# Technická špecifikácia pre službu LMS, SIEM a SOC

## Úvodné informácie

Predmetom tohto výberového konania je výber dodávateľa na poskytovanie služby Security operations center (SOC), Security Information and Event Management (SIEM) a centrálny Log management system (LMS) v rozsahu a kvalite, ktorú vyžaduje Zákon o kybernetickej bezpečnosti 69/2018 Z. z. (ďalej iba ZoKB), §15, odst. 2 d) a Vyhl. NBÚ č.362/2018.

Ďalšou oblasťou výberového konania je aktualizácia internej bezpečnostnej dokumentácie verejného obstarávateľa podľa šablón smerníc, ktoré zverejňuje Ministerstvo investícií, regionálneho rozvoja a informatizácie a odstránenie nesúladov v dokumentačnej časti zo zákonného auditu kybernetickej bezpečnosti.

## Predmet zákazky

Verejný obstarávateľ požaduje od uchádzača zabezpečenie bezpečnostného monitoringu relevantných informačných systémov verejného obstarávateľa tak, aby bola zaistená dôvernosť, pravosť, integrita a dostupnosť jeho dát a základných služieb v súlade so ZoKB.

Služby bezpečnostného monitoringu musia byť poskytované prostredníctvom osobitného pracoviska, ktoré bude v rámci služby SOC zastrešovať aj činnosti CSIRTu (Computer Security Incident Response Team) takým spôsobom, aby bola zaistená prvotná reakcia na vzniknutý incident s prvotnou analýzou príčin vzniku bezpečnostnej udalosti a jej popisom a odovzdanie udalosti na riešenie verejnému obstarávateľovi v súlade s požadovaným SLA a stanovenou cestou.

Dodávateľ služby SOC a CSIRT musí súčasne disponovať kapacitami na následné vypracovanie návrhov opatrení na elimináciu dopadu bezpečnostnej udalosti na informačné systémy verejného obstarávateľa.

Presná špecifikácia služieb a formy ich objednávania je uvedená v kapitole 3 a v kapitole 4.

Predmet zákazky pozostáva z nasledovných činností:

1. Poskytovanie služby pracoviska bezpečnostného monitoringu na úrovni L1 v režime 8/5, pričom súčasťou služby je:

a. HW infraštruktúra pre processing SIEM

b. HW infraštruktúra pre uchovanie dát v rozsahu zákonnej povinnosti

c. SW nástroj SIEM na bezpečnostný monitoring

d. SW nástroj na evidenciu životného cyklu bezpečnostného incidentu

e. SW nástroj na centrálny zber a prehľadávanie logov zo zariadení obstarávateľa v rozsahu ako je definované v Prílohe „Sizing“

2. Riešenie detegovaných bezpečnostných udalostí podľa stanovených postupov

3. Dizajn a koordinácia procesov súvisiacich s funkcionalitou SOC a CSIRT v súlade s bezpečnostnou stratégiou verejného obstarávateľa

4. Sledovanie a evidencia životného cyklu udalostí

5. Podpora verejného obstarávateľa na úrovni L2 a L3 pri riešení detegovaných udalostí

6. Podpora verejného obstarávateľa pri komunikácii s NBÚ a tretími stranami (napr. dodávateľmi)

Ďalšou oblasťou predmetu zákazky je aktualizácia bezpečnostnej dokumentácie a odstránenie nesúladov v dokumentácii na základe auditu kybernetickej bezpečnosti podrobne popísaná v kapitole 3.6.

## Požiadavky na predmet zákazky

Predmet zákazky musí spĺňať minimálne požiadavky uvedené v tejto kapitole.

#### Definícia pojmov:

**Bezpečnostná udalosť**(ďalej len „udalosť“) - event, anomália, hrozba a pod., ktorá nespĺňa parametre bezpečnostného incidentu podľa Vyhl. NBÚ č.165/2018 alebo definície incidentu v zmysle požiadavky verejného obstarávateľa

**Bezpečnostný incident** (ďalej len „incident“) - udalosť, ktorá spĺňa parametre bezpečnostného incidentu podľa Vyhl. NBÚ č.165/2018 alebo definície bezpečnostného incidentu v zmysle požiadavky verejného obstarávateľa

**Doba poskytovania služby** - doba, počas ktorej je služba dostupná.

**Čas vzniku udalosti alebo incidentu** - časová značka v SIEM nástroji.

**Doba odozvy na udalosť alebo incident** - maximálna doba, počas ktorej bude udalosť alebo incident detegovaná a zaevidovaná formou ticketu v evidenčnom nástroji.

