Reporting a vizualizace: Řešení musí poskytovat možnosti tvorby reportů a vizualizace logovacích dat. To umožní vytváření přehledných reportů a grafů, které usnadní prezentaci a analýzu logovacích informací pro bezpečnostní tým, provoz a popř. i management.
8. Auditovatelnost: Řešení musí splňovat požadavky na auditovatelnost, což zahrnuje sledování a záznam veškerých aktivit týkajících se logování i analýzy dat a auditovatelnost aktivit privilegovaných uživatelů systému Log management. To je důležité pro dodržování regulací a standardů v oblasti kybernetické bezpečnosti.
9. Rozšiřitelnost: Log management řešení musí být navrženo tak, aby bylo snadno rozšiřitelné a přizpůsobitelné rostoucím potřebám organizace (SŽ). To zahrnuje možnost přidávat nové zdroje logů a rozšiřovat kapacitu systému bez výrazného poklesu výkonu.

Celkově řečeno, kybernetické bezpečnostní řešení Log managementu s centralizovanou architekturou by mělo SŽ umožňovat efektivní shromažďování, analýzu, sledování a ochranu logovacích dat z různých zdrojů v celé organizaci (SŽ). Splnění těchto požadavků pomůže organizaci (SŽ) zlepšit svou schopnost detekovat, reagovat a předcházet kybernetickým hrozbám a incidentům a vyhovět požadavkům vyplývajícím ze ZoKB a VoKB.

### SIEM

Nedílnou součástí požadovaného řešení je také komponenta SIEM (Security Information and Event Management), která poskytne rozšířené funkcionality pro analýzu bezpečnostních událostí a monitorování hrozeb. Kybernetické bezpečnostní řešení SIEM pro SŽ s centralizovanou architekturou by mělo splňovat následující požadavky:

1. Detekce a analýza hrozeb: SIEM řešení musí poskytovat pokročilou detekci a analýzu bezpečnostních hrozeb. To zahrnuje monitorování aktivit a událostí v reálném čase, vyhledávání anomálií, identifikaci známých indikátorů kompromitace (IOC) a podporu pro vyhledávání souvislostí mezi různými událostmi.
2. Korelace událostí: Funkce pro korelaci událostí je klíčovou součástí SIEM řešení. Tímto způsobem lze identifikovat spojitosti a vzorce mezi různými událostmi a aktivitami v prostředí. To umožňuje identifikovat sofistikované hrozby a předcházet jim dříve, než způsobí větší škody.
3. Pravidla a upozornění: SIEM musí umožňovat vytváření pravidel a upozornění pro rychlou identifikaci a reakci na bezpečnostní události. Administrátoři by měli mít možnost definovat specifická pravidla a podmínky, na jejichž základě systém vygeneruje upozornění na potenciální bezpečnostní incidenty.
4. Integrace s Log managementem: SIEM musí být plně integrované s nabízeným Log management řešením. Tím se zajišťuje, že logy z různých zdrojů jsou k dispozici pro analýzu a monitorování bezpečnostních událostí a zároveň poskytuje holistický pohled na bezpečnostní situaci organizace (SŽ). Toto však neznamená, že všechny logy uložené v prostředí Log management budou zpracovávány komponentou SIEM. SŽ požaduje, aby bylo možné licenčně rozlišit data ukládaná jen v Log management a data, která budou určena ke zpracování v komponentě SIEM.
5. Vizualizace a reporting: SIEM řešení by mělo poskytovat možnosti vizualizace dat a tvorby reportů. To umožňuje uživatelům snadno sledovat a analyzovat bezpečnostní události prostřednictvím interaktivních grafů, tabulek a dashboardů. Reporty pak umožňují prezentaci důležitých informací managementu a auditům.
6. Sledování souladu: SIEM by měl poskytovat funkcionalitu pro sledování souladu s příslušnými bezpečnostními předpisy, normami a regulacemi, jako je například GDPR, ZoKB. Tím se organizaci (SŽ) umožní dodržování požadovaných standardů a předpokladů v oblasti ochrany dat a informací.
7. Rozšiřitelnost a výkon: SIEM by měl být navržen s ohledem na vysokou škálovatelnost a výkon. To umožní efektivní zpracování velkých objemů dat a událostí, které vznikají v rozsáhlých a dynamických prostředích SŽ.

