

Zmluvné strany:

Objednávateľ: **Fakultná nemocnica Trenčín**
sídlo: Legionárska 28, 911 71 Trenčín
IČO: 00 610 470
DIČ: 2021254631
IČ DPH: SK2021254631
registrácia: v Registri a identifikátore právnických osôb, podnikateľov a orgánov verejnej
moci vedenom Štatistickým úradom SR pod reg. č. 11902/2020
zriadená: Zriaďovacia listina vydaná MZ SR č. 1970/1991-A/VIII-1 zo dňa 14.06.1991
v zastúpení: Ing. Tomáš Janík, MBA, riaditeľ
bank. spojenie: Štátna pokladnica, Bratislava
IBAN: SK23 8180 0000 0070 0028 0438
(ďalej len „objednávateľ“)

a

Poskytovateľ: **AUTOCONT s.r.o.**
sídlo: Krasovského 14, 851 01 Bratislava, Slovenská republika
IČO: 36396222
DIČ: 2020105428
IČ DPH: SK2020105428
zápis: v Obchodnom registri Okresného súdu Bratislava I, Oddiel: Sro, Vložka číslo:
130357/B
v zastúpení: Mario Háronik, konateľ
bank. spojenie: Slovenská sporiteľňa, a.s.
IBAN: SK53 0900 0000 0050 3080 8601

(ďalej aj len ako „poskytovateľ“)

Objednávateľ ako verejný obstarávateľ a poskytovateľ ako úspešný uchádzač vo verejnom obstarávaní v postupe zadávania nadlimitnej zákazky v súlade so zákonom č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov (ďalej aj len ako „zmluvné strany“) uzatvárajú v súlade s § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov nasledovnú zmluvu o poskytovaní služieb (ďalej aj len ako „zmluva“), ktorej plnenie zo strany objednávateľa bude čiastočne realizované zo štrukturálnych fondov Európskej únie v rámci projektu „Implementácia, vyladenie, testovanie a nasadenie služby LMS, SIEM a SOC vo FN Trenčín“, s kódom výzvy: OPII-2022/7/20-DOP,“ ktorými je táto zmluva limitovaná.

Podkladom na uzavretie zmluvy je ponuka úspešného uchádzača predložená v postupe zadávania nadlimitnej verejnej súťaže na predmet zákazky: „Poskytovanie služby LMS, SIEM a SOC“ zadávanej na základe Oznámenia o vyhlásení verejného obstarávania.

Čl. I

Predmet zmluvy

1.1 Predmetom tejto zmluvy je záväzok poskytovateľa poskytnúť objednávateľovi služby špecifikované v čl. II bode 2.1 tejto zmluvy v dojednanom termíne a za podmienok dohodnutých v tejto zmluve a jej prílohách, a záväzok objednávateľa za poskytnuté služby zaplatiť poskytovateľovi odmenu vo výške dohodnutej podľa čl. II tejto zmluvy.

- 1.2 Služby, ktoré sú predmetom tejto zmluvy, sú špecifikované v čl. II bode 2.1 tejto zmluvy. Podrobná špecifikácia jednotlivých položiek a podmienok ich poskytovania je uvedená v Prílohe č. 1 tejto zmluvy- „Špecifikácia služieb LMS, SIEM a SOC“, ktorá tvorí jej neoddeliteľnú súčasť. Poskytovateľ je povinný vypracovať podrobný popis ním navrhovaného riešenia rozdelený na fázy: Analýza a dizajn, Implementácia a testovanie, Nasadenie, Prevádzka, ktorý tvorí Prílohu č. 4 tejto zmluvy ako jej neoddeliteľnú súčasť.
- 1.3 Služby podľa tejto zmluvy budú zo strany poskytovateľa poskytované objednávateľovi s cieľom, aby si objednávateľ zabezpečil plnenie povinnosti objednávateľa podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, v platnom znení.

Čl. II Cena a platobné podmienky

- 2.1 Zmluvné strany sa dohodli v zmysle zákona č. 18/1996 o cenách v aktuálnom znení na cene - odmene za poskytovanie služieb - jednotlivých činností poskytovaných na základe tejto zmluvy vo výške:

Položka	Cena
1. Analýza a dizajn	21 600,00 Eur
2. Implementácia a testovanie	26 210,00 Eur
3. Nasadenie	18 160,00 Eur
4. Prevádzka – mesačný paušál za HW infraštruktúru	152,00 Eur
5. Prevádzka – mesačný paušál za licencie	309,00 Eur
6. Prevádzka – mesačný paušál za LMS, SIEM, SOC	1 350,00 Eur

Cena za služby podľa položiek č. 1 - 3 bude poskytovateľom fakturovaná jednorazovo do 15 dní odo dňa jej poskytnutia poskytovateľom objednávateľovi na základe vzájomne potvrdeného akceptačného protokolu, ktorý musí byť vypracovaný v súlade s Prílohou č. 2 tejto zmluvy - „Kalkulácia ceny“ pre príslušnú etapu. Objednávateľ prehlasuje, že cena za služby podľa položiek č. 1 - 3 bude uhradená zo štrukturálnych fondov Európskej únie v rámci projektu „Implementácia, vyladenie, testovanie a nasadenie služby LMS, SIEM a SOC vo FN Trenčín“, s kódom výzvy: OPII-2022/7/20-DOP“.

Cena za služby podľa položiek č. 4 - 6 bude fakturovaná na jednej faktúre mesačne v mesiaci nasledujúcom po mesiaci, v ktorom bude uvedená služba poskytnutá, a to počnúc dňom začatia poskytovania služby podľa týchto položiek v zmysle čl. IV tejto zmluvy, pričom prílohou faktúry musí byť výkaz prác, ktoré boli vykonané a s počtom logovaných zariadení v uplynulom mesiaci. V rámci výkazu prác bude špecifikovaný počet hodín podpory L2, L3 a počet nevyčerpaných hodín tejto podpory za aktuálny rok. Cena za službu podľa položky č. 6 – paušál za LMS, SIEM, SOC, sa bude počítať každý mesiac podľa skutočného počtu logovaných zariadení objednávateľa na základe tabuľky 6 Prílohy č. 2 „Kalkulácia ceny“, pričom štartovací počet zariadení objednávateľa je uvedený v Prílohe č. 3 „Sizing zariadení objednávateľa“. Objednávateľ prehlasuje, že cena za služby podľa položiek č. 4 - 6 bude uhradená z vlastných zdrojov objednávateľa.

Služby uvedené v položkách č. 1 až 6 nebudú vyžadovať vystavenie objednávky, za objednávku sa považuje táto zmluva.

- 2.2 Predmetom fakturácie môžu byť len skutočne poskytnuté služby v súlade s touto zmluvou.
- 2.3 V cene sú zahrnuté všetky náklady, ktoré poskytovateľovi vzniknú pri poskytnutí služieb podľa tejto zmluvy.
- 2.4 Ceny sú uvedené v EUR bez DPH. K cenám bude pripočítaná DPH podľa platných právnych predpisov.

