Zmluva o poskytovaní služieb č. Z20241526_Z

uzatvorená v zmysle §269 ods. 2 Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Generálne riaditeľstvo Zboru väzenskej a justičnej stráže
Sídlo:	Šagátova 1, 82108 Bratislava, Slovenská republika
IČO:	00212008
DIČ:	2020801838
IČ DPH:	
Telefón:	+421220831111

1.2 Dodávateľ:

Obchodné meno:	AXENTA s. r. o.
Sídlo:	Mlynská 898/12, 03101 Liptovský Mikuláš, Slovenská republika
IČO:	51142708
DIČ:	2120600878
IČ DPH:	SK2120600878
Telefón:	+421907136800

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Rozšírenie služieb nad implementovanými softvérovými technológiami
Kľúčové slová:	kybernetická bezpečnosť, riadenie kybernetických bezpečnostných incidentov
CPV:	48211000-0 - Softvérový balík na vzájomnú prepojiteľnosť počítačových platforiem
Druh/y:	Tovar

2.2 Funkčná a technická špecifikácia predmetu Zmluvy:

Položka č. 1: **Predmetom požiadavky je pilotné nasadenie SW technológií nevyhnutných pre zabezpečenie sledovania výstupov z jednotlivých bezpečnostných systémov a aplikácií a riadenie bezpečnostných incidentov.**

Funkcia				
Pilotné nasadenie SW technológií nevyhnutných pre zabezpečenie sledovania výstupov z jednotlivých bezpečnostných systémov a aplikácií a riadenie bezpečnostných incidentov ks 1				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Pilotné nasadenie SW technológií nevyhnutných pre zabezpečenie sledovania výstupov z jednotlivých bezpečnostných systémov a aplikácií a riadenie bezpečnostných incidentov	ks			1
Technické vlastnosti	**Hodnota/Charakteristika**			
Poskytovanie služieb predmetu zákazky musí byť v súlade s požiadavkami kladenými zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej v texte len ako „Zákon“) a s ním súvisiacimi aktuálnymi vykonávacími vyhláškami na prevádzkovateľov základnej služby v súvislosti s prevádzkovanými základnými službami Objednávateľa.	Základné požiadavky na systém			