SIEM řešení s centralizovaným Log managementem by mělo poskytovat pokročilé funkce pro detekci, analýzu a monitorování bezpečnostních událostí. Integrace s existujícími nástroji, vizualizace dat, správa incidentů a podpora souladu s regulacemi jsou další klíčové aspekty, které budou zohledněny při výběru SIEM řešení.

### Lokality určené k provozu komponent Log management a SIEM

|  |  |  |
| --- | --- | --- |
| Typ lokality | Adresa lokality | Účel |
| CDP | V Trianglu 2474, Praha 9 | Centrální komponenty LM / SIEM |
| Datové centrum | Pod Táborem 369/8a, Praha 9 | Centrální komponenty LM / SIEM |
| Datové centrum | Kulkova 1, Brno (Maloměřice) | Satelitní log kolektor |
| Datové centrum | Škroupova 1017/11, Plzeň | Satelitní log kolektor |
| Datové centrum /CDP | Tovární 3286, Přerov | Satelitní log kolektor |
| Oblastní ředitelství | ATU, Ostrava | Satelitní log kolektor |
| Oblastní ředitelství | Kounicova 26, Brno | Satelitní log kolektor |
| Oblastní ředitelství | Pávovská 2, Jihlava | Satelitní log kolektor |
| Oblastní ředitelství | Křižíkova 552, Praha 1 | Satelitní log kolektor |
| Oblastní ředitelství | Pernerova 2819/2a, Praha 2 | Satelitní log kolektor |
| Oblastní ředitelství | Riegrovo náměstí 1660, Hradec Králové | Satelitní log kolektor |
| Oblastní ředitelství | ATU, Pardubice | Satelitní log kolektor |
| Oblastní ředitelství | Sušická 1168/23, Plzeň | Satelitní log kolektor |
| Oblastní ředitelství | A. Trägera 2899/90, České Budějovice | Satelitní log kolektor |
| Oblastní ředitelství | Železničářská 1386/31, Ústí nad Labem | Satelitní log kolektor |
| Organizační jednotka | Kounicova 26, Brno | Satelitní log kolektor |
| Organizační jednotka | Nerudova 773/1, Olomouc | Satelitní log kolektor |
| Technologická / sdělovací místnost | Wilsonova 300/8, Praha 2 | Satelitní log kolektor |
| Technologická / sdělovací místnost | Havlíčkova 1011, Praha 1 | Satelitní log kolektor |

### Požadavky na technické funkcionality řešení

Všechny parametry požadované v tomto dokumentu a přílohách zadávací dokumentace jsou pro dodavatele závazné a SŽ vyžaduje jejich naplnění.

Požadavky na vybrané funkcionality poptávaného řešení, které SŽ vyžaduje splnit technickými prostředky, a u nichž Účastník musí popsat způsob, kterým jím nabízené řešení naplní požadavek, jsou specifikovány v přiloženém dotazníku „Log management a SIEM dotazník“, který je Přílohou č. 20 zadávací dokumentace; v tomto dotazníku Účastník potvrdí připravenost nabízeného řešení splnit vybrané požadavky a vyplní způsob, kterým je každý požadavek naplněn. Účastník do přiloženého dotazníku doplní také soupis všech licencí nabízeného řešení, kterým zajistí naplnění požadovaných funkcionalit.

SŽ upozorňuje, že nesplnění kteréhokoliv požadavku na technické funkcionality řešení uvedeného v přiloženém dotazníku, povede k vyloučení Účastníka ze zadávacího řízení. V případě, že bude nesplnění takového požadavku odhaleno až v průběhu realizace plnění, bude to považováno za hrubé porušení povinností dle přílohy č. 6 zadávací dokumentace – Závazného vzoru smlouvy a bude důvodem pro odstoupení od této smlouvy.