- 2.5 Splatnosť každej faktúry je 60 dní odo dňa jej doručenia objednávateľovi za predpokladu, že faktúra bude spĺňať všetky náležitosti v zmysle bodu 2.7 tohto článku zmluvy. Objednávateľ je povinný uhradiť poskytovateľovi fakturovanú sumu prevodom na bankový účet poskytovateľa uvedený na faktúre, pričom na faktúre musí byť uvedený účet poskytovateľa uvedený v záhlaví tejto zmluvy. Faktúra sa považuje za uhradenú dňom pripísania fakturovanej sumy na bankový účet poskytovateľa.
- 2.6 V prípade omeškania úhrady faktúry zo strany objednávateľa v lehote splatnosti, je poskytovateľ oprávnený vyúčtovať objednávateľovi úroky z omeškania v zákonom stanovenej výške.
- 2.7 Faktúra – daňový doklad musí obsahovať všetky náležitosti stanovené platnými právnymi predpismi a musí byť k nej priložený objednávateľom potvrdený písomný doklad podľa bodu 2.1 tohto článku zmluvy, v opačnom prípade je objednávateľ oprávnený vrátiť poskytovateľovi faktúru na prepracovanie a nie je v omeškaní s úhradou za poskytnuté služby.
- 2.8 Výdavky na faktúre za služby uvedené v bode 2.1 položky 1-3 musia byť rozdelené podľa sumáru vykonanej práce jednotlivých špecialistov s jednotkovými cenami zaokrúhlenými na dve desatinné miesta s jednoznačnou identifikáciou, ktorej položky rozpočtu /kalkulácie podľa Prílohy č. 2 tejto zmluvy sa predmetná fakturovaná čiastka týka. Ku každej faktúre musí byť priložený originál akceptačného protokolu podpísaného zmluvnými stranami.
- 2.9 V prípade že objednávateľovi nebudú pridelené finančné prostriedky z výzvy "Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach" s kódom : OPII-2022/7/20-DOP na projekt „Implementácia, vyladenie, testovanie a nasadenie služby LMS, SIEM a SOC vo FN Trenčín“, oprávnenou osobou, objednávateľ je oprávnený odstúpiť od zmluvy a zmluvné strany sú povinné si bezodkladne vrátiť dovtedy poskytnuté vzájomné plnenie. Takéto odstúpenie nebude mať za následok žiadne sankcie voči objednávateľovi.

Čl. III

Práva a povinnosti zmluvných strán

- 3.1 Poskytovateľ je povinný pri poskytovaní služieb podľa tejto zmluvy postupovať s odbornou starostlivosťou a konať pri plnení tejto zmluvy podľa svojich schopností a znalostí a dodržiavať platné všeobecne záväzné právne predpisy.
- 3.2 Poskytovateľ je povinný chrániť práva a oprávnené záujmy objednávateľa, konať čestne a svedomito a pri poskytovaní služby postupovať podľa oprávnených požiadaviek objednávateľa.
- 3.3 Objednávateľ je povinný poskytovať poskytovateľovi súčinnosť potrebnú pre riadne a včasné poskytnutie služieb. Potrebnou súčinnosťou sa rozumie predovšetkým včasné dodanie potrebných podkladov, informácií, listín, vysvetlení a pod., ktoré si poskytovateľ vyžiadal, alebo ktoré môžu podľa názoru objednávateľa slúžiť ako zmysluplný podkladový materiál pre poskytovanie služieb podľa tejto zmluvy.
- 3.4 V prípade, že by niektoré informácie, údaje, alebo podklady poskytnuté objednávateľom, neboli dostatočné, alebo kompletne, poskytovateľ bez zbytočného odkladu požiada objednávateľa o ich spresnenie a/alebo zabezpečenie.
- 3.5 Na poskytovanie plnení podľa tejto Zmluvy má Poskytovateľ za podmienok dohodnutých v tejto Zmluve, právo uzatvárať subdodávateľské zmluvy a zabezpečiť plnenie tejto Zmluvy alebo jeho častí prostredníctvom subdodávateľov v súlade s podmienkami Verejného obstarávania a tejto Zmluvy. Poskytovateľ zodpovedá za každé plnenie poskytnuté na základe tejto Zmluvy subdodávateľom, ako keby toto plnenie poskytoval sám. Zodpovednosť Poskytovateľa za plnenie Zmluvy v súlade s § 41 ods. 8 ZVO nie je dotknutá a Poskytovateľ je povinný sám odovzdávať

Objednávateľovi plnenia poskytnuté subdodávateľom podľa tejto Zmluvy, na svoju zodpovednosť, v dohodnutom čase a v dohodnutej kvalite.

- 3.6 Zoznam subdodávateľov s ich identifikačnými údajmi v rozsahu: (i) meno a priezvisko alebo obchodné meno, resp. názov, (ii) adresa pobytu alebo sídlo, (iii) IČO alebo dátum narodenia, ak nebolo pridelené IČO, (iv) podiel plnenia Zmluvy v percentuálnom vyjadrení, ako aj údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia, tvorí neoddeliteľnú súčasť tejto Zmluvy ako Príloha č. 6 tejto Zmluvy.
- 3.7 Poskytovateľ je povinný písomne oznámiť Objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi bezodkladne po tom, ako sa o takej zmene dozvedel.
- 3.8 Poskytovateľ je oprávnený zmeniť alebo doplniť subdodávateľa počas trvania Zmluvy len po predchádzajúcom písomnom súhlase Objednávateľa. Poskytovateľ je povinný písomne požiadať Objednávateľa o súhlas so zmenou alebo doplnením subdodávateľa najneskôr 10 pracovných dní pred dňom, v ktorom Poskytovateľ plánuje aby sa zmenený alebo doplnený subdodávateľ začal podieľať na poskytovaní Služieb podľa tejto Zmluvy. Poskytovateľ doručí písomnú žiadosť o súhlas so zmenou alebo doplnením subdodávateľa, ktorá bude obsahovať údaje o navrhovanom subdodávateľovi v rozsahu podľa bodu 3.6 tohto článku Zmluvy. Objednávateľ sa zaväzuje vyjadriť sa písomne k doručenej žiadosti Poskytovateľa v lehote do 7 pracovných dní od doručenia žiadosti. Zmenu subdodávateľa sú Zmluvné strany povinné zaznamenať v dodatku uzatvorenom k tejto Zmluve.
- 3.9 Porušenie ktorejkoľvek povinnosti vyplývajúcej z bodov 3.7 a 3.8 tohto článku Zmluvy sa považuje za podstatné porušenie Zmluvy Poskytovateľom a je dôvodom, ktorý oprávňuje Objednávateľa na odstúpenie od Zmluvy.
- 3.10 Poskytovateľ je povinný zabezpečiť, aby subdodávatelia, ktorým vznikla povinnosť zápisu do registra partnerov verejného sektora, mali riadne splnené povinnosti ohľadom zápisu do registra partnerov verejného sektora v zmysle Zákona o registri partnerov verejného sektora.
- 3.11 Objednávateľ má právo odstúpiť od Zmluvy z dôvodov uvedených v § 15 ods. 1 Zákona o registri partnerov verejného sektora, ako aj z dôvodu výmazu subdodávateľa v prípade, ak trvá jeho povinnosť zápisu v registri partnerov verejného sektora. Objednávateľ nie je v omeškaní a nie je povinný plniť, čo mu ukladá táto Zmluva, ak nastanú dôvody podľa § 15 ods. 2 Zákona o registri partnerov verejného sektora. Zmluva v takom prípade zaniká doručením oznámenia o odstúpení od Zmluvy. Riadne poskytnuté plnenia, vzájomne poskytnuté do dňa odstúpenia od Zmluvy, si Zmluvné strany ponechajú; tým nie je dotknutý nárok Poskytovateľa na odplatu za riadne dodané plnenie podľa tejto Zmluvy do dňa odstúpenia od Zmluvy.
- 3.12 Poskytovateľ je povinný bez zbytočného odkladu písomne upozorniť objednávateľa na zjavnú nesprávnosť pokynov poskytnutých objednávateľom alebo treťou osobou.
- 3.13 Za vecný a právny obsah poskytovateľovi dodaných materiálov, podkladov, pokynov a informácií zodpovedá výlučne v plnom rozsahu objednávateľ.
- 3.14 Poskytovateľ sa zaväzuje pri poskytovaní služieb dodržiavať všeobecne záväzné predpisy BOZP a PO. V prípade, že si plnenie služby vyžiada prítomnosť poskytovateľa v priestoroch objednávateľa, zaväzuje sa poskytovateľ dodržiavať miestne podmienky pre výkon služieb, s ktorými bude preukázateľne oboznámený.
- 3.15 Zmluvné strany sa zaväzujú oznámiť si navzájom akékoľvek zmeny údajov dôležitých pre bezproblémové plnenie zmluvy, a to najmä údajov uvedených v záhlaví tejto zmluvy, príp. iných kontaktných údajov vymedzených v tejto zmluve.
- 3.16 Poskytovateľ sa zaväzuje umožniť výkon kontroly súvisiaci s predmetom plnenia tejto zmluvy, ako aj s ostatnými ustanoveniami tejto zmluvy zo strany osôb oprávnených na výkon kontroly, kedykoľvek po uzavretí tejto zmluvy a počas platnosti a účinnosti Zmluvy o

