***Príloha č. 2 k zmluve č. Z-009.10.1003.00***

**Požiadavky na upgrade systému**

#### Základné informácie

Použité skratky:

AD – Active Directory

Flowmon ADS – Flowmon Anomaly Detection System

Flowmon FMC – Flowmon Monitoring Center

Flowmon OS – Flowmon Operating System

HTP – hlavné technologické pracovisko (ústredie NBS) – I. Karvaša 1, 813 25 Bratislava

HW – hardvér

MPS – messages per second

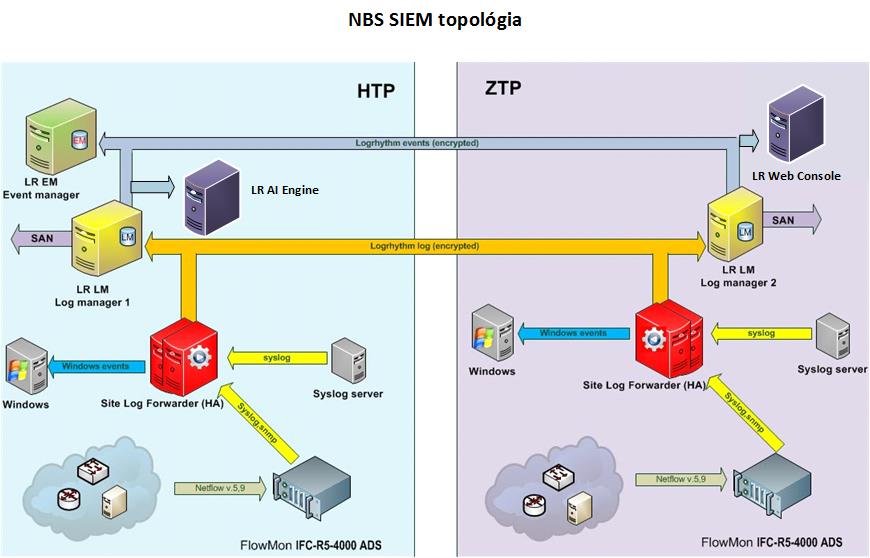
OS - operačný systém

SIEM – Security Information and Event Management

SW – softvér

ZTP – záložné technologické pracovisko

* 1. Základné informácie o súčasnej infraštruktúre SIEM objednávateľa:
     1. Objednávateľ používa 2 SIEM technológie:
        1. monitoring dátových tokov a detekcia anomálií v sieti postavený na technológii Flowmon
        2. zber a vyhodnocovanie logov postavený na technológii LogRhythm
     2. Technológia Flowmon je implementovaná v lokalitách HTP a ZTP nasledovne:
        1. využíva dve Flowmon sondy (Invea FlowMon Probe 20000 SFP+). Jedna Flowmon sonda je umiestnená na HTP a druhá Flowmon sonda je umiestnená na ZTP. Na každej Flowmon sonde zároveň beží Flowmon FMC. Flowmon sondy monitorujú dátové toky v lokálnej sieti objednávateľa a zozbierané dáta posielajú na Flowmon kolektory podľa lokality, t.j. Flowmon sonda na HTP posiela dáta do Flowmon kolektora na HTP a podobne Flowmon sonda na ZTP posiela zozbierané dáta do Flowmon kolektora na ZTP.
        2. využíva dva Flowmon kolektory (Invea FlowMon Collector R5-6000 Pro). Jeden Flowmon kolektor je umiestnený na HTP a druhý Flowmon kolektor je umiestnený na ZTP. Na každom Flowmon kolektore zároveň beží Flowmon ADS a Flowmon FMC. Flowmon kolektory nazbierané dáta spracovávajú a vyhodnocujú anomálie. Vyhodnotené anomálie sú posielané z Flowmon kolektorov do LogRhythm Data Collectorov (DC). Takisto Flowmon kolektory posielajú do LogRhythm DC prevádzkové a auditné informácie.
        3. operačný systém Flowmon kolektorov a Flowmon sond je pravidelne aktualizovaný ako aj modul Flowmon ADS.
        4. technológiou Flowmon sa monitorujú v LAN HTP a LAN ZTP všetky dátové toky a detegujú a vyhodnocujú anomálie v sieťovej prevádzke.
     3. Technológia LogRhythm je implementovaná v lokalitách HTP a ZTP nasledovne:
        1. Na HTP je jeden LogRhythm Platform Manager, ktorý je centrálnym prvkom celej LogRhythm architektúry. Slúži na centrálnu správu LogRhythm infraštruktúry, konfiguráciu alarmov, notifikácií, security incident management, nastavenia workflow ai.
        2. V každej lokalite (HTP a ZTP) je umiestnený jeden Data Processor na ktorom beží aj Data Indexer. Úlohou Data Processora spolu s Data Indexerom je spracovanie, indexácia a archivácia udalostí a zasielanie spracovaných udalostí v štruktúrovanej forme na ich analýzu do AI Engine a zasielanie spracovaných udalostí do LogRhythm Platform Managera na vytvorenie alarmov.
