# **OPIS PREDMETU ZÁKAZKY:**

NÁZOV: **Zabezpečenie licenčného modulu pre knižnicu informácií o kybernetických hrozbách, analýze hrozieb a posudzovanie hrozieb – Threat Intelligence Platforma**

### **SÚČASNÝ STAV**

Cieľom obstarania predmetu zákazky Threat Intelligence Platforma (TIP) je posilniť svoje proaktívne služby a získať, resp. poskytovať prehľad o relevantných rizikách a neznámych hrozbách dotýkajúcich sa subjektov verejnej správy v konštituencii Objednávateľa, a tým dosiahnuť zvýšenie efektivity ochrany a zavádzať stratégiu proaktívneho prístupu ku kybernetickej bezpečnosti.

V rámci Investície č. 6: Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (Informačné technológie vo verejnej správe – ITVS) Komponentu 17 Digitálne Slovensko Plánu obnovy a odolnosti Slovenskej republiky plánuje Objednávateľ obstaranie predmetu zákazky TIP. Strategickým cieľom objednávateľa je doplniť zdroje o aktuálnych hrozbách v oblasti kybernetickej bezpečnosti, zlepšiť technické a technologické vybavenie v systémoch kritickej infraštruktúry verejnej správy a zároveň zvýšiť úroveň centralizovaného zberu a vyhodnocovania informácií s následným vylepšením komunikácie na relevantné subjekty s cieľom predchádzať škodám spôsobeným kybernetickými bezpečnostnými incidentmi.

Ako strategický postup preto Objednávateľ vníma obstaranie predmetu zákazky posilnením v oblasti TIP. Zabezpečenie tejto oblasti na centrálnej úrovni súvisí s plnením úloh podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a je vysoko efektívne, keďže zabezpečenie tejto schopnosti na úrovni jednotlivých OVM by bolo nielen nákladné, ale chýbal by konkrétny nadhľad pre podsektor informačné systémy verejnej správy.

Threat Intelligence Platforma (TIP) je technológia, ktorá pomáha organizáciám agregovať, korelovať a analyzovať údaje o aktuálnych hrozbách z viacerých zdrojov na podporu analytických činností. Objednávateľ vníma, že v rámci proaktívneho prístupu je tradičný prístup k bezpečnosti nedostačujúci. Tradičný prístup k podnikovej bezpečnosti zahŕňa bezpečnostné tímy využívajúce rôzne procesy a nástroje na vykonávanie reakcie na incidenty, hrozby a ochranu siete.

Vzhľadom na to, že sa bezpečnostná situácia v kybernetickom priestore dynamicky vyvíja, je škálovateľnosť a efektívnosť náročná. Nástroje používané bezpečnostnými operačnými centrami (SOC) produkujú veľké množstvo udalostí denne, ktoré sa týkajú celého spektra IT aktív, čo sťažuje analýzu podozrivých udalostí a ich vyhodnocovanie.

Pomocou spravodajských informácií o hrozbách môžu jednotky CSIRT a sektorové orgány tiež v predstihu identifikovať zdroje hrozieb a údaje, ktoré sú najužitočnejšie a najrelevantnejšie pre ich vlastné prostredie, čím môžu potenciálne znížiť náklady spojené s možnými hrozbami v prostredí OVM.

Objednávateľ týmto sleduje strategický plán naplnenia vízie sekcie kybernetickej bezpečnosti a vládnej jednotky CSIRT poskytovať proaktívnu službu, podporu výkonného rozhodovania, a reálnu pomoc bezpečnostným tímom pri identifikácii hrozieb, ktoré sú relevantné pre ich organizácie, preto Objednávateľ vníma obstaranie SaaS TIP ako jeden zo základných kameňov budovania systému včasného varovania, ktorý predstavuje hlavnú časť Investície č.6.

## OPIS PREDMETU LICENCIE

### **CIELE TIP**

* Uľahčiť a zefektívniť identifikáciu podozrivých udalostí a kybernetických bezpečnostných incidentov
* Identifikácia potenciálnych hrozieb relevantných pre konkrétnu organizáciu, OVM zapojené do bezpečnostného monitoringu a podsektor verejná správa
* Zabezpečenie prechodu Objednávateľa na proaktívny spôsob ochrany