nenávratnom finančnom príspevku č. 4258/2022 uzavretej medzi poskytovateľom nenávratného finančného príspevku a objednávateľom dňa 20.12.2022 ; oprávnenými osobami sú najmä:

- Riadiaci orgán (poskytovateľ) a ním poverené osoby;
- Najvyšší kontrolný úrad SR;
- príslušná správa finančnej kontroly;
- certifikačný orgán a nimi poverené osoby;
- orgán auditu, jeho spolupracujúce orgány a nimi poverené osoby;
- splnomocnení zástupcovia Európskej Komisie a Európskeho dvora audítorov, osoby prizvané orgánmi, ktoré sú uvedené ako oprávnené osoby v súlade s príslušnými právnymi predpismi SR a EÚ.

Táto povinnosť sa vzťahuje aj na subdodávateľov Poskytovateľa.

- 3.17 Poskytovateľ sa zaväzuje poskytnúť osobám oprávneným na výkon kontroly špecifikovaným v bode 3.9 tohto článku, všetku potrebnú súčinnosť. V prípade, že v dôsledku kontroly vykonanej oprávneným orgánom, dôjde zavinením poskytovateľa k uznaniu plnenia predmetu tejto zmluvy ako neoprávneného výdavku, t. j. výdavku, ktorý nezodpovedá cenám bežným na trhu v čase ich vzniku a v mieste ich vzniku, a ktorý preto nebude objednávateľovi uznaný ako oprávnený, je poskytovateľ povinný nahradiť objednávateľovi v plnom rozsahu škodu, ktorá mu v dôsledku tejto skutočnosti vznikne.
- 3.18 Poskytovateľ bude rešpektovať právo osôb oprávnených na výkon kontroly podľa bodu 3.9 tohto článku vstupovať do objektov, ak to súvisí s predmetom tejto zmluvy a požadovať od poskytovateľa predloženie originálnych dokladov a inú potrebnú dokumentáciu, alebo iné ďalšie doklady súvisiace s touto zmluvou.
- 3.19 Poskytovateľ sa zaväzuje prijať opatrenia na nápravu nedostatkov zistených kontrolou, overovaním na mieste v zmysle Správy z kontroly, v lehote stanovenej osobami oprávnenými na výkon kontroly podľa bodu 3.9 tohto článku, a zároveň zaslať objednávateľovi informáciu o splnení opatrení prijatých na nápravu zistených nedostatkov bezodkladne po ich splnení.
- 3.20 Zmluvné strany sa dohodli, že poskytovateľ v postavení veriteľa nepostúpi akúkoľvek svoju pohľadávku z tejto zmluvy tretej osobe bez predchádzajúceho písomného súhlasu dlžníka - objednávateľa. Rovnakým spôsobom poskytovateľ pohľadávku voči objednávateľovi nezabezpečí ručením treťou osobou alebo žiadnym iným právne prípustným spôsobom poskytovateľ neposkytne práva k takejto pohľadávke tretej osobe. Písomný súhlas objednávateľa s takýmito úkonmi je zároveň platný len za podmienky, že bol na tento úkon udelený predchádzajúci písomný súhlas Ministerstva zdravotníctva SR. V prípade, že dôjde zo strany poskytovateľa k porušeniu tejto povinnosti a svoje práva a povinnosti z tejto zmluvy postúpi, resp. prijme ručenie tretej osobe bez súhlasu protistrany, bude sa takýto úkon považovať za neplatný a neúčinný voči objednávateľovi.
- 3.21 Odklad účinnosti: „Odkladacia podmienka nadobudnutia účinnosti zmluvy: Zmluva nadobudne účinnosť až po schválení procesu verejného obstarávania poskytovateľom nenávratného finančného príspevku – dňom vydania správy z administratívnej kontroly procesu VO. Ak výsledok predmetnej kontroly verejného obstarávania nebude kladný, nie je splnená podmienka k nadobudnutiu účinnosti zmluvy. Z uvedeného dôvodu k plneniu zmluvy nemôže dôjsť skôr, ako sa zmluva s úspešným uchádzačom stane účinnou. Po doručení správy z kontroly verejného obstarávania prijímateľ (Objednávateľ) bezodkladne upozorní na túto skutočnosť Poskytovateľa.“

Čl. IV

Trvanie zmluvy

- 4.1 Táto zmluva sa uzatvára na dobu určitú, na 69 mesiacov odo dňa nadobudnutia jej účinnosti.
- 4.2 Zmluvné strany sa dohodli, že pred uplynutím dojednanej doby platnosti, táto zmluva zaniká:
- 4.2.1 písomnou dohodou zmluvných strán,

- 4.2.2 výpoveďou ktorejkoľvek zmluvnej strany aj bez udania dôvodu s trojmesačnou výpovednou lehotou, ktorá začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane, alebo
- 4.2.3 odstúpením od zmluvy v prípadoch upravených touto zmluvou.
- 4.3 Objednávateľ má právo odstúpiť od zmluvy, ak poskytovateľ opakovane neposkytne služby v súlade s touto zmluvou. V takom prípade sa rušia tie služby, u ktorých ešte nedošlo k ich prevzatiu zo strany objednávateľa v súlade s touto zmluvou a poskytovateľ nemá nárok na úhradu žiadnych nákladov, ktoré mu v súvislosti s danými službami vznikli. Právo objednávateľa na náhradu škody tým nie je dotknuté.

Čl. V **Kontaktné osoby**

- 5.1 Osobami oprávnenými konať za zmluvné strany pri plnení predmetu tejto zmluvy sú:
- za objednávateľa (ktorákoľvek z nasledovných osôb) – preberanie plnení a súvisiace úkony v mene objednávateľa: 1) meno: RNDr. Ivan Záhumenský, funkcia: vedúci Oddelenia informačných technológií, tel., email:, 2) meno: Ing. Lukáš Križan, tel., email:, 3) meno:, tel., email:
 - za poskytovateľa (ktorákoľvek z nasledovných osôb) – odovzdávanie plnení a súvisiace úkony v mene poskytovateľa: meno: Mario Háronik funkcia: konateľ, tel., email:
- 5.2 Každá zmluvná strana je oprávnená zmeniť svojich zástupcov uvedených v bode 5.1 tohto článku zmluvy písomným oznámením doručeným druhej zmluvnej strane.