        3. V každej lokalite (HTP a ZTP) sú umiestnené dva Data Collectory, ktoré sú v rámci lokality spojené do klastra prostredníctvom aplikácie LifeKeeper. Úlohou Data Collectorov je zber logov z jednotlivých zariadení a ich bezpečné doručenie do Data Processorov. Data Collectory zbierajú logy z cca 100 zdrojov (databázy, sieťové zariadenia, iné security systémy).
        4. Na HTP je umiestnený AI Engine a umožňuje spracovávať rôzne typy udalostí vytvorením korelačných pravidiel, t.j. vzťahov medzi súvisiacimi udalosťami.
        5. Na ZTP je umiestnená LogRhythm Web Console, ktorá poskytuje používateľom jednotné web rozhranie umožňujúce pohľad v reálnom čase na udalosti, alerty a reporty spolu s analytickými nástrojmi.
        6. Na každom aktívne monitorovanom systéme (serveri) beží LogRhythm agent, ktorý štandardne zbiera udalosti zo systémových logov OS (Windows Event logy, Linux syslog) a zo špecifických aplikačných logov. LogRhyhm agenti navyše štandardne monitorujú aktivity v OS (user, proces, network, registry, file a data loss). LogRhyhm agenti sú nainštalovaní na cca 200 serveroch.
        7. operačný systém všetkých LogRhythm zariadení je pravidelne aktualizovaný a je Windows 2008 R2 okrem AI Engine, kde je Windows 2012 R2.
        8. technológiou LogRhythm sa monitorujú zariadenia v LAN HTP, LAN ZTP a DMZ (HTP a ZTP), t.j. zbierajú a vyhodnocujú sa logy z operačných systémov Windows a Linux, sieťových prvkov, databáz Oracle a MS SQL, bezpečnostných systémov (McAfee, Nesuss), mailových systémov (Lotus Notes, Exchange), infraštruktúrnych komponentov (AD, Web serverov, file serverov a pod.) a aplikačných logov systémov (Mittel, SWIFT, atď.).

Obrázok č.1 LogRhythm a Flowmon infraštruktúra

* + - 1. Flowmon licencie:
      2. Licencia pre Flowmon kolektory Flowmon Gold Support service je platná do 31.1.2020
      3. Licencia pre Flowmon sondy Flowmon Gold Support service je platná do 31.12.2019 s platnou zmluvou na automatické predĺženie platnosti licencií až do 9.6.2024.
      4. LogRhythm licencie:

Typ licencie: Non Expiring

License Type Licensed Quantity

AI Engine (MPS) 1 500

CIS Critical Security Controls 1

Data Processor (MPS) [SIEM-LM-HTP1] 1 500

Data Processor (MPS) [SIEM-LM-ZTP1] 1 500

Endpoint Threat Detection 1

Financial Fraud Detection (FFD) 1

Holistic Threat Analytics 1

Network Threat Detection 1

Platform Manager Server 1

System Monitor Lite 100

System Monitor Pro 152

User Threat Detection 1

* + - 1. Zmluva pre LogRhythm Support je platná do 31.1.2020.
  1. HW konfigurácia Flowmon zariadení:

Flowmon Collector: Invea FlowMon Collector R5-6000 Pro Physical appliance 6 TB

Flowmon Probe: Invea FlowMon Probe 20000 SFP+ Physical appliance 500 GB

* 1. HW konfigurácia LogRhythm zariadení:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Názov servera** | **RAM** | **Procesor** | **Počet logických procesorov** | **C:\ (GB)** | **D:\ (GB)** |
|
| SIEM-AI-HTP1 | 160 GB | **Intel® Xeon® CPU E5-2650 0 @ 2.00GHz** | **32** | 279 | nie je |
| SIEM-EM-HTP1 | 120 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **8** | 80 | 836 |
| SIEM-DS-ZTP1 | 64 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **4** | 80 | 272 |
| SIEM-LM-HTP1 | 64 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **8** | 80 | 1,63 TB |
| SIEM-LM-ZTP1 | 64 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **8** | 80 | 1,63 TB |
| SIEM-SLF-HTP1 | 12 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **4** | 40 | 93 |
| SIEM-SLF-HTP2 | 12 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **4** | 40 | 93 |
| SIEM-SLF-ZTP1 | 12 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **4** | 40 | 93 |
| SIEM-SLF-ZTP2 | 12 GB | **Intel® Xeon® CPU E5-2407 0 @ 2.20GHz** | **4** | 40 | 93 |

* 1. Verzie používaných SIEM technológií
     1. Flowmon OS 10.01.06
     2. Flowmon ADS 9.05.06
     3. LogRhyhm 7.2.6
  2. **Rozsah a obsah predmetu zmluvy** – predmetom zmluvy je upgrade existujúceho SIEM, predĺženie podpory a náhrada zastaraných komponentov SIEMu ktorých nie je možné predlžiť podporu, pozostávajúci z dodávky HW a SW komponentov, ich inštalácie a konfigurácie, vrátane analýzy, revízie, optimalizácie a implementácie infraštruktúry SIEM a vypracovania súvisiacej dokumentácie SIEM. Objednávateľ požaduje aby zhotoviteľ:
     1. vykonal revíziu konfigurácie súčasného stavu SIEM
     2. navrhol konfiguráciu upgradu SIEM so zreteľom na ochranu existujúcich investícií a zastarané SIEM komponenty, u ktorých nie je možné predlžiť podporu, nahradil novými podľa požiadaviek objednávateľa uvedených v časti 2
     3. navrhol postup migrácie na upgradovaný SIEM tak, aby nedošlo k ovplyvneniu produkčnej prevádzky systémov objednávateľa
     4. navrhol akceptačné testy funkčných čŕt upgradu SIEM a v spolupráci s objednávateľom tieto testy vykonal
     5. vykonal migráciu, vrátane dodávky, inštalácie a konfigurácie nových komponentov SIEM v oboch lokalitách objednávateľa (HTP, ZTP)
     6. zabezpečil školenie zamestnancov objednávateľa v požadovanom rozsahu
     7. vypracoval súvisiacu dokumentáciu podľa požiadaviek objednávateľa uvedených v časti 2