### Požadavky na specifikaci virtualizačních prostředků Zadavatele

V souvislosti se schválenou strategií IS/ICT SŽ, konkrétně cílem zajištění dlouhodobého koncepčního a efektivního rozvoje IS/ICT, požaduje SŽ využití možností jeho hardwarové a virtualizační platformy pro jednotlivé komponenty poptávaného řešení. Popis platformy je uveden v příloze č. 4 zadávací dokumentace, která je označena jako „Platforma SŽ 2.0“.

Pro veškeré prostředky, ve všech lokalitách určených k provozu řešení Log management a SIEM, které je možné provozovat v platformě SŽ, vyplní Účastník specifikaci technických požadavků na platformu SŽ, a to do připraveného listu „Požadavky“ v Příloze č. 19 zadávací dokumentace, která je označena jako „Požadavky na služby Platformy SŽ pro Log Management a SIEM“.

Jedná se zejména o následující parametry:

* Požadovaný počet kusů daného řešení
* Požadovaný počet Core
* Požadovaná velikost RAM
* Požadovaná velikost diskového prostoru na úložišti typu COLD storage
* Požadovaná velikost diskového uložiště v úložišti typu HOT/WARM storage
* Požadovaná velikost diskového uložiště pro zálohování (BACKUP).

Náklady na rozšíření virtualizační platformy SŽ do požadovaných parametrů, nebude Účastník uvádět jako součást nabídkové ceny, tedy do svých nákladů. SŽ bude hodnotit nároky nabízeného řešení na virtualizační platformu pomocí bodovacího systému, na základě celkového požadovaného výpočetního výkonu uvedeného v listu „Požadavky“, který je součástí Přílohy č. 19 zadávací dokumentace.

SŽ limituje celkové požadavky na výpočetní výkon a kapacitu, který je připraven pro účely projektu nabídnout, takto:

|  |  |
| --- | --- |
| Parametr výkonu a kapacity | Maximální povolená hodnota |
| Počet v CPU | 1046 |
| Kapacita RAM (GB) | 4877 |
| Kapacita disků (GB) | 1860000 |

### Dodávka hardwarových a softwarových prostředků

Výjimkou, kdy není nutné využití platformy SŽ, jsou samozřejmě komponenty řešení, které virtualizaci neumožňují. V takovém případě uvede dodavatel veškeré náklady na hardware, který je součástí dodávaného řešení a nebude provozován v platformě SŽ, do své cenové kalkulace a učiní jej součástí své dodávky.

Pokud bude součástí nabízeného řešení také dodávka technických a programových prostředků, bude Účastník respektovat, že:

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) na základě ZoKB Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: „*Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

* *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*
* *ZTE Corporation, Šen-čen, Čínská lidová republika*“.

Dne 4. ledna 2019 vydal NÚKIB Metodiku k varování ze dne 17. prosince 2018 (dále jen „metodika“), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou provedla SŽ analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 VOKB. V návaznosti na to SŽ identifikovala rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná, a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

**SŽ tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.**

## Oblasti, které nejsou předmětem plnění veřejné zakázky

* Instalace a správa virtualizační platformy, která zajišťuje prostor pro provoz komponent řešení Log management a SIEM.
* Instalace a správa operačních systémů, které jsou součástí nabízených instancí virtualizační platformy SŽ, pokud dodavatel nebude vyžadovat instalaci specifického OS, nebo provádění zásahů do standardní instalace.
* Provozní monitoring HW a virtualizačního prostředí SŽ, které zajišťuje provoz jednotlivých komponent řešení Log management a SIEM.
* Úprava a konfigurace zdrojů logů pro účely jejich integrace na komponenty řešení Log management a SIEM.
* Provoz archivačního systému pro dlouhodobé uložení logů mimo prostředí řešení Log management a SIEM.

# Současný stav a popis prostředí

Současný stav ICT prostředí SŽ je popsán v přiložených dokumentech:

* Analýza prostředí – architektura prostředí SŽ (Příloha č. 2 zadávací dokumentace)
* Analýza prostředí – popis prostředí sítě UAS (Příloha č. 3 zadávací dokumentace)
* Platforma 2.0 - souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT (Příloha č. 4 zadávací dokumentace)

# Požadavky na plnění

SŽ očekává dodávku komplexního řešení, která se bude sestávat z jednorázových projektových činností, dodávky nástroje se souvisejícími technickými komponenty a průběžných služeb dodavatele řešení.