Čl. VI **Závazok mlčanlivosti**

- 6.1 Zmluvné strany týmto berú na vedomie, že informácie nadobudnuté v rámci plnenia zmluvy budú považované za informácie dôverné a za súčasť obchodného tajomstva druhej zmluvnej strany.
- 6.2 Zmluvné strany sa zaväzujú zachovávať mlčanlivosť o dôverných informáciách. Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej zmluvnej strany neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k dôverným informáciám.
- 6.3 Za dôverné informácie sa považujú všetky a akékoľvek údaje, dáta, podklady, poznatky, dokumenty alebo akékoľvek iné informácie, bez ohľadu na formu ich zachytenia:
- a) ktoré sa týkajú tejto zmluvy a jej plnenia (najmä zmluva, informácie o právach a povinnostiach zmluvných strán ako i informácie o cene);
 - b) ktoré sa týkajú zmluvnej strany (najmä informácie o jej činnosti, štruktúre, hospodárskych výsledkoch, všetky zmluvy, finančné, štatistické a účtovné informácie, informácie o jej majetku, aktívach a pasívach, pohľadávkach a záväzkoch, informácie o jej technickom a programovom vybavení, know-how, hodnotiace štúdie a správy, podnikateľské stratégie a plány, informácie týkajúce sa predmetov chránených právom priemyselného alebo iného duševného vlastníctva a všetky ďalšie informácie o zmluvnej strane;
 - c) ktoré sa týkajú obchodných partnerov zmluvných strán;
 - d) pre ktoré je stanovený všeobecne záväznými právnymi predpismi Slovenskej republiky osobitný režim nakladania (najmä obchodné tajomstvo, bankové tajomstvo, daňové tajomstvo, telekomunikačné tajomstvo, osobné údaje, utajované skutočnosti);
 - e) ktoré boli poskytnuté zmluvnej strane/získané zmluvnou stranou pred nadobudnutím platnosti a účinnosti zmluvy, pokiaľ sa týkajú jej predmetu a/alebo obsahu (najmä žiadosť o cenovú ponuku, cenová ponuka);
 - f) ktoré sú výslovne zmluvnou stranou označené ako „dôverné“, „confidential“, „proprietary“ alebo iným obdobným označením.

- 6.4 Dôverné informácie poskytnuté, odovzdané, oznámené, sprístupnené a/alebo akýmkoľvek iným spôsobom získané jednou zmluvnou stranou od druhej zmluvnej strany na základe a/alebo v akejkoľvek súvislosti so zmluvou môžu byť použité výhradne na účely plnenia predmetu zmluvy a v súlade s predpismi, ktoré upravujú nakladanie s takýmito údajmi. Zmluvné strany sa zaväzujú dôverné informácie ako aj všetky informácie poskytnuté, odovzdané, oznámené, sprístupnené a/alebo akýmkoľvek iným spôsobom získané zmluvnými stranami na základe zmluvy a/alebo v akejkoľvek súvislosti so zmluvou udržiavať v prísnej tajnosti, zachovávať o nich mlčanlivosť a chrániť ich pred zneužitím, poškodením, zničením, znehodnotením, stratou a odcudzením, a to i po ukončení platnosti a účinnosti zmluvy. Zmluvná strana nie je oprávnená bez predchádzajúceho písomného súhlasu druhej zmluvnej strany dôverné informácie poskytnúť, odovzdať, oznámiť, sprístupniť, zverejniť, publikovať, rozširovať, vyzradiť ani použiť inak než na účely plnenia predmetu zmluvy, a to ani po ukončení platnosti a účinnosti zmluvy, s výnimkou prípadu ich poskytnutia /odovzdania /oznámenia/ sprístupnenia:
- a) (i) ovládanej osobe zmluvnej strany; (ii) ovládajúcej osobe zmluvnej strany; (iii) osobe, vo vzťahu ku ktorej má ovládajúca osoba zmluvnej strany postavenie ovládanej osoby alebo podobné postavenie; a (iv) osobe, v ktorej má ovládajúca osoba zmluvnej strany postavenie ovládajúcej osoby alebo podobné postavenie, pričom uvedené osoby budú mať vo vzťahu k ochrane dôverných informácií rovnaké povinnosti ako zmluvné strany;
- 6.5 Povinnosť zmluvných strán zachovávať mlčanlivosť o dôverných informáciách sa nevzťahuje na informácie, ktoré:
- a) boli zverejnené už pred podpisom zmluvy, čo musí byť preukázateľné na základe poskytnutých podkladov, ktoré túto skutočnosť dokazujú;
 - b) sa stanú všeobecne a verejne dostupné po podpise zmluvy z iného dôvodu ako z dôvodu porušenia povinností podľa zmluvy, čo musí byť preukázateľné na základe poskytnutých podkladov, ktoré túto skutočnosť dokazujú;
 - c) majú byť sprístupnené na základe povinnosti stanovenej zákonom, rozhodnutím súdu, prokuratúry alebo iného oprávneného orgánu verejnej moci, pričom v tomto prípade zmluvná strana, ktorá je povinná informácie sprístupniť, bezodkladne doručí druhej zmluvnej strane písomné oznámenie o tejto skutočnosti ešte pred sprístupnením týchto informácií;
 - d) boli získané zmluvnou stranou od tretej strany, ktorá ich legitímne získala alebo vyvinula a ktorá nemá žiadnu povinnosť, ktorá by obmedzovala ich zverejňovanie;
 - e) na prípady, ak zmluvná strana zverejnila dôverné informácie s predchádzajúcim písomným súhlasom druhej zmluvnej strany.
- 6.6 V prípade, že zmluvná strana zistí, že došlo, alebo môže dôjsť k prezradeniu, resp. získaniu dôverných informácií neoprávnenou osobou, zaväzuje sa bezodkladne informovať o tejto skutočnosti druhú zmluvnú stranu a podniknúť všetky kroky potrebné k zabráneniu vzniku škody alebo k jej maximálnemu obmedzeniu, pokiaľ sa zmluvné strany nedohodnú inak.
- 6.7 V prípade, že v rámci plnenia tejto zmluvy budú za účelom riadnej realizácie predmetu plnenia poskytovateľovi poskytnuté osobné údaje, tieto sa taktiež považujú za dôverné informácie. V takom prípade je poskytovateľ povinný plniť všetky príslušné povinnosti podľa aktuálnej právnej úpravy týkajúcej sa ochrany osobných údajov. V prípadoch, ak by si realizácia spolupráce medzi poskytovateľom a objednávateľom podľa tejto zmluvy vyžadovala akékoľvek spracúvanie osobných údajov fyzických osôb, sú zmluvné strany povinné dodržiavať ustanovenia Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a tiež zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a vstúpiť do potrebných zmluvných vzťahov regulujúcich podmienky ich spracúvania.
- 6.8 Ak jedna zo zmluvných strán poruší podmienky uvedené v tomto článku tejto zmluvy, uhradí druhej zmluvnej strane preukázateľnú škodu.
- 6.9 Zánikom tejto zmluvy nie sú dotknuté prípadné povinnosti zmluvných strán, týkajúce sa dôverných informácií, vyplývajúce zo všeobecne záväzných právnych predpisov.