#### Technické požiadavky

**Všeobecné požiadavky**

* 1. Upgrade SIEM musí byť navrhnuté tak, aby využívalo existujúce technológie a licencie LogRhythm a Flowmon.
  2. Navrhovaný upgrade SIEM musí poskytovať funkčnosť minimálne v rozsahu funkčnosti existujúceho SIEM riešenia v prípade, že nebola odstránená výrobcom.
  3. Zhotoviteľ v ugradovanom SIEM navrhne optimalizovanú architektúru SIEM s dôrazom na zníženie počtu SIEM HW komponentov pri zachovaní funkčnosti a výkonu SIEM.
  4. Upgradované SIEM musí obsahovať HW a SW komponenty, ktorým výrobca deklaruje podporu minimálne na 5 rokov. Táto požiadavka sa vzťahuje aj na komponenty, ktoré nebudú nahradené.
  5. Upgradované SIEM musí byť navrhnuté tak, aby ho bolo možné nasadiť „on premise“.
  6. Upgradované SIEM musí byť komponentovo nezávislé od prvkov sieťovej infraštruktúry, tak aby po výmene sieťových komponentov tej istej kategórie od rovnakého výrobcu nedošlo k obmedzeniu alebo znefunkčneniu upgradovaného SIEM.
  7. Upgradované SIEM musí byť postavené na štandardných HW a SW produktoch výrobcov.
  8. Žiadne z dodaných zariadení ani ich modulov a ani SW pre ich správu nesmie byť v čase predloženia ponuky na zozname výrobcu oznamujúcom koniec predaja (End of Sale) alebo koniec životnosti (End of Life).
  9. Súčasťou plnenia musia byť všetky HW a SW komponenty (HW + OS + SW serverov a storage, databázová infraštruktúra, SAN konektory a pod.) vrátane všetkých licencií, umožňujúce v prostredí objednávateľa používať a spravovať upgradované SIEM od prvého dňa nasadenia.
  10. Všetky zariadenia musia obsahovať firmvér alebo operačný systém v poslednej výrobcom doporučenej verzii v čase predloženia ponuky pre daný typ zariadenia a takisto rovnaké typy zariadení musia obsahovať rovnaký firmvér alebo operačný systém.
  11. Všetky systémy a zariadenia, ktoré sú predmetom plnenia musia spĺňať požadovanú funkčnosť, technické parametre a špecifikácie, zároveň to musia byť nové nerepasované zariadenia.

**Požiadavky na funkčnosť, výkon a škálovateľnosť**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na funkčnosť:

* 1. Primárny centrálny systém na HTP (LogRhythm Gen5 XM Appl45xx with minimal 1000 MPS Log Volume license and unlimited log sources (All in one DP, DI, PM, AI). Includes Advanced Intelligence Engine with minimal 2000 MPS license (transferable). Windows Server 2016 Standard. SQL Server 2016 Standard with 10CAL Enterprise License for Gen5 Appliances).

Úlohou (primárneho) centrálneho systému na HTP (ďalej len HTP CS) bude zabezpečovať spracovanie dát a komunikáciu s LogRhythm infraštruktúrou (LogRhythm agenti, Network Monitory) a združovať všetky potrebné komponenty SIEMu pre jeho beh (PM platform manager, DP data processor, DI data indexer, AI advanced intelligence korelačná jednotka, WC web console).

Systém musí umožniť spracovať min. 1000 log záznamov za sekundu vrátane Advanced Intelligence Engine s možnosťou transferu licencií medzi jednotlivými zariadeniami (appliance).

* 1. Sekundárny centrálny systém na ZTP (XM45xx Appliance HW, OS+ iDRAC Enterprise License for Gen5 Appliances).

Sekundárny centrálny systém na ZTP (ďalej len ZTP CS) s rovnakou funkcionalitou ako na HTP bude nakonfigurovaný v disaster recovery móde (failover), ktorý bude slúžiť ako záložný systém pre prípadné výpadky primárneho systému.

* 1. Data Collector na HTP zapojený v HA clustery (Site log forwarder DC-SLF HA cluster hw refresh)

Na HTP budú 2 Data Collector-y (ďalej HTP DC) zapojené v HA clustery, tak aby bola zabezpečená vysoká dostupnosť zberu dát. Dáta budú zbierané z HTP prostredia a posielané na HTP CS. V prípade výpadku HTP CS budú dáta zasielané z HTP DC na ZTP CS.

* 1. Data Collector na ZTP (Site log forwarder DC-SLF hw refresh).

Na ZTP bude 1 Data Collector (ZTP DC). Dáta budú zbierané zo ZTP prostredia a posielané na HTP CS. V prípade výpadku HTP CS budú dáta zasielané zo ZTP DC na ZTP CS.

* 1. LogRhythm Network monitor Appliance. Includes license for minimal 500 Mb/s, HW, OS+ iDRAC Enterprise License for Gen5 Appliances na http.