## Jednorázové projektové činnosti

Jednorázové projektové činnosti jsou nedílnou součástí dodávaného řešení, jsou zahrnuty mezi akceptační milníky a je k nim vázána etapizace dodávky a fakturace.

### Před-implementační analýza

|  |  |
| --- | --- |
|  | **Před-implementační analýza** |
| Popis | Před-implementační analýza popisuje způsob a podmínky nasazení technologie Log management a SIEM do prostředí SŽ. Dokument musí popisovat charakteristiku dodávaného technického řešení, popis jednotlivých jeho komponent, navrhovaný způsob zapojení do prostředí SŽ a samozřejmě způsob integrace zdrojů logů.  Dokument musí mít charakter detailní technické specifikace pro všechny uvažované implementační postupy, na jejichž předběžném schválení závisí umožnění provádět technické zásahy do prostředí SŽ. |
| Výstupy | Výstupem tohoto kroku bude dokument obsahující alespoň:   * Popis dodávaného technického řešení a jeho komponent * Návrh architektury dodávaného řešení v prostředí SŽ * Detailní popis implementačních kroků * Detailní technická specifikace   + Umístění technologií   + Napájení   + Síťové segmenty pro správu technologie   + IP adresace   + HW požadavky na virtualizační platformu SŽ   + Požadavky na síťové prostupy   + Požadavky na přístup do internetu   + Požadavky na vzdálený přístup pro správu technologie   + Požadavky na systémový monitoring   + Postup napojení zdrojů logů do Log management / SIEM * Revizi USE-CASES, které jsou uvedeny v listu „USE-CASES“ v příloze č. 21 zadávací dokumentace, zadaných v rámci TS a doporučení dalších USE-CASES dodavatelem * Požadované součinnosti na SŽ * Návrh akceptačních testů * Katalog projektových rizik a návrh způsobu jejich ošetření * Specifikace kroků, součinností dodavatele a jejich rozsah v MD, při ukončení projektu (exit plán), které budou součástí poskytované služby * Detailní harmonogram implementace řešení |

### Instalace a konfigurace řešení

|  |  |
| --- | --- |
|  | **Instalace a konfigurace řešení** |
| Popis | V této části projektu dojde k dodání, instalaci a konfiguraci všech komponent technického řešení Log management a SIEM, které naplní požadavky předmětu veřejné zakázky a naplní specifika projektu uvedená v dokumentu před-implementační analýza. |
| Výstupy | Výstupem tohoto kroku bude funkční technické řešení Log management a SIEM, které bude:   * Obsahovat všechny potřebné licence, předplatné a technické podpory výrobce. * Dodáno s nezbytným hardwarem pro komponenty, které není vhodné provozovat ve virtuálním prostředí SŽ. * Nasazeno na všech požadovaných lokalitách pro etapu 1 včetně komponent pro přenos logů od zdroje do centrálních úložišť. * V souladu se schválenou architekturou. * Zcela funkční pro výkon funkce Log management a SIEM, tak jak SŽ požaduje v této Technické specifikaci. * Napojeno na systémový monitoring SŽ (systém Zabbix). * Schopno vyhovět definovaným akceptačním testům v rozsahu specifikovaným v před-implementační analýze a schváleným SŽ. |