Čl. VII

Zodpovednosť za škodu

- 7.1 Zmluvné strany sa dohodli, že poskytovateľ zodpovedá objednávateľovi iba za škodu, ktorú mu spôsobí zavineným porušením svojich povinností a omisívnym konaním pri poskytovaní služieb podľa tejto zmluvy.
- 7.2 Zmluvné strany sa dohodli, že v prípade porušenia povinností poskytovateľa má objednávateľ nárok uplatniť si skutočnú škodu, ktorá mu bola spôsobená a ušlý zisk a nemá právo uplatniť si škodu spôsobenú pre nemožnosť plnenia, spôsobenú inou okolnosťou ako okolnosťou vylučujúcou zodpovednosť v zmysle § 353 Obchodného zákonníka alebo vyššou mocou.
- 7.3 Poskytovateľ je povinný pri uzatvorení tejto zmluvy preukázať písomné uzatvorenie poistnej zmluvy, z ktorej plnenie bude poisťovňou poukávané v prípade spôsobenia škody priamo na účet objednávateľa.

Čl. VIII

Práva duševného vlastníctva

- 8.1 Za predpokladu, že v rámci plnenia svojich záväzkov z tejto zmluvy poskytovateľ poskytne také plnenie, ktoré by požívalo autorskoprávnu ochranu v zmysle zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov, udeľuje touto zmluvou objednávateľovi licenciu na užívanie daného plnenia, pričom v takom prípade je odplata za licenciu zahrnutá v cene za poskytovanie služby.
- 8.2 V prípade ak súčasťou predmetu plnenia sú aj licencie v zmysle bodu 8.1 tohto článku zmluvy, poskytovateľ v zmysle zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov, týmto prevádza na objednávateľa licenciu na dielo vytvorené na základe tejto zmluvy podľa § 65 a nasl. autorského zákona nasledovne:
- a) licencia je výhradná,
 - b) licencia je v neobmedzenom rozsahu,
 - c) licencia sa udeľuje na dobu neurčitú,
 - d) bez práva objednávateľa udeľovať sublicencie,
 - e) spôsob použitia diela: bežné používanie a zabezpečenie funkcionality predmetu plnenia, spracovanie, právo začleniť dielo do súborného diela, právo dielo meniť.

Čl. IX

Záverečné ustanovenia

- 9.1 Táto zmluva je vyhotovená v šiestich vyhotoveniach, pričom každý má povahu originálu. Objednávateľ obdrží päť vyhotovení zmluvy a poskytovateľ obdrží jedno vyhotovenie zmluvy.
- 9.2 Zmluvné strany sa dohodli, že meniť alebo dopĺňať túto zmluvu je možné len formou obojstranne potvrdených písomných dodatkov k tejto zmluve pri dodržaní podmienok podľa § 18 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, na ktorých platnosť sa vyžaduje, aby boli riadne potvrdené a podpísané oprávnenými zástupcami zmluvných strán. K návrhom dodatkov k tejto zmluve sa zmluvné strany zaväzujú vyjadriť písomne, v lehote 14 dní od doručenia návrhu dodatku. Po tú istú dobu je týmto návrhom viazaná zmluvná strana, ktorá ho podala.

- 9.3 Právne vzťahy neupravené touto zmluvou sa riadia najmä príslušnými ustanoveniami Obchodného zákonníka, v znení neskorších predpisov a súvisiacimi platnými právnymi predpismi Slovenskej republiky.
- 9.4 Zmluvné strany sa dohodli, že všetky rozpory vyplývajúce z plnenia zmluvy, budú riešiť predovšetkým dohodou a vzájomným rokovaním. Až v prípade, ak nedôjde k dohode, uplatní ktorákoľvek zo zmluvných strán svoje práva zo zmluvy na príslušnom súde Slovenskej republiky.
- 9.5 Každé ustanovenie tejto zmluvy sa, pokiaľ je to možné, interpretuje tak, že je účinné a platné podľa platných právnych predpisov. Pokiaľ by však niektoré ustanovenie tejto zmluvy bolo podľa platných právnych predpisov nevymožiteľné alebo neplatné, bude neúčinné iba v rozsahu tejto nevymožiteľnosti alebo neplatnosti a ostatné ustanovenia tejto zmluvy budú i naďalej záväzné a v plnom rozsahu platné a účinné. V prípade takejto nevymožiteľnosti alebo neplatnosti budú zmluvné strany v dobrej viere rokovať, aby sa dohodli na zmenách alebo doplnkoch tejto zmluvy, ktoré sú potrebné na realizáciu zámerov tejto zmluvy z hľadiska tejto nevymožiteľnosti alebo neplatnosti.
- 9.6 Zmluvné strany sa dohodli, ak nie je v tejto zmluve pri jednotlivých úkonoch ustanovené inak, že akékoľvek oznámenia, správy a pod. (ďalej aj len ako „**oznámenia**“) týkajúce sa tejto zmluvy, si zmluvné strany budú doručovať niektorým z nasledovných spôsobov: osobne, doporučeným listom s doručenkou, kuriérom, faxom alebo emailom na adresy zmluvných strán a kontaktné údaje uvedené v záhlaví a texte tejto zmluvy. V prípade, ak zmluvná strana doručuje formou doporučeného listu s doručenkou a zmluvná strana, ktorej je oznámenie adresované, jeho prijatie odmietne alebo iným spôsobom jeho prijatiu zabráni (neoznámením zmeny jej adresy alebo iných kontaktných údajov), považuje sa na účely tejto zmluvy za preukázané doručenie vrátane nedoručenej zásielky odosielateľovi podľa poslednej známej adresy takejto zmluvnej strany. To platí aj vtedy, ak je v tejto zmluve začiatok dohodnutej lehoty viazaný na okamih doručenia písomnosti. V takomto prípade sa za okamih doručenia považuje okamih vrátenia nedoručenej zásielky odosielateľovi. Za poslednú známu adresu zmluvnej strany sa považuje adresa pozostávajúca z označenia obce, názvu ulice alebo verejného priestranstva (ak je obec členená na ulice a inak označované verejné priestranstvá), súpisného, popr. i orientačného čísla a poštového smerovacieho čísla a v prípade, ak ide o adresu mimo Slovenskej republiky i označenie štátu, oznámená písomne inej zmluvnej strane, inak adresa, ktorá je uvedená pri každej zo zmluvných strán v záhlaví tejto zmluvy. Ak niektorá zo zmluvných strán v súlade a za podmienok uvedených v tejto zmluve oznámi inej zmluvnej strane zmenu adresy, považuje sa za poslednú známu adresu táto oznámená adresa, a to vždy tá, ktorá bola oznámená najneskôr. Pre účely tejto zmluvy budú oznámenia považované za doručené dňom:
- potvrdenia doručenia adresátom, alebo dňom odmietnutia prevzatia zásielky adresátom, ak sa doručuje osobne, alebo
 - potvrdenia doručenia adresátom alebo dňom odmietnutia prevzatia zásielky adresátom, ak sa doručuje kuriérom, alebo
 - potvrdenia doručenia adresátom alebo dňom odmietnutia prevzatia zásielky adresátom, ak sa doručuje doporučenou poštovou zásielkou s doručenkou alebo
 - potvrdenia prenosu faxovej správy, ak sa doručuje faxom, alebo
 - potvrdenia doručenia emailu adresátom, a v prípade, ak k potvrdeniu doručenia emailu nedôjde ani nasledujúci deň po jeho odoslaní, dňom otvorenia emailovej zásielky druhou stranou.
- 9.7 Zmluvné strany sa zaväzujú, že sa budú počas realizácie tejto zmluvy oboznamovať o všetkých skutočnostiach spôsobilých mať vplyv na realizáciu práv a povinností vyplývajúcich z právnych vzťahov založených touto zmluvou. Zmluvné strany sa tiež zaväzujú, že bez zbytočného odkladu, najneskôr však v lehote 30 dní, sa budú vzájomne oboznamovať o všetkých skutočnostiach spôsobilých mať vplyv na práva a právom chránené záujmy inej zmluvnej strany.