Objednávateľ v produkčnom prostredí prevádzkuje (má vo vlastníctve) implementované bezpečnostné monitorovacie technológie v rozsahu:• Network Detection and Response (NDR)• Log Management (LM)• EndPoint Detection Response/XDR (EDR/XDR)• Data Lost Prevention (DLP)• Network Access Control (NAC)• Privileged Access Management (PAM)	Architektúra a druhy existujúcich SW technológií Objednávateľa
Popis zdrojov napojených do Log Managementu:HW (Windows, LINUX, virtuálne zdroje):• Windows System or Application Event• Windows Security Event• SQL Servers• Exchange Servers• Microsoft Windows Update Client• Virtual Center• Apache, MS IIS• SCCMAktívne prvky:• Firewall Sophos• WAF F5• Firewall Checkpoint• Cisco switch&router• FortiGate• FortiMailAplikácie Objednávateľa – APV IS ZVJS, NAVIS.Web aplikácie.	Architektúra a druhy existujúcich SW technológií Objednávateľa - Log Managment
Log managment – ArcSight Logger Standard Edition 2500 EPSDLP - SafeticaEDR/XDR - ESETNDR - GreyCortex MendelNAC - EasyNacPAM – One Identity Safeguard Privileged Security	Architektúra a druhy existujúcich SW technológií Objednávateľa - Bezpečnostné monitorovacie aplikácie
Všeobecné požiadavky: Nevyhnutnou súčasťou je prevádzkovanie Security Operations Center nad uvedenými technologickými platformami, vrátane jeho pravidelnej údržby zahŕňajúcej činnosti minimálne v rozsahu:• kontrola dát,• asset manažment,• access manažment,• ostatné činnosti prevádzkového charakteru bezpečnostných v súčinnosti s Objednávateľom a tretími stranami tak, aby bola zabezpečená kontinuálna a bezporuchová prevádzka bezpečnostného monitoringu.	Funkčné a technické požiadavky
Riešenie musí obsahovať centrálny dashboard – webovú aplikáciu s centrálnym riadiacim panelom pre jednotný pohľad na aplikácie a systémy prevádzkované v security operation centre	Funkčné a technické požiadavky
SIEM – súčasť služby SOC: logy zbierané do Log managmentu (on prem) musia byť prenášané prostredníctvom zabezpečeného kanála (napr. IPSEC tunel) k poskytovateľovi služby SIEM (SOC), kde budú vyhodnocované a ukladané pre potreby analýzy. Rozsah poskytovanej služby SIEM (SOC) má byť 1500 EPS. Zdroje ktoré budú napojené do SIEM (SOC) sú uvedené v vyššie v technických vlastnostiach.	Funkčné a technické požiadavky - SIEM
Funkčné a technické požiadavky - Security ticketing Security ticketing – súčasť služby SOC (oddelený od prevádzkového monitoringu)Ticketing nástroj (ako centrálne rozhranie pre komunikáciu v rámci služby SOC), ktorý je modifikovaný a prispôsobený na plnenie špecifických požiadaviek evidencie a spracovania bezpečnostných udalostí / incidentov a prepojenia s Jednotným informačným systémom kybernetickej bezpečnosti NBÚ SR (ďalej JIS KB). Na tento účel slúžia najmä tieto bezpečnostné vlastnosti a dodatočná základná funkcionalita:	Funkčné a technické požiadavky - Security ticketing
Oddelenie a zabezpečenie dát, ktoré sú svojou povahou citlivé / dôverné a musia byť zabezpečené z pohľadu dôvernosti tak, aby sa k nim nedostala neoprávnená osoba, z dôvodu, že môže prebiehať šetrenie, ktoré sa týka administrátora štandardného ticketing nástroja.• Zároveň s plnou podporou multitenantnosti, odd.dát, procesov a prístupov z pohľadu IT, ako aj z pohľadu organiz. štruktúry Obstarávateľa.• Oddelené modif.komunikačné priestory, tzv. fronty, umožňujúce rozdelenie jednotlivých tiketov podľa účelu komunikácie, typu bezpečnostného incidentu, osôb poverených riešením a ďalších parametrov	Funkčné a technické požiadavky - Security ticketing

Incident Response• Pokročilé možnosti analýz vstupných dát, spájanie tiketov, možnosť rôznych front a viacerých fáz (incident report, incident, analýza, náprava).• Rôzne druhy kategorizácie bezpečnostných incidentov zodpovedajúce best practice a ich kombinácie.• Možnosť vizuálnej analýzy vzťahov medzi jednotlivými tiketmi popisujúcimi súvisiace tikety.• Delegácia reakcie na incidenty s využitím špeciálnych front pre rôzne typy incidentov.• Integrácia so SIEM pre automatické zakladanie tiketov.	Funkčné a technické požiadavky - Incident Response
Incident Response • Integrácia s analytickými nástrojmi Threat Intelligence – informácie o kybernetických hrozbách (napr. MISP, TAXII).• Integrácia s analytickými nástrojmi pre pokročilé analýzy, typicky so SOAR produktmi.• Umožňuje automatizované hlásenia incidentov detegovaných v systéme SIEM do JIS KB podľa požiadaviek ZoKB.• Umožňuje automatické prijímanie a vhodné nastavenie taktických varovaní o kybernetických hrozbách publikovaných v JIS KB.• Možnosť integrácie s rôznymi technologickými prvkami siete a dohladovanými systémami (AD / LDAP, firewall, anti-spam).	Funkčné a technické požiadavky - Incident Response
Funkčné a technické požiadavky - SOAR SOAR – súčasťou služby SOC musí byť aj systém Security Orchestration, Automation and Response, ktorý je centrálnym miestom pre spracovanie bezpečnostných udalostí a automatizáciu reakčných playbookov a runbookov ako aj pre obohacovanie získaných dát a samotnú evidenciu vykonaných krokov. Technológia SOAR musí byť implementovaná multitenante a distribuovane u Dodávateľa, ktorý ju využíva ako centrálny systém pre riadenie.Počet serverov – 900,Počet akcií/mesiac – predpoklad 10 000	Funkčné a technické požiadavky - SOAR
• centrálny monitorovací nástroj pre vulnerability assessment a management prvkov IT (information technology),• služba posudzuje riziká podľa teoretických hrozieb a existencie reálnej hrozby,• služba obsahuje agenta pre koncové body (Lightweight Endpoint Agent),• služba poskytuje podrobné informácie o nainštalovaných aplikáciách na koncových zariadeniach,• počet zariadení zahrnutých do VA/VM - IP ADRIES = 1500	Funkčné a technické požiadavky - Vulnerability Assessment a Vulnerability Management
Funkčné a technické požiadavky - MISP MISP – súčasťou služby SOC musí byť systém na báze MISP projektu pre zdieľanie threat intelligence dát, indikátorov kompromitácií (IoC), feedy hrozieb a zraniteľností. Dáta spracovávané v MISP sú použité v ostatných bezpečnostných technológiách ako SIEM a SOAR.	Funkčné a technické požiadavky - MISP
Security Dashboard – súčasťou služby SOC musí byť plne konfigurovateľný centrálny bezpečnostný dashboard umožňujúci zobraziť bezpečnostne relevantné dáta z rôznych zdrojov do jedného grafického rozhrania, v ktorom si Objednávateľ za pomoci šablón môže vytvárať jednotlivé dasboardy (pohľady).	Funkčné a technické požiadavky - Security Dashboard
Predmetom zákazky je poskytovanie služieb dohľadového a monitorovacieho centra kybernetickej bezpečnosti nad požadovanými technológiami s nasledovnými funkciami:Analýza udalostí v reálnom čase• príjem bezpečnostných udalostí a incidentov v reálnom čase (Real Time Monitoring)• nástroje, ktoré neposkytujú „Real Time Monitoring“ nebudú Objednávateľom akceptované• triedenie a kategorizácia podľa preddefinovaných tried kritickosti v reálnom čase• analýza bezpečnostných udalostí a ich spracovanie podľa stanovených a dohodnutých „playbookov“	Funkčné a technické požiadavky – SOC - Analýza udalostí v reálnom čase