### Napojení určených zdrojů logů

|  |  |
| --- | --- |
|  | **Napojení určených zdrojů logů** |
| Popis | V této části projektu dojde k napojení určených zdrojů logů, které SŽ určila k napojení do prostředí Log management a SIEM pro odpovídající etapu projektu. Zdroje logů jsou zvlášť specifikovány pro etapu 1, etapu 2 a etapu 4 v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ uvedením odpovídající etapy ve sloupci „Priorita napojení“. |
| Výstupy | Výstupem tohoto kroku bude funkční napojení zdroj logů na Log management a SIEM a bude obsahovat:   * Nasazení komponent infrastruktury pro přenos logů ze satelitních lokalit do centrálních úložišť řešení (nad rámec komponent instalovaných v etapě 1). * Provedení technické integrace se zdrojem logu   + Výběr komunikačního protokolu   + Výběr typů logových zpráv. * Nastavení přenosové platformy pro zajištění garantovaného odeslání logů od zdrojového systému k centrálním prvkům řešení Log management a SIEM. * Ověření přenosu logů od zdroje do centrálního úložiště. * Nastavení zpracování logů od zdrojů pro podporu další datové analýzy (parsing). * Nastavení normalizace logů, pokud je to vyžadováno řešením pro naplnění požadavků uvedených v technické specifikaci a požadavcích na detekční USE-CASES, které jsou uvedeny v listu „USE-CASES“ v příloze č. 21 zadávací dokumentace. * Nastavení retenční politiky pro logy. |

### Tvorba a optimalizace bezpečnostní / detekční politiky řešení

|  |  |
| --- | --- |
|  | **Tvorba a optimalizace bezpečnostní / detekční politiky řešení** |
| Popis | V této části projektu bude dodavatelem provedeno vyhodnocení účinnosti nasazeného řešení Log management a SIEM, bude upravena bezpečnostní / detekční pravidla a zdokumentovány všechny provedené konfigurační úpravy, které vedou k vyšší efektivitě detekce kybernetických bezpečnostních událostí pro analytický tým SOC SŽ. |
| Výstupy | Výstupem tohoto kroku bude funkční technické řešení Log management a SIEM, které bude mít upravenu bezpečnostní / detekční politiku tak, že bude minimalizován objem falešných detekcí, které by musel analytický tým SOC zpracovávat. SŽ požaduje provedení alespoň následujících činností:   * Zohlednění reálných dostupných IP adresací SŽ v detekčních politikách. * Upřesnění konkrétních druhů validních aktiv SŽ zaznamenaných v komunikacích, které jsou důležité pro fungování detekčních pravidel (DNS, SMTP, WEB, NTP, PROXY, MS AD). * Vytvoření specifických detekčních politik (tzv. detekčních use-cases), dle specifikace SŽ, které jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05.“ v listu „USE-CASES“. * Aplikace výjimek, které doporučí SŽ. * Předávání detekovaných událostí jejich odběratelům, kterými budou pracoviště SOC, nebo provozní tým SŽT.   Všechny upravené konfigurace budou zdokumentovány a předány jako výstup této části projektu. |

### Školení

|  |  |
| --- | --- |
|  | **Školení** |
| Popis | V této části projektu bude dodavatelem provedeno zaškolení technického servisního týmu SŽ a týmu Security Operations Center SŽ. Cílem je přenesení znalostí o správě dodaných nástrojů a předání rutinní správy na tým SŽ. Druhé specifické školení by se mělo hlouběji zaměřit na školení práce s řešením Log management a SIEM, jehož odběratelem bude pracoviště SOC SŽ. |
| Výstupy | Výstupem tohoto kroku bude realizované školení se zaměřením na využívání a správu technického řešení Log management a SIEM:   * Prezenční školení servisního týmu SŽ. SŽ nominuje 8 pracovníků a bude požadovat naplnění časové dotace alespoň 3 MD.   + komponenty systému   + konfigurační parametry komponent   + ladění výkonnostních a kapacitních parametrů řešení   + troubleshooting   + update a upgrade. * Prezenční školení týmu SOC SŽ v prostorách výrobce zakončené certifikací účastníků. SŽ nominuje 4 pracovníky a bude požadovat naplnění časové dotace alespoň 3 MD.   + zaměření na užívání nástroje Log management a SIEM   + tvorba a úprava detekčních pravidel   + vyšetřování a analýza událostí   + aktivní vyhledávání kybernetických hrozeb. |