- 9.8 Ak niektoré ustanovenia tejto zmluvy neskôr stratia účinnosť, nie je tým dotknutá platnosť ostatných ustanovení. Namiesto neúčinných ustanovení a na vyplnenie medzier sa použije úprava, ktorá, pokiaľ je to právne možné, sa čo najviac približuje zmyslu a účelu tejto zmluvy.
- 9.9 Zmluvné strany vyhlasujú, že ich zmluvná voľnosť nie je obmedzená, ich zmluvné prejavy sú určité a zrozumiteľné. Zmluva je uzavretá za vzájomne dohodnutých podmienok, nie v tiesni, omyle alebo za nápadne nevýhodných podmienok.
- 9.10 Zmluva je platná dňom jej podpisu zmluvnými stranami a účinná podľa bodu 3.15 tejto Zmluvy.
- 9.11 Neoddeliteľnou súčasťou tejto zmluvy sú nasledovné prílohy:
- Príloha č. 1: Špecifikácia služieb LMS, SIEM a SOC
 - Príloha č. 2: Kalkulácia ceny
 - Príloha č. 3: Sizing zariadení objednávateľa
 - Príloha č. 4: Popis navrhovaného riešenia
 - Príloha č. 5: Poistná zmluva poskytovateľa
 - Príloha č. 6: Zoznam subdodávateľov

V Trenčíne, dňa

V Žiline dňa.....

Za objednávateľa:

Za poskytovateľa:

.....
Ing. Tomáš Janík, MBA
riaditeľ
Fakultná nemocnica Trenčín

.....
Mario Háronik
Konateľ
AUTOCONT s.r.o.

1. 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 nesúladow v dokumentačnej časti zo zákonného auditu kybernetickej bezpečnosti.

2. 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 objednávaní 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 nesúladow v dokumentácii na základe auditu kybernetickej bezpečnosti podrobne popísaná v kapitole 3.6.

3. 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 verejnemu 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 verejnemu 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 verejnemu 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 prioritizácia 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. Nevyužitú MD je možné v rámci jedného roku preniesť do ďalšieho mesiaca. Na konci každého roku sa nevyužitú 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 vyšetrení 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 vyšetrení 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“.

3.5.1 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 zedefinovanie procesov pre činnosti SOC a jeho zaintegrovanie do bezpečnostného riešenia verejného obstarávateľa
- zedefinovanie udalosti a bezpečnostného incidentu,
- zedefinovanie podmienok pre klasifikáciu a prioritizáciu 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 nesúladv 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.

4. 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 poskytnie 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:

- a) 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.
- b) Cenu za riešenie v prílohe „Kalkulácia ceny“

Uchádzačom ponúkané riešenie splňa vyššie uvedené požiadavky.

Príloha č. 2
Kalkulácia ceny

Tab. 1	Fáza projektu	% kapacít	min. MD	počet MD	percento	poč. mes.
Etapa 1	Analýza a dizajn	10-35 %	45	45	32,61%	2
Etapa 2	Implementácia a testovanie	30-80 %	55	55	39,86%	4
Etapa 3	Nasadenie	15-30 %	38	38	27,54%	3
	SPOLU		138	138	100,01%	9

Tab. 2	špecialista	max. sadzba	revid. sadzba	reálna sadzba	reál. percento	spolu MD
	IT architekt	910 €	500 €	500 €	4,35%	6
	IT tester	570 €	380 €	500 €	1,45%	2
	IT programátor/vývojár	650 €	400 €	470 €	7,25%	10
	Projektový manažér IT projektu	890 €	500 €	470 €	20,29%	28
	IT analytik	740 €	450 €	500 €	6,52%	9
	Odborník pre IT dohľad	890 €	644 €	500 €	4,35%	6
	Špecialista pre bezpečnosť IT	1 200 €	619 €	500 €	4,35%	6
	HW špecialista	790 €	450 €	500 €	1,45%	2
	Špecialista pre databázy	600 €	464 €	500 €	4,35%	6
	Školiteľ pre IT systémy	710 €	400 €	500 €	0,00%	0
	IT/IS konzultant	900 €	448 €	470 €	45,65%	63
	Iné	570 €	560 €	500 €	0,00%	0
						138

Tab. 3	špecialista	sadzba	počet MD	cena spolu	cena+DPH
Etapa 1	IT architekt	500 €	4	2 000 €	2 400 €
	IT tester	500 €		0 €	0 €
	IT programátor/vývojár	470 €	2	940 €	1 128 €
	Projektový manažér IT projektu	470 €	8	3 760 €	4 512 €
	IT analytik	500 €	5	2 500 €	3 000 €
	Odborník pre IT dohľad	500 €		0 €	0 €
	Špecialista pre bezpečnosť IT	500 €	2	1 000 €	1 200 €
	HW špecialista	500 €	2	1 000 €	1 200 €
	Špecialista pre databázy	500 €	2	1 000 €	1 200 €
	Školiteľ pre IT systémy	500 €		0 €	0 €
	IT/IS konzultant	470 €	20	9 400 €	11 280 €
	Iné	500 €		0 €	0 €
	SPOLU		45	21 600 €	25 920 €
Etapa 2	IT architekt	500 €	2	1 000 €	1 200 €
	IT tester	500 €	2	1 000 €	1 200 €
	IT programátor/vývojár	470 €	8	3 760 €	4 512 €
	Projektový manažér IT projektu	470 €	12	5 640 €	6 768 €
	IT analytik	500 €	2	1 000 €	1 200 €

	Odborník pre IT dohľad	500 €	2	1 000 €	1 200 €
	Špecialista pre bezpečnosť IT	500 €	2	1 000 €	1 200 €
	HW špecialista	500 €		0 €	0 €
	Špecialista pre databázy	500 €	2	1 000 €	1 200 €
	Školiteľ pre IT systémy	500 €		0 €	0 €
	IT/IS konzultant	470 €	23	10 810 €	12 972 €
	Iné	500 €		0 €	0 €
	SPOLU		55	26 210 €	31 452 €
Etapa 3	IT architekt	500 €		0 €	0 €
	IT tester	500 €		0 €	0 €
	IT programátor/vývojár	470 €		0 €	0 €
	Projektový manažér IT projektu	470 €	8	3 760 €	4 512 €
	IT analytik	500 €	2	1 000 €	1 200 €
	Odborník pre IT dohľad	500 €	4	2 000 €	2 400 €
	Špecialista pre bezpečnosť IT	500 €	2	1 000 €	1 200 €
	HW špecialista	500 €		0 €	0 €
	Špecialista pre databázy	500 €	2	1 000 €	1 200 €
	Školiteľ pre IT systémy	500 €		0 €	0 €
	IT/IS konzultant	470 €	20	9 400 €	11 280 €
	Iné	500 €		0 €	0 €
	SPOLU		38	18 160 €	21 792 €
	Cena za licencie počas etapy 1-3			19 000 €	22 800 €
	SUMA ZA ETAPU 1-3			84 970 €	101 964 €