Analýza udalostí v reálnom čase : • prvotná analýza bezpečnostnej udalosti• vyšetrovanie bezpečnostných udalostí a ich riešenie• zber relevantných informácií• koordinácia aktivít počas celého životného cyklu bezpečnostnej udalosti• vyhodnocovanie potenciálnej možnosti vzniku incidentov kybernetickej bezpečnosti, • poskytovanie súčinnosti vo fáze ladenia systému monitorovania a vyhodnocovania („lessons learned“)	Funkčné a technické požiadavky – SOC - Analýza udalostí v reálnom čase
Threat Intelligence and Advisory• kontinuálny monitoring a analýza spravodajských zdrojov a hľadanie relevantných hrozieb, zraniteľností alebo TTPs (tactics, techniques, procedures)• analýza relevantnosti hrozieb pre Objednávateľa podľa regiónu, sektora, používaných technológií, atď.• priebežný reporting/notifikácia kritických hrozieb relevantných pre Objednávateľa• získavanie nových indikátorov kompromitácie v rámci monitoringu hrozieb a ich kontext• analýza informácií o hrozbách prichádzajúcich iným kom.kanálom (varovania manažmentu, SK CERT a pod.)• spolupráca na vyšetrovaní bezp. Ud.	Funkčné a technické požiadavky – SOC - Analýza incidentov a koordinácia reakcií na incidenty (CSIRT)
Threat Hunting• analýza trendov, korelácia dát z rôznych zdrojov Objednávateľa a systémov detekcie anomálií• vyhodnocovanie pokročilých pretrvávajúcich hrozieb (APT) a ich možností a dopadov na systémy Objednávateľa• hľadanie nových alebo doposiaľ neodhalených TTP podľa MITRE ATT&CK® alebo inej znalostne bázy v prostredí Objednávateľa• spolupráca pri tvorbe plánov a návrh požiadaviek na cielené cvičenia kybernetickej bezpečnosti	Funkčné a technické požiadavky – SOC - Threat Hunting
Riadenie zraniteľností• spolupráca na návrhu plánu testovania zraniteľností• vyhodnocovanie výsledkov z pravidelného testovania zraniteľností s ohľadom na kritickosť a citlivosť zraniteľného aktíva• návrh tvorby plánu ošetrenia s popisom možností (odstránenie, zmiernenie alebo akceptácia)• spolupráca na návrhu a vytvorenie požiadaviek s mitigačnými opatreniami pre riešiteľské skupiny•	Funkčné a technické požiadavky – SOC - Riadenie zraniteľností
Riadenie zraniteľností• • prijímanie nových informácií z procesu Threat intelligence o nových, zero-day, kritických alebo aktuálne zneužívaných zraniteľností, ich okamžité posúdenie kritickosti vzhľadom na prostredie a kritickosť aktíva a varovanie kompetentných riešiteľských skupín• zaslanie reportov• zaevidovanie zraniteľností zaznamenaných do servisdesku Dodávateľa	Funkčné a technické požiadavky – SOC - Riadenie zraniteľností
Monitoring• kontrola statusu všetkých prvkov bezpečnostného monitoringu (monitorovací agent, kolektor logov) ako aj nadstavbových systémov nevyhnutných pre poskytovanie služieb	Funkčné a technické požiadavky – SOC - Monitoring
Podpora procesov a bezpečnostných nástrojov• návrh úprav procedúr (Riadenie incidentov, Riadenie zraniteľností. Threat intelligence)• návrh úprav konfigurácii a architektúry technológií SOC,• návrh úprav auditnej politiky• návrh úprav perimetrových systémov alebo architektúry systémov• návrh úprav informačných systémov (servery, pracovné stanice, sieť, monitorovacie systémy),	Funkčné a technické požiadavky – SOC - Podpora procesov a bezpečnostných nástrojov
Podpora procesov a bezpečnostných nástrojov• návrh úpravy a spolupráca pri ladení senzorov ako sú IDS, IPS, Netflow,• tvorba a podpora pri vytváraní vlastných signatúr pre detekčné mechanizmy v prípade potreby,• návrh, výber, testovanie a nasadzovanie nových bezpečnostných technológií,• vývoj vlastných nástrojov a úprava existujúcich.• navrhovanie úprav a aktualizácie prvkov bezpečnostného monitoringu,	Funkčné a technické požiadavky – SOC - Podpora procesov a bezpečnostných nástrojov