## Průběžné služby dodavatele řešení

### Technická podpora servisního týmu SŽ

|  |  |
| --- | --- |
|  | **Technická podpora servisního týmu zadavatele** |
| Popis | Technická podpora bude řízena dle parametrů uvedených ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT SŽ (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně v ustanovení kapitoly „12. SERVISNÍ MODELY“. SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný“.  SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT SŽ (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně v ustanovení kapitoly „10. HELPDESK“. SŽ požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“. |
| Výstupy | Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ a definovaných v servisní smlouvě s dodavatelem. |

### Údržba řešení

|  |  |
| --- | --- |
|  | **Údržba řešení** |
| Popis | Dodavatel zajistí pravidelnou údržbu všech komponent dodaného řešení, a to včetně bezpečnostní údržby. Cílem je, aby byl zajištěn provoz řešení v aktuální verzích produktu, které budou považovány za stabilní a bezpečné.  Dodavatel zajistí aplikaci výrobcem vydávaných opravných balíčků, nových funkcionalit a bezpečnostních záplat.  Průběžně prováděné a pravidelné činnosti zahrnují (prováděné min. 1x měsíčně):   * Aktivní sledování a využívání nových postupů v oblasti zabezpečení systémů a komunikací. * Průběžné aplikování bezpečnostních oprav od výrobců. * Udržování aktuálnosti SW verzí dodaného řešení, a to minimálně v režimu aktuální MAJOR verze a MINOR verze ne starší než 2 vydání. Případné výjimky musí schválit SŽ. * Sběr podkladů pro aktualizaci dokumentace / evidence aktiv SŽ. * Pravidelná profylaxe systémových prostředků systému, včetně návrhu řešení nalezených problémů nebo rozvoje systému. * Kontrola provozních systémových logů s následným řešením případných incidentů. * Kontrola funkčnosti a bezpečnosti úložiště hesel. * Vypracování protokolu o údržbě s detailním popisem veškerých nalezených nedostatků a postupu pro jejich odstranění. |
| Výstupy | Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ. |

### Konzultace a rozvojové aktivity

|  |  |
| --- | --- |
|  | **Konzultace a rozvojové aktivity** |
| Popis | Dodavatel poskytne SŽ služby konzultace na vyžádání. Maximální souhrn těchto služeb bude činit 250 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ. Jedná se o rozvojové aktivity, které budou souviset především s:   * změnami v prostředí SŽ, které mohou mít dopad na provoz řešení Log management a SIEM. * integrací prostředí Log management a SIEM na procesy Security Operations Center   + Incident Response   + Forenzní analýza   + Sběr IoC. * pokročilou analýzou dat. * zajištěním udržitelnosti prostředí Log management a SIEM. |
| Výstupy | Výstupem tohoto bude poskytnutí služby konzultace na vyžádání podle potřeb SŽ. |

# Akceptační milníky

Plnění musí být dodáno v níže uvedených etapách. Každá z níže uvedených etap (tj. každý řádek níže uvedené tabulky) musí být SŽ separátně akceptována nejpozději v termínu uvedeném v harmonogramu. SŽ akceptuje výstupy dané Etapy, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky.

| **Etapa** | **Popis** | **Kapitola obsahující požadavky** |
| --- | --- | --- |
| Etapa 1A | Jednorázové projektové činnosti:   * Před-implementační analýza | 4.1.1 |
| Etapa 1B | Jednorázové projektové činnosti:   * Instalace a konfigurace řešení * Napojení určených zdrojů logů pro etapu 1 | 4.1.2  4.1.3 |
| Etapa 2 | Jednorázové projektové činnosti:   * Napojení určených zdrojů logů pro etapu 2 | 4.1.3 |
| Etapa 3 | Jednorázové projektové činnosti:   * Tvorba a optimalizace bezpečnostní / detekční politiky řešení * Školení | 4.1.4  4.1.5 |
| Etapa 4 | Jednorázové projektové činnosti:   * Napojení určených zdrojů logů pro etapu 4 | 4.1.3 |
| Etapa 5 | Průběžné služby dodavatele řešení:   * Technická podpora servisního týmu SŽ * Údržba řešení | 4.2.1  4.2.2 |
| Etapa 6 | Průběžné služby dodavatele řešení:   * Konzultace a rozvojové aktivity | 4.2.3 |