Tab. 4	PREVÁDZKA - PAUŠÁL		mesiac	rok	5 rokov	cena+DPH
	Služba - poskytnutie HW infraštruktúry		152 €	1 824 €	9 120 €	10 944 €
	Služba - SOC, SIEM, LMS - úvodná cena		1 350 €			
	Odhad - SOC, SIEM, LMS - záverečná cena		1 350 €			
	SOC, SIEM, LMS - priemerná cena		1 350,0 €	16 200 €	81 000 €	97 200 €
	Cena za licencie počas prevádzky		309 €	3 708 €	18 540 €	22 248 €
	SUMA ZA PREVÁDZKU				108 660 €	130 392 €

Tab. 5	SUMA CELKOM				193 630 €	232 356 €
--------	-------------	--	--	--	-----------	-----------

Tab. 6	typ zariadenia	prírastok	poplatok	paušál	c.cena
	Windows Desktopy / Notebooky	150	245 €	0 €	0 €
	Windows Servery	7	245 €	0 €	0 €
	Linux / Unix servery	0	245 €	0 €	0 €
	Switche	10	245 €	0 €	0 €
	WiFi AP	46	580 €	0 €	0 €
	Diskové polia	1	245 €	0 €	0 €
	VLAN	35	245 €	0 €	0 €
	Antivírusový klient	180	245 €	0 €	0 €
	Web Servery (IIS, Apache, Tomcat)	3	580 €	0 €	0 €

	Databázy (MSSQL, PostgreSQL, MySQL)	4	580 €	0 €	0 €
	Email - Office365 klient	81	580 €	0 €	0 €
	ILO, iDrac	3	245 €	0 €	0 €
	SPOLU				0 €

LMS, SIEM, SOC - príloha č. 9 SP – Sizing		
	FAKULTNÁ NEMOCNICA TRENČÍN Legionárska 28, 911 71 Trenčín	
Fakultná nemocnica Trenčín	štartovací počet zariadení	odhad koncového počtu po 5 rokoch
Windows Servery	37	44
Windows Desktopy / Notebooky	680	830
Windows AD DC servery	2	2
Linux / Unix servery	10	10
Virtualizácia (počet nodov, typ virtualizácia)	36	45
Sieťová infraštruktúra		
Sieťové routre	3	3
Sieťové switche	90	100
Sieťové WiFi AP	94	140
Diskové polia	5	6
Bezpečnostná infraštruktúra		
VLAN	15	50
Sieťové firewally	3	2
IPS/IDS	1	1
VPN brány	2	2
Antivírusoví klienti	700	880
Aplikácie		
Web Servery (IIS, Apache, Tomcat)	22	25
Databázy (MSSQL, Oracle, PostgreSQL, MySQL) - počet inštancií	10	14
Email - Office365 (počet užívateľov)	369	450
Nemocničný informačný systém - vysoké EPS	2	2
PACS systém - vysoké EPS	2	2
Laboratórny informačný systém - vysoké EPS	2	2
Iné		
Out of Band Management serverov - ILO, iDrac	5	8

Uchádzačom ponúkané riešenie zohľadňuje odhadovaný počet zariadení na konci 5-ročného obdobia.

Popis navrhovaného riešenia

1. Služby AC Bezpečnostného dohľadu – popis

1.1 Služba kontaktného miesta AC SOC

Hlavný prístupový a komunikačný bod je Servis Desk AC SOC Poskytovateľa, ktorý zaisťuje komunikáciu a predáva Požiadavky na riešiteľské tímy. Požiadavky môžu zadávať Kontaktné osoby Objednávateľa nasledujúcim spôsobom:

- telefonicky: +421 XXX[SIEM AC SOC] – úplné číslo bude uvedené pri podpise zmluvy
- prostredníctvom emailu: [\[SIEM AC SOC\]@autocont.sk](mailto:[SIEM AC SOC]@autocont.sk)

Obsahom Služby je:

- príjem požiadaviek,
- odovzdanie na riešiteľské tímy (pracovníci Poskytovateľa a súčinnosť s Objednávateľom),
- sledovanie životného cyklu požiadaviek,
- administratívne uzatváranie požiadaviek podľa nastavených procesov.

Za vyriešenie sa považuje každá Požiadavka, ktorej riešenie bolo akceptované Kontaktnou osobou Objednávateľa. Požiadavka sa považuje za vyriešenie aj bez toho, aby Kontaktná osoba akceptovala vyriešenie Požiadavky vtedy, pokiaľ nevzniesie k jeho riešeniu pripomienky v lehote 5 pracovných dní po písomnej výzve k akceptácii vyriešenia predmetnej Požiadavky.

Služba je poskytovaná v režimoch od 5 x 8 až do 7 x 24 s SLA od 4 hodín (podľa klasifikácie)

1.2 Služba riadenia a koordinácie poskytovaných služieb AC SOC

Pridelený Service Delivery Manager Poskytovateľa zaisťuje projektové vedenie v úvodnej fáze predimplementačnej analýzy a implementácie až do okamihu zahájenia poskytovania služby.

Potom funguje jako garant kvality služieb Poskytovateľa. Koordinuje dodávku Servisných služieb, dbá na kvalitu poskytovaných Servisných služieb, riadi a kontroluje dodávky Servisných služieb, sprostredkováva statické výstupné informácie (reporty), ktoré predkladá podľa nastaveného zmluvného plnenia Objednávateľovi. Proaktívne identifikuje možnosti zlepšenia dodávky poskytovaných Servisných služieb.

Rieši zmluvné zmeny v úrovni poskytovania služby.

1.3 AC SOC priebežný bezpečnostný dohľad

Služby AC Bezpečnostného dohľadu sú prostredníctvom „Security Operations Centra“ (SOC) spoločnosti AUTOCONT s.r.o. poskytované v tomto rozsahu:

- Obsluha kontaktného miesta AC SOC (príjem požiadaviek)
- Sledovanie dostupnosti služby a funkčnosti SIEM
- Analýzu korelácií vzniknutých KBÚ z logov a flow niekoľkokrát denne
- Analýza KBÚ s cieľom identifikácie možných KBI
- Riadenie a koordinácia služieb smerom k Objednávateľovi pri riešení KBÚ a KBI podľa SLA
- Alerting v reálnom čase pomocou základných komunikačných nástrojov: mail, sms, telefón
- Reporting – 1x mesačne - report o detekovaných incidentoch (Offenses) s návrhy prípadných systematických opatrení (report dokument). Výkonnostné štatistiky (zaplnenie, EPS, FPM).
- Požiadavky na zmenu konfigurácie SIEM (úpravy parserov, aktualizácie pravidiel, zmeny referenčných číselníkov, úpravy v reportoch, apod.)
- Napojenie nových zdrojov do SIEM

- Mesačná profylaxia a aktualizácia SW SIEM a úložiska logov (údržba HW, pokiaľ je súčasťou dodávky služby)

Pozn.: Vlastné riešenie KBI nie je predmetom plnenia tejto Servisnej služby.

Servisná služba je poskytovaná Vzdialeným pripojením pracovníka Poskytovateľa, mailom či telefonicky.