Monitoring aktivít používateľov pri komunikácií s vonkajším svetom (externé siete, resp. internet) bude zabezpečovať LogRhythm Network Monitor (NM). NM bude zapojený tak, aby monitoroval a vyhodnocoval správanie používateľov a detegoval použité aplikácie. Jeden NM bude umiestnený v HTP lokalite a druhý NM bude umiestnený v ZTP lokalite. Nazbierané dáta budú posielané do HTP DC, resp. ZTP DC pre ďalšie vyhodnotenie a obohatenie nazbieraných informácií.

* 1. LR XM 10 Gb Eth Adapter with optical transceivers Gen5 pre primárny a sekundárny centrálny systém na HTP a ZTP.
  2. LogRhythm Dual Fiber Channel Qlogic/Emulex HBA Card for Gen4/Gen5 Appliances pre primárny a sekundárny centrálny systém na HTP a ZTP

Fiber Channel bude určený na pripojenie LogRhythm infraštruktúry na externé SAN úložisko s priepustnosťou min. 10Gbit/s. Pripojenie bude slúžiť ako externý a archivačný storage pre logy a dáta.

* 1. Flowmon Collector R5-6000PRO HW + iDRAC na HTP a ZTP (HW refresh)

Analýza zozbieraných dát z Flowmon sond bude vykonávaná vo Flowmon kolektoroch. Jeden Flowmon kolektor bude umiestnený na HTP lokalite a bude spracovávať dáta z Flowmon sond z HTP lokality a druhý Flowmon kolektor bude umiestnený na ZTP lokalite a bude spracovávať dáta zo ZTP lokality. Spracované informácie budú posielané formou udalostí (eventov) do HTP DC, resp. ZTP DC podľa lokality.

* 1. Flowmon ADS business

Detekcia a analýza anomálií v sieťových tokoch bude zabezpečená softvérovým modulom Flowmon ADS business. Moduly budú nainštalované vo Flowmon kolektoroch.

* 1. Flowmon Sonda IFP-40000-SFP+ (4x10Gbps) na HTP a ZTP

Monitoring sieťových tokov v lokálnej dátovej sieti (LAN) bude zabezpečený Flowmon sondami umiestnenými v LAN a informácie o dátových tokoch budú posielané z core prepínačov na tieto sondy. Jedna Flowmon sonda bude umiestnená v HTP lokalite a druhá Flowmon sonda bude umiestnená v ZTP lokalite.

Monitoring sieťových tokov v demilitarizovanej zóne (DMZ) bude zabezpečený Flowmon sondami umiestnenými v DMZ a informácie o dátových tokoch budú posielané z vybraných DMZ na tieto sondy. Jedna Flowmon sonda bude umiestnená v HTP lokalite a druhá Flowmon sonda bude umiestnená v ZTP lokalite.

* 1. LogRhytm System Monitor Pro

LogRhytm System Monitor Pro bude zabezpečovať bez agentový zber dát z monitorovaných systémov.

* 1. LogRhythm System Monitor Lite

LogRhythm System Monitor Lite bude zabezpečovať zber dát priamo z monitorovaných systémov (agentový zber dát).

* 1. LogRhythm infraštruktúra musí na každom pracovisku objednávateľa umožniť interne uložiť udalosti po dobu min. 10 dní, t.j. min. 650 miliónov záznamov na HTP a min. 650 miliónov záznamov na ZTP.
  2. Flowmon infraštruktúra musí na každom pracovisku objednávateľa umožniť interne uložiť udalosti po dobu min. 10 dní, t.j. min. 10 miliárd záznamov na HTP a min. 10 miliárd záznamov na ZTP.
  3. Upgrade SIEM musí podporovať súčasnú prácu min. 10 používateľov v obidvoch lokalitách, t.j. 10 používateľov na HTP alebo 10 používateľov na ZTP.

**Požiadavky na technológie**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na technológie:

* 1. Upgradované zariadenia musia byť montovateľné do štandardného 19’’ technologického stojana (montážna sada súčasťou dodávky) s pripojením ku dvom samostatným zdrojom napájania 230V, dĺžka napájacích káblov min. 3m ukončenými IEC 60 884-1 a IEC320 C14 (oba typy napájacích káblov sú súčasťou dodávky) a obsahovať min. 2x LAN port, každý aspoň 1Gbit/s.