Reporting• Dodávateľ vypracuje a odovzdá Objednávateľovi Mesačný report za kalendárny mesiac najneskôr k 10. pracovnému dňu nasledujúceho mesiaca Mesačný report obsahuje najmä:• Priemerný čas trvania incidentu a fáz riešenia• Počet udalostí a incidentov• Rozsah pokrytia systémov bezpečnostným monitoringom• počet aktívnych logsource a trend	Funkčné a technické požiadavky – SOC - Reporting
Funkčné a technické požiadavky – Prevádzkový monitoring Súčasťou služby SOC je implementácia a produkčná prevádzka systému na monitoring prevádzkových parametrov všetkých vyššie definovaných informačno-komunikačných technológií Objednávateľa. Akceptuje sa „open-source“ platforma, napr. ZABBIX alebo ekvivalent.	Funkčné a technické požiadavky – Prevádzkový monitoring
Minimálne sledované parametre musia byť:• dostupnosť monitorovanej technológie• využitie CPU, RAM, HDD, siete• priepustnosť portov sieťových a bezpečnostných zariadení• upozornenia na poruchy a chybové stavySúčasťou implementácie je vytvorenie a udržiavanie užívateľských „dashboard-ov“ vo forme prehľadných tabuliek a grafickej obrazovej topológie, ktorej dizajn bude definovaný Objednávateľom, tak isto neoddeliteľnou súčasťou implementácie je napojenie na existujúci Log Manažment Objednávateľa.	Funkčné a technické požiadavky – Prevádzkový monitoring
Korelačné pravidlá• Dodávateľ bude pravidelne kontrolovať aktívne korelačné pravidlá.• Dodávateľ priebežne upravuje dokumentáciu k jednotlivým korelačným pravidlám• Dodávateľ bude monitorovať a spravovať použité dočasné výnimky, ak platnosť dočasnej výnimky vyprší, • Dodávateľ navrhne zmeny v pravidlách, pri každej zmene bude upravená dokumentácia a všetky zistenia zaznamená v tiketovacom systéme.	Definície činností, SLA podmienky zákazky - Korelačné pravidlá
Kontrola a revízia dát v listoch• Dodávateľ poskytne súčinnosť pri pravidelných kontrolách listov a ich využívania v korelačných pravidlách a skriptoch.• Dodávateľ navrhne neplatné a nevyužívané listy upraviť alebo vymazať.	Definície činností, SLA podmienky zákazky - Korelačné pravidlá
Kontrola a revízia dát v listoch • Kontrola automatických reportov a dashboardov• Dodávateľ bude pravidelne minimálne raz za pol roka kontrolovať, či sú automatické reporty a dashboardy správne nastavené, či sa správne generujú a či ponúkajú výpovednú hodnotu, ktorá je od daného reportu alebo dashboardu požadovaná.	Definície činností, SLA podmienky zákazky - Korelačné pravidlá
TTO – Time to Open- je čas prevzatia bezpečnostnej udalosti/incidentu konkrétnym pracovníkom SOC max. 60 minútTTR – Time to Response- Čas ukončenia udalosti/incidentu max. 12 hodín- Za ukončenie incidentu sa považuje:o vyhodnotenie false positiveo aplikácia pripraveného playbookuo aplikácia runbookuo odovzdanie manažérovi kybernetickej bezpečnosti Objednávateľa s návrhom riešeniaReakčný čas - je čas od prevzatia incidentu do prvotného návrhu relevantných opatrení pre elimináciu rizika.	Definície činností, SLA podmienky zákazky - Vyhodnotenie kvality poskytovanej služby (Key Performance Indicators – KPI)
Prevádzkový časDodávateľ vykonáva činnosti pre Objednávateľa v dohodnutej kvalite pri dodržaní KPI v rozsahu dní:• Monitoring bezpečnostných technológií 24 hodín denne, 7 dní v týždni (7x24) od 0:00 do 24:00Bezpečnostný monitoring L1 a L2 8 hodín denne, 5 dní v týždni (8x5) od 8:00 do 16:00	Definície činností, SLA podmienky zákazky - Prevádzkový čas