1.4 AC SOC konzultačné služby

Servisná služba je poskytovaná Pracovníkmi Poskytovateľa v prípade rozsiahlych zmien v infraštruktúre Objednávateľa, poradenstvom v súvislosti s obstaraním nových systémov alebo technológií, školením, apod.

Objem prác sa riadi ceníkom a SLA (harmonogram plnenia je podľa vzájomnej dohody).

IBM Security QRadar XDR Package: Modernizuje zabezpečenie pomocou otvorenej platformy

IBM Security QRadar XDR Package je otvorená platforma pre oblasť kybernetickej bezpečnosti a automatizácie SOC procesov, postavená na kontajnerizačnej platforme, vďaka čomu môže bezpečnostný tím IBM veľmi rýchlo a efektívne vyvíjať nové aplikácie a funkcie do Package. Technológia postavená na otvorených štandardoch tak ponúka možnosť prepojenia s cloudovým aj on-premisovým svetom. Zároveň umožňuje pripájať množstvo rôznych dátových zdrojov a nástrojov tretích strán.

Prostredníctvom otvorených štandardov a inovácií IBM Security QRadar XDR Package umožňuje prístup k nástrojom IBM a tretích strán na vyhľadávanie indikátorov hrozieb v cloude alebo na lokálnych miestach. IBM prispela technológiou open source používanou v QRadar XDR Package na zabezpečenie a nadviazala vzťahy s desiatkami spoločnosťami prostredníctvom OASIS Open Cybersecurity Alliance, aby podporila interoperabilitu a pomohla znížiť viazanosť dodávateľov.

IBM Security QRadar XDR Package sa skladá z kontajnerového softvéru vopred integrovaného s platformou podnikových aplikácií. Táto integrácia umožňuje bežať on-premise a v súkromných alebo verejných cloudoch, čo organizáciám poskytuje flexibilitu pri nasadzovaní tam, kde sa rozhodnú.

IBM Security QRadar XDR Package kombinuje technológiu kontajnerov, softvér a dynamickú formu licencovania. Zákazník si flexibilne vyberie, čo bude chcieť využívať. Táto architektúra prináša celý rad benefitov: rýchlejší deployment aplikácií, nižšie nároky na IT operations, perfektný súlad s korporátnymi štandardmi.

IBM Security QRadar XDR Package je podniková bezpečnostná superplatforma, ktorá môže pomôcť rýchlo posunúť kľúčové obchodné aplikácie do vhodného typu cloudu (privátneho, hybridného či verejného). Základom sú kontajnery a kontajnerizované aplikácie, špeciálne optimalizované na beh v Red Hat OpenShift, zaisťujúce orchestráciu a správu. Vďaka tomu poskytuje vývojárom, správcom dát a administrátorom otvorené prostredie pre rýchle vytváranie nových natívnych cloudových aplikácií, modernizáciu existujúcich aplikácií a možnosť zaradiť AI konzistentným spôsobom a to aj vo viacerých cloudoch. Umožňuje ľahko nasadiť moderný podnikový softvér podľa svojho výberu formou on-premise, cloudových alebo predintegrovaných systémov a rýchlo tak preniesť pracovnú záťaž do produkčných systémov. Celá platforma využíva otvorený softvér a štandardy s vysokou mierou bezpečnosti. Pokročilé nástroje pre správu umožňujú dosiahnuť požadovanú úroveň kvality aplikácií v priebehu celého životného cyklu.

Formy obstarania IBM Security QRadar XDR Package

1) Nové, trvalé (perpetual) licencie

Prvotný nákup licencií IBM SW formou CAPEX, ako trvalé licencie s 12-mesačnou podporou. Po ubehnutí tohto cyklu je možnosť zakúpiť predĺženie softvérovej podpory alebo ďalej natrvalo užívať softvér bez výhod plynúcich z aktívnej podpory produktu.

2) Trade-up z existujúcich IBM riešení

Povýšenie existujúcich licencií IBM SW, ktoré sú obsiahnuté v niektorom z Cloud pakov, formou tzv. Trade-up.

Licencovanie IBM Security QRadar XDR Package cez MVS

Managed Virtual Server (MVS) je mernou jednotkou, na základe ktorej môže byť IBM Security QRadar XDR Package licencovaný. Server je fyzický počítač, ktorý sa skladá z CPU, pamäte a vstupných/výstupných rozhraní, a ktorý vykonáva požadované procedúry, príkazy alebo spúšťa aplikácie pre jedného alebo viacerých používateľov alebo klientskych zariadení. Ak sa používajú racky, blade serveri alebo iné podobné vybavenie, každé oddeliteľné fyzické zariadenie (napríklad blade server alebo zariadenie namontované v racku), ktoré má požadované komponenty sa považuje za samostatný server. Virtuálny server je buď virtuálny počítač vytvorený rozdelením zdrojov dostupných pre fyzický server, alebo fyzický server bez oddielov. Držiteľ Licencie musí získať oprávnenia na riadený virtuálny server pre každý virtuálny server.

Pri licencovaní prostredníctvom MVS je rozsah spracovávaných EPS a FPM dynamický podľa potrieb zákazníka a nie fixný. Licenčné kľúče QRadar pri nákupe prostredníctvom licencovania cez MVS (tzv. ENTERPRISE) sú generované nasledovne:

- 40 EPS na server MVS
- 500 FPM na server MVS

Ak zákazník potrebuje viac, je možné požiadať o vygenerovanie vyššieho kľúča oprávnení.

Za MVS sa počíta:

1. Windows Active Directory Servers
2. Windows IIS and Exchange Servers
3. Antivirus, Anti-Malware Servers: from the centralized server
4. EDR: from the EDR itself
5. FIM/FAM/DLP: only if installed on a server
6. Windows General Purpose Servers
7. UNIX and Linux Servers
8. Database Servers
9. VPN Servers
10. Proxy Servers, Reverse Proxy
11. DNS, DHCP Servers
12. IDS, IPS, WAF
13. DAM
14. O365
15. Web and Mail Servers
16. AS/400
17. Cloud Servers/Services
18. AIX
19. zOS
20. Print/File Servers
21. RADIUS/LDAP
22. Application Server
23. IBM AIX Servers
24. Privileged identity/Identity management Servers
25. Two-factor authentication servers
26. Public key and certificate management

Za MVS sa nepočíta:

1. Firewalls
2. Network routers
3. Network switches
4. Other Network devices
5. Workstations on Network
6. ESX - Virtualization Server (reason: we count the servers on top)
7. Point of Sale devices
8. CASB
9. Terminal Server

Produkty obsiahnuté v IBM Security QRadar XDR Package

Data Explorer

Threat Intelligence Insights

Threat Intelligence Insights Advanced (TII Required)

Threat Investigator

Threat Investigator Advanced (TI Required)

QRadar SOAR

QRadar Breach Response QRadar SIEM (Event Analytics) QRadar NDR (QNI + Flow Analytics) Data Store (Included w/Event Analytics) Risk Manager

Podpísané elektronickým podpisom

AUTOCONT s.r.o., Mario Háronik, konateľ

Príloha č. 6

Zoznam subdodávateľov

P.č.	Označenie subdodávateľa (názov, sídlo, IČO)	Podiel plnenia zmluvy	Osoba/osoby oprávnené konať v mene subdodávateľa (meno priezvisko, bydlisko a dátum narodenia)
1.	AUTOCONT a.s. Hornopolská 3322/34, Moravská Ostrava 702 00 Ostrava IČO: 043 08 697	30 %	Ondřej Matušík Ing. Martin Rabík