**Požiadavky na prevádzku**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na prevádzku:

* 1. Upgrade SIEM musí byť navrhnutý minimálne s výhľadom na 5 rokov a uchádzač sa zaviaže, že počas tejto doby bude poskytovať na upgrade SIEM zmluvný servis ako aj priebežnú aktualizáciu upgradovaného SIEM.

**Požiadavky na integráciu**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na integráciu:

* 1. Zhotoviteľ v rámci funkčnej špecifikácie vykoná revíziu pôvodných nastavení LogRhythm a Flowmon a navrhne prípadné zmeny integračných nastavení vyplývajúce zo zmeny SIEM architektúry a požiadaviek objednávateľa.
  2. Rozsah integrácie musí pokrývať všetky integračné rozhrania a komunikácie v pôvodných systémoch LogRhythm a Flowmon (Microsoft AD, McAfee ePO atď)

**Požiadavky na zber dát**

Objednávateľ požaduje, aby upgrade spĺňal minimálne nasledujúce požiadavky na zber dát.

* 1. Zhotoviteľ v rámci funkčnej špecifikácie vykoná revíziu pôvodných nastavení LogRhythm a Flowmon a navrhne prípadné zmeny nastavení zberu dát vyplývajúce zo zmeny SIEM architektúry a požiadaviek objednávateľa, pričom počet zdrojov udalostí a monitorovaných systémov sa nezmení.

**Požiadavky na spracovanie udalostí**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na spracovanie udalostí:

* 1. Zhotoviteľ v rámci funkčnej špecifikácie vykoná revíziu pôvodných nastavení LogRhythm a Flowmon a navrhne, podľa požiadaviek objednávateľa, prípadné zmeny spracovania udalostí pomocou Message Processing Engine (MPE), pričom počet zdrojov udalostí a monitorovaných systémov sa nezmení.
  2. Zhotoviteľ v rámci funkčnej špecifikácie navrhne, podľa požiadaviek objednávateľa, a v rámci implementácie vytvorí konfiguračné politiky pre System Monitor Agentov (Windows, Linux).
  3. Zhotoviteľ v rámci funkčnej špecifikácie navrhne, podľa požiadaviek objednávateľa, a v rámci implementácie mennú konvenciu pre vytváranie objektov v LogRhythm a Flowmon.

**Požiadavky na ukladanie a archiváciu udalostí**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na ukladanie a archiváciu udalostí:

* 1. Zhotoviteľ v rámci funkčnej špecifikácie vykoná revíziu pôvodných nastavení LogRhythm a Flowmon a navrhne prípadné zmeny nastavení ukladania a archivácie udalostí vyplývajúce zo zmeny SIEM architektúry a požiadaviek objednávateľa.
  2. Objednávateľ požaduje aby bol zachovaný prístup z upgradovaného LogRhythm riešenia k archívnym dátam/udalostiam pôvodného LogRhythm riešenia.

**Požiadavky na správu a bezpečnosť**

Objednávateľ požaduje, aby upgrade SIEM spĺňal minimálne nasledujúce požiadavky na správu a bezpečnosť:

* 1. Zhotoviteľ v rámci funkčnej špecifikácie vykoná revíziu pôvodných nastavení LogRhythm a Flowmon a navrhne prípadné zmeny nastavení týkajúce sa správy a bezpečnosti SIEM vyplývajúce zo zmeny SIEM architektúry a požiadaviek objednávateľa.
  2. Upgradovaný upgrade SIEM musí byť nadimenzovaný tak, aby umožnilo prácu minimálne 10 súčasne pripojených používateľov do LogRhythm Web Console v obidvoch lokalitách, t.j. 10 používateľov na HTP alebo 10 používateľov na ZTP.
  3. Dodané komponenty SIEM musia umožniť ich vzdialený manažment (napr. iDRAC) cez dedikovaný LAN manažment port.

#### Požiadavky na implementačné práce a služby

Objednávateľ požaduje aby zhotoviteľ v rámci realizácie predmetu zmluvy dodal vo obidvoch lokalitách objednávateľa nasledovné implementačné práce a služby v zmysle bodu 2 Technologické požiadavky.