Súčinnosť Objednávateľa Objednávateľ v spolupráci s Dodávateľom zabezpečí pre poskytovanie služby SOC IPSec site2site tunel s definovaným nekonfliktným IP rozsahom, port forwardingom na strane Objednávateľa aj Dodávateľa. Dodávateľ musí na strane SOC prevádzkovať VPN koncentrátory kompatibilné s najnovšími štandardami na nadviazanie zabezpečeného sieťového pripojenia medzi Dodávateľom a Objednávateľom.Objednávateľ zabezpečí pre Dodávateľa potrebné užívateľské prístupy pre poskytovanie služby SOC.	Súčinnosť Objednávateľa
Objednávateľ poskytne Dodávateľovi všetky jemu známe informácie a technických parametroch svojho chráneného prostredia.Objednávateľ zabezpečí tím interných odborných pracovníkov (pracovná skupina), ktorí budú súčinní pri implementácii ako aj pri poskytovaní služby (Incident Response Team).Objednávateľ zabezpečí HW a SW prostriedky nevyhnutné pre úspešné plnenie predmetu zákazky.	Súčinnosť Objednávateľa
Celkovo 18 mesiacov, z toho 4 mesiace implementačná fáza projektu a 14 mesiacov produkčná fáza projektu (plnenie predmetu)	Trvanie zákazky