**Doba analýzy udalosti alebo incidentu** - maximálna doba, počas ktorej bude vykonaná analýza a ostatné stanovené kroky a udalosť alebo incident bude postúpený na riešenie verejnému obstarávateľovi cestou definovanou v príslušnom postupe (napr. preklopenie ticketu na riešiteľskú skupinu, čas telefonického hovoru, čas odoslania mailu).

**Doba ukončenia udalosti alebo incidentu** - čas, kedy bude uzatvorený ticket na udalosť alebo incident na základe informácie od riešiteľa udalosti alebo incidentu – verejného obstarávateľa alebo ním stanovenej tretej strany.

### 3.1 Požiadavky na HW infraštruktúru, SW nástroj SIEM a SW nástroj na evidenciu životného cyklu bezpečnostných incidentov

#### Špecifikácia požiadaviek na HW infraštruktúru a parametre jej poskytovania:

* Spracovanie logov a iných zdrojov dát pre bezpečnostný monitoring v počiatočnom objeme približne 1500 EPS, čo predstavuje cca 130 GB denne (oba údaje sú iba odhadnuté) **zo systémov verejného obstarávateľa podľa Prílohy „Sizing“**
* Dodávateľ musí navrhnúť a poskytnúť takú kapacitu diskového priestoru, ktorý umožní archivovanie, prehliadanie a filtrovanie všetkých zaslaných logov, auditných logov a logov vzniknutých vlastnou činnosťou SIEM počas 180 dní **zo systémov podľa**

**Prílohy „Sizing“** a **to minimálne v rozsahu definovanom v Prílohe č. 2 vyhlášky č. 179/2020 Z. z. k zákonu č. 95/2019 Z. z.**

* HW infraštruktúra, na ktorej budú dáta spracovávané, musí byť identifikovateľná
* Prevádzkovanie HW infraštruktúry musí spĺňať požiadavky ZoKB najmä §20, odst. 3 a musí umožniť obstarávateľovi výkon kontrolnej činnosti alebo auditu v súlade s Vyhl. NBÚ č.362/2018, §8, odst. 2, písm. h)
* Dostupnosť HW infraštruktúry bude spĺňať požiadavky uvedené v kap. 3.4
* Prenos dát medzi dátovými zdrojmi verejného obstarávateľa a HW infraštruktúrou bude šifrovaný
* Prenos dát medzi dátovými zdrojmi verejného obstarávateľa a HW infraštruktúrou bude riešený prostredníctvom dedikovanej linky v prípade, že HW infraštruktúra nebude v areáli verejného obstarávateľa. Kapacitu dedikovanej linky stanoví uchádzať v rámci návrhu svojho riešenia. Dostupnosť dedikovanej linky bude spĺňať požiadavky uvedené v kap. 3.4.

#### Špecifikácia požiadaviek na SW nástroje a parametre ich poskytovania:

* Spracovanie logov a iných zdrojov dát pre bezpečnostný monitoring v počiatočnom objeme približne 1500 EPS, čo predstavuje cca 130 GB denne **zo systémov podľa Prílohy „Sizing“**
* LMS musí umožňovať prístup aj pre administrátorov verejného obstarávateľa a umožniť im plnohodnotne prehľadávať uložené logy aj bez súčinnosti dodávateľa s možnosťou uloženia rôznych „pohľadov“ na tieto logy, možnosť exportu logov a to po celú dobu retencie dát
* LMS musí umožňovať prehľady o všetkých pripojeniach a využití Internetovej linky z logov firewallu - kto, kde (IP adresa), kedy a koľko (prenesené dáta v oboch smeroch) po celú dobu retencie dát. Prehľad by malo byť možné vytvoriť tak ako pre jedného užívateľa (IP adresu) tak aj pre všetkých užívateľov za ľubovoľné obdobie.
* V SIEM nástroji možnosť spracovať logy zo všetkých informačných systémov verejného obstarávateľa uvedených v Prílohe „Sizing“ čo do typu aj objemu dát
* Prezentácia spracovaných dát operátorovi a umožnenie ďalšej analýzy tak, aby boli splnené požiadavky na reakciu na bezpečnostnú udalosť uvedené v kapitole 3.4
* Počet definovaných korelačných pravidiel – min. 20
* Korelačné pravidlá musia byť prekonzultované a odsúhlasené verejným obstarávateľom
* Minimálny počet MD na definovanie a doladenie korelácií - 20
* Súčasťou prevádzkovania nástroja bude jeho pravidelná údržba min. v rozsahu:
	+ kontrola dát,
	+ asset manažment,
	+ access manažment,
	+ aktualizácie,
	+ zálohovanie,
	+ ostatné činnosti prevádzkového charakteru
* Možnosť rozšírenia bezpečnostného monitoringu pre nové informačné technológie verejného obstarávateľa minimálne do odhadnutého počtu nových zariadení, ktoré pribudnú verejnému obstarávateľovi do konca doby podpory (5 rokov) podľa Prílohy „Sizing“, a to v dohodnutej cene.
* Prevádzkovanie SIEM nástroja musí spĺňať požiadavky ZoKB, najmä §20, odst. 3 a musí umožniť verejnému obstarávateľovi výkon kontrolnej činnosti alebo auditu v súlade s Vyhl. NBÚ č.362/2018, §8, odst. 2, písm. h)
* SW nástroj na evidenciu životného cyklu bezpečnostných incidentov bude spĺňať min. nasledovné požiadavky:
	+ prístup pre verejného obstarávateľa umožňujúci sledovanie incidentov v režime „read only“
	+ vytváranie periodických reportov (týždenné, mesačné) a reportov na vyžiadanie
	+ poskytne informácie min. v rozsahu §24 ZoKB
* Dostupnosť SW nástrojov bude spĺňať požiadavky uvedené v kap. 3.4.
* SW nástroje musia umožňovať rozšírenie pre spracovanie logov a udalostí zo zdravotníckych prístrojov (OT svet), ktoré bude možno verejný obstarávateľ potrebovať v neskorších etapách.