**Všeobecné požiadavky:**

* 1. Zhotoviteľ v rámci upgradu SIEM vypracuje funkčnú špecifikáciu – detailný technický popis cieľového stavu upgradu SIEM a ako aj postup prechodu na cieľový stav v súlade so zmluvou a požiadavkami objednávateľa. Funkčná a technická špecifikácia systému musí obsahovať minimálne:
     1. schému a popis zapojenia jednotlivých komponentov
     2. konfiguračné parametre LogRhythm a Flowmon zariadení
     3. konfigurácia LogRhythm prostredia (entity, system monitors, log sources, AI rules, users, ...)
     4. konfigurácia Flowmon prostredia (Configuration Center, FMC a ADS)
     5. definície menných konvencií pre vytvorené objekty v LogRhythm a Flowmon
     6. popis integračné rozhraní a komunikácie
     7. popis nastavení zberu dát (LogRhythm a Flowmon)
     8. popis spracovania udalostí pomocou Message Processing Engine (MPE)
     9. popis nastavení konfiguračných politík pre System Monitor Agentov (Windows, Linux)
     10. popis nastavení týkajúce sa správy a bezpečnosti upgradu SIEM
     11. popis nastavení pravidelnej automatickej archivácie logov
     12. popis migrácie nastavení z pôvodného prostredia LogRhythm a Flowmon do upgradovaného prostredia LogRhythm a Flowmon
     13. popis migrácie dát z pôvodného prostredia LogRhythm a Flowmon do upgradovaného prostredia LogRhythm a Flowmon
     14. popis migrácie use casov, custom reportov a nastavení z pôvodného prostredia LogRhythm a Flowmon do upgradovaného prostredia LogRhythm a Flowmon
     15. popis konfigurácie automatického zálohovania systémov LogRhythm a Flowmon.
     16. popis postupov pre diaster recovery (LogRhythm a Flowmon)
  2. Zhotoviteľ realizuje implementáciu upgradovaného SIEM tak, aby bola počas celej implementácie zachovaná prevádzka existujúceho SIEM, resp. v nevyhnutných prípadoch prerušená len na minimálny čas.
  3. Zhotoviteľ v rámci upgradu SIEM vypracuje časový plán inštalácie a konfigurácie LogRhythm a Flowmon a plán migrácie z pôvodného na upgradovaný systém v prostredí objednávateľa s odhadom nutnej súčinnosti zamestnancov objednávateľa.

**Požiadavky na dodávku, montáž a inštaláciu upgradovaného SIEM**

* 1. Zhotoviteľ dodá a zabezpečí montáž a inštaláciu všetkých komponentov do technologických stojanov podľa požiadaviek objednávateľa na HTP a ZTP, vrátane označenia káblov.
  2. V prípade potreby uvoľnenia potrebného priestoru v technologických stojanoch zhotoviteľ presunie existujúce zariadenia v technologických stojanoch.
  3. Zhotoviteľ zabezpečí demontáž zariadení, ktoré budú nahradené novými zariadeniami. Náklady spojené s demontážou a odvozom zariadení bude znášať zhotoviteľ.
  4. Zhotoviteľ zabezpečí bezpečné vymazanie konfigurácie demontovaných zariadení a vymazanie dát na nich uložených.
  5. Zhotoviteľ zabezpečí vzájomne prepojenie dodaných zariadení, ako i prepojenie dodaných zariadení so zariadeniami objednávateľa a zariadeniami ktoré nebudú nahradené, kde to bude potrebné, kabelážou priamo, resp. cez existujúce patch panelové prepojenia.
  6. Zhotoviteľ zabezpečí inštaláciu a konfiguráciu upgradovaného prostredia LogRhythm a Flowmon podľa funkčnej špecifikácie.
  7. Zhotoviteľ zabezpečí migráciu dát z pôvodného prostredia LogRhythm a Flowmon do upgradovaného prostredia LogRhythm a Flowmon podľa funkčnej špecifikácie.
  8. Zhotoviteľ zabezpečí migráciu nastavení z pôvodného prostredia LogRhythm a Flowmon do upgradovaného prostredia LogRhythm a Flowmon podľa funkčnej špecifikácie.
  9. Zhotoviteľ zabezpečí migráciu use casov, custom reportov a nastavení z pôvodného prostredia LogRhythm a Flowmon do upgradovaného prostredia LogRhythm a Flowmon podľa funkčnej špecifikácie.
  10. Zhotoviteľ zabezpečí konfiguráciu pravidelnej automatickej archivácie logov podľa funkčnej špecifikácie.
  11. Zhotoviteľ zabezpečí konfiguráciu automatického zálohovania systémov (NetBackup – Veritas) LogRhythm a Flowmon.
  12. Zhotoviteľ zabezpečí dodávku a inštaláciu aktuálneho softvérového vybavenia vrátane firmvéru na všetky dodávané zariadenia.