2.3 Osobitné požiadavky na plnenie:

Názov
Ak je Dodávateľ identifikovaný pre DPH v inom členskom štáte EÚ alebo je zahraničnou osobou z tretieho štátu a miesto dodania služby je v SR, tento Dodávateľ nebude pri plnení Zmluvy fakturovať DPH. Vo svojej Kontraktačnej ponuke však musí uviesť príslušnú sadzbu a výšku DPH podľa zákona č. 222/2004 Z.z. a cenu vrátane DPH. Objednávateľ nie je zdaniteľnou osobou a v tomto prípade je/bude registrovaný pre DPH podľa § 7 a/alebo § 7a zákona č. 222/2004 Z.z. a bude povinný odviesť DPH v SR podľa zákona č. 222/2004 Z.z..
. Úhrada plnenia bude uskutočnená bankovým prevodom po riadnom dodaní akceptačného protokolu vystavenom najneskôr ku dňu ukončenia implementačnej fázy projektu a doručenej faktúry so splatnosťou 30 dní, s uvedením celkovej ceny s DPH a jednotkových cien s DPH zaokrúhlenými na dve desatinné miesta.
3. Objednávateľ nebude akceptovať kumuláciu rolí jednotlivých expertov z dôvodu spoľahlivej prevádzky služby, personálnej zastupiteľnosti a zníženia rizika dostupnosti služby pri výpadku experta.
4. Objednávateľ nebude akceptovať potvrdenia o absolvovaní školenia. Podkladom certifikácie musí byť absolvovanie certifikačnej skúšky uznávanou autoritou.
5. Požadovaný expert musí byť k dispozícii v rozsahu potrebnom pre plnenie úloh predmetu zákazky počas obdobia platnosti Zmluvy.
6. Potvrdením a preukázaním odborných znalostí experta bude požadovaný certifikát a CV experta s uvedenými požadovanými praktickými skúsenosťami
7A- Dodávateľ do 3 pracovných dní od nadobudnutia účinnosti zmluvy preukáže, že disponuje odbornými certifikovanými pracovníkmi a to min. v rozsahu:Expert pre oblasť Security Information and Event Management – min.2osoby.- min. 3ročná preukázateľná prax v oblasti SOC a jeho procesmi- min. 2 referencie - praktické skúsenosti z 2 projektov obdobného zamerania ako je predmet zákazky----
7A. --- platný certifikát certifikátom IBM Cerified Deployment Profesional, resp. IBM Certified Associate Administrator – Qradar, alebo IBM Administrator - Cloud Pack for Security vydaný akreditačnou a certifikačnou autoritou uznávanou v oblasti IT bezpečnosti. Postačujúca je kópia certifikátu. praktické skúsenosti s návrhom a tvorbou „UseCase“
7B. Expert pre architektúru systémov bezpečnosti (architekt kybernetickej bezpečnosti) minimálne 1 osoba- minimálne 5 ročná prax- odborná znalosť NDR, LM, SIEM, SOAR a SOC procesov preukázaná profesijným životopisom- platný certifikát CISSP alebo Architekt kybernetickej bezpečnosti alebo ekvivalent. Postačujúca je kópia certifikátu- Expert musí preukázať minimálne 3 referencie účasti na projekte obdobného zamerania a rozsahu
7C- Analytik dohľadového centra kybernetickej bezpečnosti – Expert/L2 úroveň - minimálne 1 osoba- Odbornosť preukázať prof. životopisom, - Minimálne 3 ročná prax, - Platný certifikát (CISSP, CompTIA CySA+, Cybersecurity Analyst Professional) alebo ekvivalent- znalosť SIEM, SOAR, praktické skúsenosti (Hands on Purple Team)- Vyšetrovanie incidentu na úrovni L2 musí začať do stanoveného času podľa KPI- Analytik musí mať preukázateľnú prax s vyšetrovaním a riešením bezpečnostných incidentov- Expert musí preukázať minimálne 2 referencie účasti na projekte obdobného zamerania a rozsahu
7D- Analytik dohľadového centra kybernetickej bezpečnosti – Špecialista/L1 úroveň - minimálne 4 osoby- Odbornosť preukázaná profesijným životopisom- Platný certifikát Cybersecurity Analyst alebo Threat Intelligence alebo ekvivalent pre špecialistu L1 SOC analytika. Postačujúca je kópia certifikátu- Predpokladom je analytické myslenie, schopnosť sa rozhodovať a postupovať podľa preddefinovaného postupu. Expert musí preukázať minimálne 2 referencie účasti na projekte obdobného zamerania a rozsahu