### **FUNKCIE TIP – SÚHRN HLAVNÝCH KATEGÓRIÍ**

* Integrácia s bezpečnostným stackmi
* Funkcionality TIP platformy
* Threat Intellingence knižnice
* Monitorovacia funkcionalita Brand Proteciton a Abuse
* Monitorovacia funkcionalita tretích strán
* Segmentácia a upozorňovanie na zranitelnosti
* Správa upozornení
* Súhrnná knižnica hrozieb definovaná funkčnými požiadavkami
* Filtrovanie údajov
* Informačné kanály s možnosťami pridania alebo konzumácie vlastných feedov
* Indikátori kompromitácie
* Intergrácie s platformami a SW zložkami vybraných produktov a spoločností
* Dostupnosť rozhrania API
* Informačné panely (dashboards) - prehľadové zostavy a analytické nástroje
* Dokumentácia
* Reporting – súhrnné reporty

### **TECHNICKÁ ŠPECIFIKÁCIA**

Predmet zákazky v rozsahu požiadaviek je v celom rozsahu opísaný tak, aby bol presne a zrozumiteľne špecifikovaný. Ak sa technické špecifikácie odvolávajú na konkrétneho Výrobcu, výrobný postup, obchodné označenie, patent, typ, oblasť alebo miesto pôvodu alebo výroby, ak by tým dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov alebo tovarov, obstarávateľ umožní v ponuke uchádzača nahradiť takýto výrobok ekvivalentným výrobkom alebo ekvivalentom technického riešenia pod podmienkou, že ekvivalentný výrobok alebo ekvivalentné technické riešenie bude spĺňať alebo prevyšovať úžitkové, prevádzkové a funkčné charakteristiky, ktoré sú nevyhnutné na zabezpečenie účelu, na ktoré sú uvedené technológie a zariadenia určené, pričom dôkazné bremeno tejto skutočnosti je na uchádzačovi a preukáže to vo svojej ponuke. Pri výrobkoch a/alebo príslušenstvách konkrétnej značky, uchádzač môže predložiť aj ekvivalenty inej značky v rovnakej alebo vyššej kvalite, ak tým zabezpečí funkčnosť celku.

**Predmetom zákazky je dodanie a nasadenie Threat Intelligence Platformy, jej integrácie s bezpečnostným stackom MISP do už existujúcej infraštruktúry Objednávateľa. Rovnako implementácia cez definované API rozhranie a ostatné funkcionality rozpísané v detailnej špecifikácií.**

V rámci zvyšovania úrovne kybernetickej bezpečnosti, dostupnosti a kvality prevádzkovaných aplikácií a v súvislosti s proaktívnou stratégiou prístupu z pohľadu kybernetickej bezpečnosti a jej smerovania plánuje verejný obstarávateľ nasadenie TIP ako komplexného nástroja pre posilnenie kybernetickej bezpečnosti. Objednávateľ požaduje, aby informácie a dáta z tohto zdroja (TIP) mohol využívať v rámci plnenia úloh vládnej jednotky CSIRT, analytických činností bezpečnostného dohľadového centra (tzv. SOC pracovisko) a tieto informácie a dáta **ďalej nekomerčne distribuovať a sprístupňovať akýmkoľvek spôsobom (napr. prostredníctvom platformy MISP) ostatným záujemcom, ktorí vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti podľa § 4 zákona č. 69/2019 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov alebo patria medzi prevádzkovateľov základnej služby, ktorí sú zaradení v podsektore informačné systémy verejnej správy.** Ponúkaný produkt musí túto podmienku spĺňať.

### **DETAILNÁ ŠPECIFIKÁCIA**

Verejný obstarávateľ požaduje, aby predmetné riešenie pre TIP malo nasledujúce parametre a funkcionality a definuje ich určenými funkčnými a nefunkčnými požiadavkami v Príloha č. 3 - Špecifikácia požiadaviek TIP. Objednávateľ sa rozhodol pre zamedzenie diskrepancií a možnej zmätočnosti informatívne priložiť parametre špecifikované aj v anglickom jazyku v Prílohe č.4 - Špecifikácie požiadaviek TIP a súhrn použitých skratiek v Prílohe č.5 - Použité skratky TIP. Verejný obstarávateľ rovnako požaduje, aby budúci Poskytovateľ bol platným obchodným a technických partnerom dodávateľa Threat Intelligence Platformy, tento aspekt bude musieť klarifikovať samostatným dokumentom alebo certifikáciou.