**Požiadavky na testovanie upgradovaného SIEM**

* 1. Zhotoviteľ vypracuje testovacie scenáre pokrývajúce testovanie všetkých funkčných čŕt implementovaného upgradovaného SIEM, vrátane testovania vybraných výkonových parametrov a výpadkov jednotlivých komponentov.
  2. Zhotoviteľ vykoná testovanie upgradovaného SIEM v spolupráci s objednávateľom.

**Dokumentácia**

* 1. Zhotoviteľ dodá dokumentáciu k upgradovanéhmu SIEM v elektronickej verzii vo formátoch MS Word, Excel a Visio.
  2. Zhotoviteľ vypracuje podrobnú technickú dokumentáciu implementovaného upgradu SIEM, ktorá nad rámec funkčnej špecifikácie bude zahŕňať minimálne:
     1. detailný popis a schému funkčného prepojenia SIEM komponentov
     2. detailný popis a schému fyzického zapojenia dodaných zariadení (el. kabeláž, LAN a SAN)
     3. detailný popis konfigurácie jednotlivých zariadení (hostname, IP adresy, HW, OS, SW, komunikujúce porty a pod.)
     4. detailný popis bezpečnostných čŕt a ich konfigurácie
     5. detailný popis vykonaných natívnych aj custom integrácií so systémami objednávateľa, ich nastavení a konfigurácií, vrátane dodania kompletných zdrojových kódov s popisom kódu a použitých vývojových prostredí
     6. detailný popis zálohovania, archivácie a obnovy logov a dát pre analýzu a vyhľadávanie v historických údajoch s prepojením na zálohovací systém objednávateľa
     7. detailný popis integrácie s centrálnym monitorovacím systémom dostupnosti objednávateľa
  3. Zhotoviteľ vypracuje podrobnú prevádzkovú dokumentáciu implementovaného upgradu SIEM a príslušných zariadení, ktorá nad rámec funkčnej špecifikácie bude zahŕňať minimálne:
     1. detailné postupy pravidelnej údržby a profylaktiky
     2. detailné postupy diagnostiky a monitorovania prevádzky
     3. detailné postupy riešenia havarijných stavov
     4. detailné postupy zálohovania, archivácie a obnovy konfigurácií zariadení, systémov a dát
     5. detailné postupy pre failover primárneho systému (súbor postupov, ktoré umožnia obnovu služby na záložnom, sekundárnom zariadení)

**Požiadavky na školenia**

* 1. Zhotoviteľ zabezpečí realizáciu školení správcov objednávateľa pre dodávané zariadenia a systémy v rozsahu umožňujúcom správcom vykonávať:
     1. bežnú rutinnú prevádzku a údržbu dodaného upgradu SIEM, vrátane vykonania príslušných konfiguračných zmien,
     2. monitoring stavu SIEM komponentov,
     3. diagnostiku a riešenie problémov s funkčnosťou a dostupnosťou SIEM komponentov,
     4. zálohovanie a obnovu konfiguračných nastavení,
     5. obnovu logov a dát pre dodatočnú analýzu zaznamenaných údajov,
     6. tvorbu pohľadov a reportov,
     7. konfiguráciu SIEM komponentov (vrátane všetkých nových čŕt implementovaného upgradu SIEM).