7E- Expert pre systémy bezpečnosti sieťovej prevádzky (Bezpečnostný monitoring siete) - minimálne 1 osoba- Expert musí disponovať platným certifikátom Technical Engineer, alebo ekvivalent vydaný výrobcom alebo autorizovaným certifikačným strediskom výrobcu. Postačujúca je kópia certifikátu- Odbornosť preukázaná profesijným životopisom za obdobie minimálne 3 posledné roky a aktívnu činnosť v súčasnosti.- Expert musí preukázať minimálne 2 referencie účasti na projekte obdobného zamerania a rozsahu
7F- Expert pre systémy Endpoint detection and response - minimálne 1 osoba- Expert musí disponovať platným technickým certifikátom pre dodávanú službu EDR postačujúca je kópia certifikátu- Odbornosť preukázaná profesijným životopisom za obdobie minimálne 3 posledné roky a aktívnu činnosť v súčasnosti- Expert musí preukázať minimálne 2 referencie účasti na projekte obdobného zamerania a rozsahu
7G- Analytik zraniteľností - minimálne 1 osoba- Odbornosť preukázaná profesijným životopisom- Platný certifikát VA/VM nástroja, ktorý je súčasťou služby SOC. Postačujúca je kópia certifikátu- Minimálne 3 ročná prax- Expert musí preukázať minimálne 2 referencie účasti na projekte obdobného zamerania a rozsahu
7H- Analytik hrozieb - minimálne 1 osoba- Odbornosť preukázaná profesijným životopisom- Minimálne 3 ročná prax- Platný certifikát Cybersecurity Threat Intelligence alebo ekvivalent. Postačujúca je kópia certifikátu- Znalosť nástrojov MISP alebo ekvivalent. Expert musí preukázať minimálne 2 referencie účasti na projekte obdobného zamerania a rozsahu.
7I- Expert pre oblasť Log Managmentu - minimálne 1 osoba- minimálne 3 ročná preukázateľná prax v oblasti SOC a jeho procesmi- minimálne dve referencie - praktické skúsenosti z dvoch projektov obdobného zamerania ako je predmet zákazky- platný certifikát ArcSight Advanced Analyst, vydaný akreditačnou a certifikačnou autoritou uznávanou v oblasti IT bezpečnosti. Postačujúca je kópia certifikátu.- praktické skúsenosti s napájaním zdrojov
7J-Expert pre oblasť SOAR - minimálne 1 osoba minimálne 3 ročná preukázateľná prax v oblasti SOC a jeho procesmi- minimálne dve referencie - praktické skúsenosti z dvoch projektov obdobného zamerania ako je predmet zákazky- platný certifikát “SOAR advanced” (certifikát pre SOAR riešenie poskytnuté zákazníkom vo funkcionalite SOC), vydaný akreditačnou a certifikačnou autoritou uznávanou v oblasti IT bezpečnosti. Postačujúca je kópia certifikátu.- praktické skúsenosti s vytváraním obsahu pravidiel platformy SOAR
7K- Expert pre oblasť Prevádzkového monitoringu (PM) - minimálne 1 osoba minimálne 3 ročná preukázateľná prax v oblasti PM a jeho procesmi- minimálne dve referencie - praktické skúsenosti z dvoch projektov obdobného zamerania ako je predmet zákazky- platný certifikát “ZABBIX certified specialist” minimálne verzie 3 alebo novším vydaným výrobcom alebo autorizovaným certifikačným strediskom výrobcu. Postačujúca je kópia certifikátu
7L- Expert pre oblasť Sieťovej bezpečnosti - minimálne 1 osoba minimálne 3 ročná preukázateľná prax v oblasti bezpečnosti sieťovej infraštruktúry- minimálne dve referencie - praktické skúsenosti z dvoch projektov obdobného zamerania ako je predmet zákazky- platný certifikát “CheckPoint Certified Security Expert R80” vydaným výrobcom alebo autorizovaným certifikačným strediskom výrobcu. Postačujúca je kópia certifikátu
8. Dodávateľ do 3 pracovných dní od nadobudnutia účinnosti zmluvy preukáže, že je držiteľom akreditácie alebo má status Acreditation Candidate CSIRT od spoločnosti TI -Trusted Introducer (Trusted Introducer : Directory : Team Database (trusted-introducer.org) alebo je členom Forum of Incident Response and Security Teams (FIRST Teams)
9. Dodávateľ do 3 pracovných dní od nadobudnutia účinnosti zmluvy preukáže, že je držiteľom certifikátu manažérstva bezpečnosti podľa normy EN ISO 27001