### 3.2 Požadované činnosti SOC počas trvania zmluvy s dodávateľom – L1

#### Špecifikácia činností – podpora L1:

* aktívny monitoring minimálne v rozsahu §14, ods. 4 a §15, ods. 2 Vyhl. NBÚ č.362/2018 v režime 8/5 s trvalou prítomnosťou operátora,
* v čase mimo režim 8/5 nastavenie automatickej notifikácie udalostí
* detekcia udalosti alebo incidentu v rozsahu §14, ods. 3 Vyhlášky NBÚ č. 362/2018,
* doba odozvy - prvotná reakcia na udalosť alebo incident v súlade s SLA,
* doba analýzy - zabezpečenie základného popisu udalosti alebo incidentu a krokov, ktoré boli realizované a postúpenie udalosti alebo incidentu na riešenie verejného obstarávateľa podľa stanovených postupov a v súlade s SLA
* klasifikácia a priorizácia incidentu v súlade Vyhl. NBÚ č.165/2018,
* evidencia detegovaných bezpečnostných udalostí a incidentov v nástroji dodávateľa a sledovanie ich životného cyklu,
* zníženie ich dopadov v reakčných časoch primeraných kategórii incidentu,
* reporting (denný, týždenný, mesačný, na vyžiadanie) podľa jeho špecifikácie verejného obstarávateľa definovanej vo fáze 2,
* zdieľanie informácií, vedomostí a znalostnej databázy zachytených incidentov,
* spolupráca na priebežnom ladení data modelov/korelačných pravidiel v súlade s potrebami monitorovanej infraštruktúry a dostupnosťou potrebných informácií,
* dopĺňanie korelačných pravidiel v nadväznosti na možnosti monitorovanej technológie a požiadavky verejného obstarávateľa v rozsahu implementovaného riešenia,
* spracovanie SOC dokumentácie – playbook a ostatná SOC dokumentácia customizovaná na podmienky verejného obstarávateľa, ktorá bude priebežne aktualizovaná

### 3.3 Požadované činnosti SOC počas trvania zmluvy s dodávateľom – L2, L3

V cene v rozsahu 1 MD mesačne počas etapy 4 -štandardná prevádzka. Nevyužité MD je možné v rámci jedného roku preniesť do ďalšieho mesiaca. Na konci každého roku sa nevyžité MD vynulujú bez náhrady.

#### Špecifikácia činností – podpora L2, L3:

* získanie doplňujúcich informácií o prostredí počas vzniku udalosti alebo incidentu, prípadne dodatočných informácií zo zdrojových systémov, použitím dostupných technických prostriedkov a dokumentácie verejného obstarávateľa,
* komunikácia s dohodnutými zástupcami verejného obstarávateľa ohľadom prípadného dodania dodatočných informácií,
* L2 podpora pri zotavení sa z incidentov,
* L2/L3 podpora pri vyšetrovaní koreňových príčin incidentov ,
* rozpoznávanie vzorcov správania poukazujúcich na známe druhy útokov
* využívanie informácií o kritických zraniteľnostiach poskytovaných výrobcami IT technológií (CVE) a informáciách o aktuálnych hrozbách a relevantných útokoch
* podpora pri komunikácii s národným CSIRT, NBÚ a inými tretími stranami napr. dodávateľmi monitorovanej technológie a pod.

Dodávateľ teda musí disponovať nasledovnými personálnymi kapacitami:

* **L2 SOC analytik** – konzultácie a služby na úrovni IT security analytik, t.j. činnosti typu podpora pri vyšetrovaní koreňových príčin incidentov, podpora pri komunikácii s tretími stranami napr. dodávateľmi monitorovanej technológie, vytváranie a update postupov pre jednotlivé typy hrozieb, komunikácia so zákazníkom a súvisiacimi tretími stranami v nadväznosti na riešené udalosti
* **L3 SOC expert** – konzultácie a služby na úrovni IT security expert, vykonávanie hĺbkovej analýzy koreňových príčin vrátane podpory pri analýze zákazníka v jeho prostredí a pri šetrení bezpečnostných incidentov s národným CSIRT/NBU príp. inými orgánmi, spolupráca a súčinnosť pri posúvaní rozhrania činnosti SOCu smerom k vykonaniu aj aktívnych zásahov na monitorovanej sieti v prípade bezpečnostného incidentu, podpora a súčinnosť pri riešení asset manažmentu pre SOC

### 3.4 SLA

#### Špecifikácia požiadaviek na SLA:

**Dostupnosť HW infraštruktúry pre procesing dát** – min. 99,4% s tým, že jeden samostatný výpadok funkčnosti systému bude mať maximálnu dobu výpadku 12 hod. Do tohto času sú zahrnuté aj plánované prevádzkové výpadky

**Dostupnosť dedikovanej linky** – min. 98,0%. Do času nedostupnosti sa nezapočítava čas, kedy je linka nedostupná z dôvodu na strane verejného obstarávateľa

**Dostupnosť SW nástrojov** – min. 99,4% s tým, že jeden samostatný výpadok funkčnosti systému bude mať maximálnu dobu výpadku 12 hod. Do tohto času sú zahrnuté aj plánované prevádzkové výpadky

#### SLA pre službu SOC:

Doba poskytovania služby SOCu: 8/5

Dodávateľ musí byť schopný počas dohodnutej doby podpory (5 rokov) umožniť zmeniť dobu poskytovania služby na 24/7 na požiadanie verejného obstarávateľa a aj ju v plnej miere obsadiť kvalifikovanými zamestnancami podľa dohodnutých kvalifikačných parametrov. Prechod služby na 24/7 bude predmetom nového obstarania.

#### Incident:

Doba odozvy od času vzniku incidentu (časová značka podľa SIEM):

* 15 minút - prevzatie incidentu, pridelenie evidenčného čísla a eskalácia podľa dohodnutého postupu na verejného obstarávateľa alebo ním stanovenú tretiu stranu,
* 90 minút – poskytnutie výstupu z prvotnej analýzy pre riešiteľa vopred stanovenou cestou (na verejného obstarávateľa alebo ním stanovenú tretiu stranu)

#### Udalosť:

Doba odozvy od času vzniku udalosti (časová značka podľa SIEM):

* 90 minút - prevzatie udalosti, pridelenie evidenčného čísla a eskalácia podľa dohodnutého postupu na verejného obstarávateľa alebo ním stanovenú tretiu stranu,
* 8 hodín – poskytnutie výstupu z prvotnej analýzy pre riešiteľa vopred stanovenou cestou (na verejného obstarávateľa alebo ním stanovenú tretiu stranu)

### 3.5 Požiadavky na implementáciu služby SOC

Očakávané etapy implementácie služby a sú popísané v kapitolách 3.5.1 – 3.5.4. Uchádzač môže činnosti alebo rozdelenie do etáp zmeniť podľa ponúkaného riešenia, ale musí dodržať limity harmonogramu v prílohe „Kalkulácia ceny“.

#### Etapa 1 – Analýza a Dizajn:

* príprava HW infraštruktúry
* zrealizovanie dedikovanej linky
* analýza výberu vhodných logov podľa typov zariadení
* analýza parserov pre logy z kritických informačných systémov – NIS, LIS, PACS
* inštalácia SW (SIEM, LMS)
* aktualizácia bezpečnostnej dokumentácie podľa kapitoly 3.6

#### 3.5.2 Etapa 2 - Implementácia a testovanie:

* bez uplatňovania SLA
* on-boarding dát z aktív obstarávateľa do SIEM a LMS
* prevzatie a oboznámenie sa s dokumentáciou verejného obstarávateľa a to najmä popis prostredia (segmentácia siete, topológia siete, zoznam monitorovaných zariadení) a jeho smernice
* finálne zadefinovanie procesov pre činnosti SOC a jeho zaintegrovanie do bezpečnostného riešenia verejného obstarávateľa
* zadefinovanie udalosti a bezpečnostného incidentu,
* zadefinovanie podmienok pre klasifikáciu a priorizáciu incidentov
* vytvorenie a finálne prijatie knižnice odoziev
* stanovenie eskalačnej matice
* stanovenie reportov – obsah, periodicita, komunikačné kanály pre zasielanie reportov
* stanovenie procesov pre aktualizáciu dokumentácie, resp. update ostatných informácií alebo zdrojov potrebných pre detekciu a klasifikáciu udalosti alebo incidentu
* stanovenie procesov pre update korelačných pravidiel
* podrobné zaškolenie IT administrátorov verejného obstarávateľa

#### 3.5.3 Etapa 3 – Nasadenie:

* s uplatňovaním SLA
* overenie parametrov korelačných pravidiel
* doladenie korelácií a výstupov

#### 3.5.4 Etapa 4 – štandardná prevádzka

* s uplatňovaním SLA
* vyhodnotenie prevádzky a optimalizácia pravidiel a procesov.

**Predpoklad trvania etapy 1 až 3 je 9 mesiacov. Etapa 4 je štandardná prevádzka, predpoklad trvania ďalších 60 mesiacov.**

Dodávateľ je povinný chrániť všetky poskytnuté informácie verejného obstarávateľa - ich dôvernosť, integritu, dostupnosť, hodnovernosť a pravosť pri vytváraní, ukladaní, uchovávaní, získavaní, prenášaní alebo spracúvaní. Pred začatím realizácie predmetu zákazky je povinný spolu so zmluvou o dielo uzatvoriť aj zmluvu o mlčanlivosti (NDA).

Dodávateľ je povinný po ukončení zmluvného vzťahu vrátiť, previesť alebo preukázateľne zničiť všetky informácie, ku ktorým má počas trvania zmluvy s verejným obstarávateľom prístup.

### 3.6 Požiadavky na doplnenie bezpečnostnej dokumentácie

Predmetom zákazky je aktualizácia a doplnenie nasledovnej bezpečnostnej dokumentácie verejného obstarávateľa podľa aktuálnych šablón smerníc, ktoré zverejňuje Ministerstvo investícií, regionálneho rozvoja a informatizácie s dôrazom na odstránenie nesúladov z auditu kybernetickej bezpečnosti, ktorý prebehol v decembri 2021:

SMK-54 – Stratégia kybernetickej a informačnej bezpečnosti (2021)

SMK-15 – Správa a prevádzka výpočtovej techniky, počítačovej siete a IS (2022)

SMK-67 – Smernica pre správcov IS, databáza, IKT a počítačovej siete (2022)

SMK-56 – Bezpečnostná smernica IS MEDIS a IS PACS (2020)

SMK-66 – Smernica na obsluhu a prevádzku kamerového systému (2021)

SMK-61 – Analýza rizík IS MEDIS (2021)

SMK-62 – Analýza rizík IS PACS (2021)

SMK-72 - Klasifikácia informácií (2021)

Business Impact Analysis

Business Continuity plány

Disaster Recovery plány

a vypracovanie bezpečnostného projektu podľa zákona 95/2019 Z. z. a vyhlášky 179/2020 Z. z.

Na túto oblasť projektu je vyčlenených cca 40 dní z etapy „analýza a dizajn“ a budú sa na nej podieľať IT odborníci verejného obstarávateľa.

## Ďalšie požiadavky na ponuku

### 4.1 Harmonogram

Uchádzač navrhne harmonogram v členení podľa etáp uvedených v kap. 3.5 alebo podľa jeho vlastného návrhu, ale musí dodržať limity v tabuľkovej prílohe „Kalkulácia ceny“.

Pre naplnenie činností v príslušnej etape poskytne obstarávateľ primeranú súčinnosť v režime 8/5 minimálne v nasledovnom rozsahu:

• pre etapu 1 – 20 MD

• pre etapu 2 – 14 MD

• pre etapu 3 – 3 MD

### 4.2 Komplexnosť informácií uvedených v cenovej ponuke

Uchádzač k cenovej ponuke doloží minimálne nasledovné informácie:

1. Podrobný popis ponúkaného riešenia – musí obsahovať informáciu aký SIEM, od ktorého výrobcu, v akej verzii a aký softvérový nástroj pre evidenciu životného cyklu bezpečnostného incidentu.
2. Cenu za riešenie v prílohe „Kalkulácia ceny“