### **NAPOJENIE PREDMETU ZÁKAZKY NA PROSTREDIE OBJEDNÁVATEĽA A FORMÁT SLUŽBY**

Objednávateľ určuje ako formát napojenia pre dodanie predmetu zákazky formát služby API. Požiadavky pre tento formát napojenia sú rozpísané v Príloha č. 3 – Špecifikácia požiadaviek pre TIP a Príloha č. 4 – Špecifikácia požiadaviek pre TIP v anglickom jazyku. Objednávateľ požaduje aby bol poskytnutý prístup ku všetkým predplateným súborom a údajom minimálne prostredníctvom programovateľného rozhrania RESTful alebo SOAP. Tento formát bude podporovať minimálne 10 000 requestov denne, ktoré poskytujú údaje vo formáte JSON alebo XML. Objednávateľ rovnako určuje ako formát obstarania predmetu zákazky a napojenie licenčného modulu SaaS ako základ pre hosťovanie TIP na vlastných serveroch. Z dôvodu čiastočnej limitácie SaaS sa objednávateľ zameriava na súpis činností, ktoré sú premietnuté a rozpísané ako podmienené inštalačné a implementačné postupy v Príloha č. 1 – Protokol pre implementáciu TIP ako faktoru postupnej customizácie služby SaaS a samotného licenčné modulu. Objednávateľ sa rozhodol pre zamedzenie diskrepancií a možnej zmätočnosti informatívne priložiť súpis činností špecifikovaných aj v anglickom jazyku v Príloha č. 2 – Protokol pre implementáciu TIP v anglickom jazyku.

### **POSTUP A ROZSAH SLUŽIEB PRE JEDNOTLIVÉ FÁZY NASADENIA:**

V nadväznosti na definovanie pripojenia, Objednávateľ určuje postup a rozsah služieb pre finálne nasadenie predmetu zákazky a to rozdelením predmetných postupov do ucelených fáz so špecifikovaným rozsahom činností. Jednotlivé fázy sú umerne na seba nadväzujúce a Objednávateľ týmto sleduje progresívne a promtné naplnenie odovzdania predmetu diela.

Objednávateľ rovnako definuje časový rozsah z pohľadu jeho maximálneho časového ohraničenia a to ako Oprávnenú lehotu, počas ktorej je Poskytovateľ povinný naplniť a dokončiť Implementačnú fázu v rozsahu služieb a postupov definovaných Objednávateľom a odovzdať Predmet Zmluvy.

Rozsah a definovanie činností predstavuje postupovú chronológiu pre naplnenia a uspešné dodania predmetu zákazky.

**PRÍPRAVNÁ FÁZA -** Nadobúdateľ s ohľadom na danú fázu ako časť Implementačnej fázy definuje odporúčanú lehotu v rozsahu 15 (slovom: paťnásť) dní.

Samotná fáza začína od dátumu účinnosti Zmluvy na licenčný modul uspešným uchádzačom, ktorý následne ako Poskytovateľ bude zabezpečovať dodanie predmetu zákazky.

Súhrn činností:

* analýza súčasného stavu,
* klasifikácia systémových požiadaviek ako základ pre Implementačnú fázu a technických parametrov ako spoločný podklad pre spustenie Implementačnej fázy a protokolu pre implementáciu.

**IMPLEMENTAČNÁ FÁZA -** Nadobúdateľ s ohľadom na danú samotnú časť fázy definuje maximálnu lehotu v rozsahu 45 (slovom: štyridsaťpäť) dní.

Súhrn činností:

* aktivácia licencie,
* úvodnú Implementáciu a konfiguráciu a nastavenie TIP v rozsahu potrebnom pre business case pracoviska SOC u Objednávateľa v zhode s Prílohou č.1 Protokol pre Implementáciu,
* v rámci implementačnej fázy nasadenie poslednej a v čase dodania diela najaktuálnejšej verzie platformy MISP (verzia 2.4.XX. alebo vyššia),
* implementácia na základe rámcového protokolu, nastavenie MISP a TIP za plnej podpory Objednávateľa, zastúpeného zodpovedným členom v spolupráci so zodpovednej osobou na strane dodávateľa,
* odovzdanie predmetu zmluvy a ukončenie implementačného protokolu (Moment nadobudnutia licenčného modulu Objednávateľom),
* ukončenie Implementačnej fázy a oprávnenie Poskytovateľa fakturovať prvú splátku Primárnej odmeny v prvom roku realizácie Predmetu Zmluvy. Tento moment definuje objednávateľ z pohľadu maximálne oprávnenej lehoty ako 60 (slovom: šesťdesiat) dní od nadobudnutia účinnosti Zmluvy na licečný modul s uspešným uchádzačom.

Vystavenia faktúry je podmienená pre Poskytovateľa aktiváciou Licencie, umožnením analytického prístupu v požadovanom počte k Predmetu Licencie a kompletným rámcovým protokolom pre implementáciu, explicitne podľa Prílohy č. 2 Protokol pre Implementáciu TIP v spolupráci s Nadobúdateľom.

**POST-IMPLEMENTAČNÁ FÁZA**

Súhrn činností:

* Poskytovateľ v rámci licenčného obdobia zabezpečuje aby došlo k plnému naplneniu bodu 5.32 Licenčnej Zmluvy a podpore v rozsahu definovanom v Prílohe č.3 - Špecifikácia požiadaviek pre TIP,
* Poskytovateľ v rámci licenčného plnenia obdobia trvania zmluvy, definuje spoluučasť špecialistu zo strany Výrobcu Threat Intelligence Platform v rozsahu 1MD za mesiac pre potrebu podpory a rozvoja. Poskytovateľ tento fakt premietne do nacenovania pre licenčný modul.

### **DODATOČNÉ INFORMÁCIE:**

V rámci dodávky TIP požaduje Objednávateľ inštaláciu do MISP platformy, ktorej zabezpečenie, inštaláciu a nastavenie je rovnako súčasťou predmetu zákazky. Objednávateľ ale má za to, že budúci dodávateľ v rámci tohto úkonu bude definovať iba pracnosť predmetného úkonu, kedže MISP platforma je open source riešenie a nie je spoplatnená.

V rámci predmetu zákazky požaduje Objednávateľ dodanie licenčného modulu SaaS TIP, vrátane podpory dodávateľa a to v rozsahu nevýhradnej licencie, v neobmedzenom rozsahu, na obdobie 36 mesiacov od naimplementovania TIP, s opciou predĺženia predmetnej Licencie o ďalších 12 mesiacov. Pričom opciu je možné využiť celkovo dvakrát, t.j. spolu na 24 mesiacov.

Rovnako:

1. minimálne 2 konkurentné analytické prístupy alebo viac,
2. licenčné pokrytie počtu používateľov (tzv. entries v MS AD) v min. počte 10 tisíc, pokrytie počtu zamestnancov v sledovaných doménach v počte do 100 tis., počet sledovaných domén min. 20 (v prípade otázok nás prosím kontaktujte),
3. minimálne 1 API, ktoré umožňuje aspoň 10.000 dopytov denne.

Súčasťou dodávky musí byť aj inštalácia a konfigurácia riešenia, jeho nasadenie do prostredia obstarávateľa, naplnenie prípravnej a implementačnej v jednom bloku a post-implementačnej fázy.

Objednávateľ rovnako definuje, že predmetný budúci Poskytovateľ musí byť obchodný a technický partner predmetnej Threat Intelligence Platform. Na základe tohto aspektu, má objednávateľ za to, že nie je potrebné explicitne definovať špecialistu na strane Poskytovateľa, či už po stránke odbornej a technickej, keďže daný Poskytovateľ má svoj tím klarifikovaný zo strany Výrobcu.

### **DOKUMENTÁCIA**

V rámci realizácie požaduje Objednávateľ dodanie nasledujúcich dokumentov a to:

**Prevádzková dokumentácia** – príručka pre administrátora systému popisujúca základné prevádzkové postupy vrátane kontroly stavu, pripojenia API, integrácie s bezpečnostným stackom MISP. Rovnako dokumentáciu funkcionality integrácie cez API a definovanie postupu pre integráciu výberu IOCs.

**Inštalačná a konfiguračná príručka** – detailný postup inštalácie komponentov, popis multifaktorovej autentifikácie, funkcionality upozornení a systémových aktivít.

Po úspešnej inštalácií, nasadenení predmetu zákazky Objednávateľ požaduje a určuje ako súčasť predmetu zákazky kooperáciu predmetného experta zo strany Výrobcu č. 1 v rozsahu podpory 12MD za ročné licenčné obdobie, a to v podobe konzultačných služieb a školení potrebných pre Objednávateľa.

### **PRÍLOHY**

Príloha č. 1 – Protokol pre implementáciu TIP

Príloha č. 2 – Protokol pre implementáciu TIP v anglickom jazyku

Príloha č. 3 – Špecifikácia požiadaviek pre TIP

Príloha č. 4 – Špecifikácia požiadaviek pre TIP v anglickom jazyku

Príloha č. 5 – Použité skratky TIP