10. Dodávateľ do 3 pracovných dní od nadobudnutia účinnosti zmluvy predloží zoznam zrealizovaných dodávok a poskytnutých služieb v oblasti poskytovania služieb SOC podobného charakteru ako je predmet zákazky za predchádzajúcich 5 rokov ku dňu vyhlásenia zákazky s uvedením názvu zákazky, rozsah plnenia relevantný k predmetu zákazky podľa tohoto opisného formulára, ceny plnenia relevantného k predmetu tejto zákazky, lehôt dodania a identifikáciu odberateľa s uvedením kontaktu na osobu, ktorá referenciu môže potvrdiť a uvedením podielu plnenia zo zmluvy.
10. Zoznam musí obsahovať minimálne 3 zákazky rovnakého alebo podobného rozsahu v hodnote minimálne 277 000,00 Eur bez DPH ako je predmet zákazky. Minimálne jedna zákazka v minimálnej hodnote 92.000,00 Eur bez DPH. Za zrealizovanú dodávku a/alebo poskytnutú službu rovnakého alebo podobného charakteru sa považuje aj prebiehajúca zákazka s priebežným plnením, pričom v takom prípade sa do hodnoty zákazky nezapočítava celkový dohodnutý objem zákazky, ale len pomerná časť odpovedajúca už zrealizovaným dodávkam a službám, ktoré boli vyfakturované do dňa vyhlásenia tejto súťaže.
10. Zo zoznamu poskytnutých služieb, súčasťou ktorého budú referencie alebo ekvivalentné doklady, predloženého účastníkom, musia vyplývať vyššie uvedené požiadavky, a to tak po formálnej ako aj obsahovej stránke.Za zrealizovanú dodávku a/alebo poskytnutú službu rovnakého alebo podobného charakteru sa považuje aj zákazka, ktorý záujemca zabezpečil ako sub-Dodávateľ pokiaľ jeho podiel na plnení presiahol minimálne 25% hodnoty zákazky, a to tak, že záujemca uvedie identifikáciu partnera a vlastný vykonaný podiel na plnení.
11. Dodávateľ sa zaväzuje:• zdržať sa akéhokoľvek zásahu alebo konania, ktoré by sťažovalo alebo znemožňovalo plnenie jeho povinností a takéto konanie neumožniť ani tretím osobám ako napr. pokusy o znefunkčnenie prístupných systémov Objednávateľa.• zdržať sa akéhokoľvek konania, ktoré by znížilo dostupnosť služieb ako napr. pokus o prienik zo strany Dodávateľa, DoS útoky, penetračné testy, ...• nepreviesť žiadne práva a povinnosti na akúkoľvek tretiu osobu bez predchádzajúceho písomného súhlasu
11. • poskytovať zoznam partnerov a sub-Dodávateľov, ktorí sa ne/priamo zúčastňujú plnenia predmetu zákazky, • sub-Dodávatelia musia byť odsúhlasený Objed. min 14 dní pred začatím poskytovania subdodávky prostredníctvom Dodávateľa, pred zahájením poskytovania služby a min 30 dní pred zahájením/ukončením spolupráce s treťou stranou• 1x za dva roky preukazovať kontinuálne vzdelávanie zamest. prehľadom absolv. vzdelávacích aktivít/plánom vzdelávania.• podrobiť sa pravidelnému (min 1x za 2 roky) auditu súladu systému informačnej bezpečnosti podľa medzinárodných štandardov (ISO 27000 a pod.).

Názov	Upresnenie

2.4 Prílohy opisného formulára Zmluvy:

Popis	Názov súboru

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát:	Slovenská republika
Kraj:	Bratislavský
Okres:	Bratislava II
Obec:	Bratislava - mestská časť Ružinov
Ulica:	Šagátova 1

3.2 Čas / lehota plnenia zmluvy:

01.04.2024 00:00:00 - 30.11.2025 00:00:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka:	v celom rozsahu
Požadované množstvo:	1,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronickej platformy verzia 1.2, účinná odo dňa 3. 11. 2022 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 79 166,67 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 95 000,00 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronickej platformy uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv Trhoviska.

5.5 Túto Zmluvu bude možné meniť a doplňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:
Príloha č.1 Obchodné podmienky elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

V Bratislave, dňa 14.03.2024 10:44:01

Objednávateľ:
Generálne riaditeľstvo Zboru väzenskej a justičnej stráže
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
AXENTA s. r. o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska