040/01-018/2025

„Rámcová dohoda na nákup licencií Safetica a ESET PROTECT Elite vrátane SLA"

uzavretá podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „Obchodný zákonník"), § 40 a nasl. zákona č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (Autorský zákon) v znení neskorších predpisov (ďalej len „Autorský zákon") a v súlade so zákonom č. 343/2015 Z. z. o verejnom obstarávaní o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní") medzi zmluvnými stranami
(ďalej len „zmluva")

Článok I.
ZMLUVNÉ STRANY

Objednávateľ:	**Záchranná zdravotná služba Bratislava**
Sídlo:	Antolská 11, 850 07 Bratislava 57
Zastúpená:	Ing. Slavomír Gruška, MPH, riaditeľ ZZS Bratislava
IČO:	17 336 210
DIČ:	2020845827
Bankové spojenie:	Štátna pokladnica
IBAN:	SK85 8180 0000 0070 0028 7955
Kontaktná osoba:	
e-mail:	
Tel. č.:	

(ďalej len „**objednávateľ**")

a

Poskytovateľ:	**iServices s. r. o.**
Registrácia:	Obchodný register Mestského súdu Bratislava III, oddiel Sro, vložka č. 49450/B
Sídlo:	Strojnícka 2979/34, 821 05 Bratislava
Štatutárny orgán:	Ing. Pavol Šimák, konateľ
IČO:	43 872 930
IČ DPH:	SK2022500524
Bankové spojenie:	Tatra banka, a. s.
IBAN:	SK44 1100 0000 0026 2281 9087
Kontaktná osoba:	
e-mail:	
Tel. č.:	

(ďalej len „**poskytovateľ**")

(Objednávateľ a poskytovateľ sa ďalej v texte označujú spoločne ako „**zmluvné strany**" a ktorýkoľvek z nich jednotlivo aj ako „**zmluvná strana**".)

Článok II.
ÚVODNÉ USTANOVENIE

1. Podkladom pre uzatvorenie tejto zmluvy je úspešná ponuka Poskytovateľa, ktorú predložil v procese verejného obstarávania realizovaného podľa § 108 zákona č. 343/2015 Z.z. o verejnom obstarávaní na predmet zákazky pod názvom: „Nákup licencií Safetica a ESET Protect Elite vrátane SLA“, špecifikácia podľa Prílohy č. 1 tejto zmluvy.

Článok III.
PREDMET ZMLUVY

Poskytovateľ sa zaväzuje za podmienok uvedených v tejto zmluve dodať objednávateľovi nevýhradnú a časovo obmedzenú licenciu na používanie softvéru podľa špecifikácie predmetu zmluvy a poskytovať služby podpory a údržby. (ďalej aj ako „predmet zmluvy“).

1. Podrobný opis predmetu zmluvy je uvedený v Prílohe č. 1 tejto zmluvy – Špecifikácia predmetu zmluvy.
2. Poskytovateľ týmto vyhlasuje, že je oprávnený udeliť objednávateľovi sublicenciu k programu na základe osobitnej zmluvy o distribúcii softvéru so spoločnosťou, ktorá disponuje majetkovými právami k programu ako autorskému dielu, najmä právom udeliť poskytovateľovi ako tretej osobe súhlas na použitie programu ako autorského diela v rozsahu udelenej licencie (tzn. oprávnenie udeliť právo ďalej poskytovať sublicenciu k programu).
3. Objednávateľ sa zaväzuje predmet tejto zmluvy uvedený v tomto článku od poskytovateľa prevziať a zaplatiť poskytovateľovi dohodnutú cenu za dodanie predmetu zmluvy spôsobom a za podmienok dohodnutých v tejto zmluve.

Článok IV.
MIESTO PLNENIA

1. Miestom plnenia predmetu zmluvy je Záchranná zdravotná služba Bratislava, Úsek IT, Antolská 11, 850 07 Bratislava 57, ak sa zmluvné strany nedohodnú inak.

Článok V.
TERMÍN A SPÔSOB PLNENIA

1. K licenciám nástroja SAFETICA PRO a ESET PROTECT Elite, uvedeným v Článku III. tejto zmluvy, poskytne poskytovateľ plnú súčinnosť administrátorom objednávateľa tak, aby bolo možné softvér plne využívať po nadobudnutí účinnosti tejto zmluvy a zároveň sa zaväzuje, že po dobu platnosti a účinnosti tejto zmluvy objednávateľovi sprístupní update tohto nástroja DPL a XDR prostredníctvom internetu.
2. Predmet zmluvy sa poskytuje na dobu platnosti a účinnosti tejto zmluvy na základe prílohy č.1 – Špecifikácia predmetu zmluvy.
3. Poskytovateľ dodá predmet zmluvy do 14 dní od nadobudnutia účinnosti tejto zmluvy.

4. Poskytovateľ dodá predmet zmluvy formou implementácie v prostredí objednávateľa. Licenčné kľúče doručí na e-mailovú adresu:

Článok VI.
CENA A PLATOBNÉ PODMIENKY

1. Zmluvné strany sa dohodli na cene za poskytovanie predmetu zmluvy v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky Ministerstva financií Slovenskej republiky č. 87/1996 Z. z. ktorou sa vykonáva zákon Národnej rady Slovenskej republiky č. 18/1996 Z. z. o cenách v znení neskorších predpisov.
2. Cena za riadne a včasné dodanie predmetu zmluvy podľa Článku. III. ods. 1 a 2 tejto zmluvy je uvedená v Prílohe č. 2 - Cenník
3. Predmet zákazky bude financovaný z rozpočtu verejného obstarávateľa formou bezhotovostného platobného styku
4. Objednávateľ neposkytuje preddavky ani zálohové platby.
5. Objednávateľ sa zaväzuje zaplatiť dohodnutú cenu po dodaní predmetu zmluvy na základe faktúr vystavených poskytovateľom po dodaní licencií. Lehota splatnosti faktúr je tridsať (30) dní od jej doručenia objednávateľovi. Prílohou faktúr bude dodací list potvrdený objednávateľom, preukazujúci dodanie predmetu zmluvy a objednávka.
6. Predávajúci vystavené faktúry zašle Kupujúcemu elektronickou poštou na e-mailovú adresu: Kupujúci podpisom tejto Zmluvy udeľuje Predávajúcemu súhlas k zasielaniu faktúr v elektronickej forme v súlade s ustanovením § 71 ods. 1 písm. b) zákona č. 222/2004 Z. z. o dani z pridanej hodnoty (ďalej len „zákon o DPH"). V predmete e-mailu, ktorým bude elektronická faktúra zasielaná, musí byť (za účelom základnej identifikácie) uvedené slovo: „faktúra", „invoice", „dobropis", „ťarchopis"; popri tomto označení môžu byť v predmete e-mailu uvedené aj ďalšie znaky, slúžiace k bližšej identifikácii (čísla alebo písmená). Elektronická faktúra musí byť vystavená len vo formátoch súborov PDF, TIF, JPEG, BMP a nesmie byť zaheslovaná, zamknutá na tlačenie, ani komprimovaná. Predávajúci je povinný zabezpečiť vierohodnosť pôvodu a neporušenosť obsahu faktúry, vyhotovenej v elektronickej forme, v súlade s podmienkami zákona o DPH. Podpis faktúry kvalifikovaným elektronickým podpisom sa nevyžaduje.
7. Faktúra musí obsahovať všetky náležitosti elektronického daňového dokladu podľa zákona o DPH a zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov. Prílohou faktúry musí byť objednávka a odsúhlasené dodacie listy.
8. V prípade, že faktúra nebude obsahovať všetky príslušné náležitosti, objednávateľ faktúru poskytovateľovi vráti na doplnenie a lehota splatnosti začne plynúť až dňom doručenia opravenej faktúry objednávateľovi, ktorá má všetky náležitosti vyžadované právnymi predpismi. Za správne vyhotovenie faktúry zodpovedá v plnom rozsahu poskytovateľ.
9. Za uhradenie faktúry sa považuje deň, v ktorom bude fakturovaná suma odpísaná z účtu objednávateľa v prospech účtu poskytovateľa. V prípade, že splatnosť faktúry pripadne

na deň pracovného voľna alebo pracovného pokoja, bude sa za deň splatnosti považovať najbližší nasledujúci pracovný deň.

10. K fakturovanej čiastke bude účtovaná DPH v zmysle platných právnych predpisov v čase fakturácie. Za správne vyčíslenie výšky DPH v súlade s platnými právnymi predpismi zodpovedá poskytovateľ v plnom rozsahu.

11. Predávajúci sa zaväzuje, že pohľadávku voči Kupujúcemu, ktorá mu, ako veriteľovi, vznikne z tohto zmluvného vzťahu, nepostúpi podľa § 524 a nasl. zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej len „OZ") tretej osobe bez predchádzajúceho písomného súhlasu Kupujúceho, ako dlžníka. Postúpenie pohľadávky Predávajúcim bez predchádzajúceho písomného súhlasu Kupujúceho je neplatné podľa § 39 OZ. Súhlas Kupujúceho je platný len za podmienky, že bol na takýto úkon udelený predchádzajúci písomný súhlas jeho zriaďovateľa (Ministerstvo zdravotníctva Slovenskej republiky).

12. V prípade, ak sa preukáže po uzatvorení tejto Zmluvy, že na relevantnom trhu existuje cena (ďalej aj „nižšia cena") za rovnaký alebo porovnateľný Tovar, ako je uvedený v tejto Zmluve a Predávajúci aj reálne za takúto nižšiu cenu Tovar už dodal alebo stále dodáva, ktorá je nižšia o viac ako 5% ako cena Predávajúceho podľa tejto Zmluvy, zaväzuje sa Predávajúci Kupujúcemu pre takýto Tovar poskytnúť po preukázaní tejto skutočnosti dodatočnú zľavu vo výške rozdielu medzi ním poskytovanou cenou podľa Zmluvy a nižšou cenou.

Článok VII.
ZMLUVNÁ POKUTA A ÚROK Z OMEŠKANIA

1. Ak je poskytovateľ v omeškaní s plnením predmetu zmluvy podľa Článku V. ods. 3. tejto zmluvy, má objednávateľ právo uplatniť si voči nemu zmluvnú pokutu vo výške 0,05 % z ceny nedodaného predmetu zmluvy za každý aj začatý deň omeškania.

2. Ak je objednávateľ v omeškaní s úhradou faktúry po termíne splatnosti, má poskytovateľ právo uplatniť úrok z omeškania za každý aj začatý deň omeškania z dlžnej sumy vo výške určenej Nariadením vlády Slovenskej republiky č. 87/1995 Z. z., ktorým sa vykonávajú niektoré ustanovenia Občianskeho zákonníka v znení neskorších predpisov.

3. Rozhodnutie požadovať zaplatenie zmluvnej pokuty/úroku z omeškania oznámi oprávnená strana doručením penalizačnej faktúry druhej zmluvnej strane.

4. V prípade, že poskytovateľ nedodrží garancie dostupnosti špecialistov, v pracovnom čase od 08:00 – 16:00 s nedodržaním reakcie do 4 hodín od nahlásenia incidentu v zmysle Článku. VIII. ods. 4 tejto zmluvy, objednávateľ má právo uplatniť si jednorazovú zmluvnú pokutu vo výške 150 EUR za každý incident.

5. Uplatnením zmluvnej pokuty nie je dotknutý nárok na náhradu skutočne vzniknutej škody spôsobenej porušením zmluvných povinností.

Článok VIII.
OSOBITNÉ USTANOVENIA

1. Poskytovateľ sa zaväzuje poskytnúť okamžitú súčinnosť pri riešení závažných závad programu brániacim ich riadnemu užívaniu po ich nahlásení. Bežné vady softvéru poskytovateľ vyrieši do 24 hodín od ich zreplikovania. Za vyriešenie vady sa považuje aj poskytnutie návodu ako používať softvér tak, aby takáto vada nemala vplyv na funkciu softvéru. Poskytovateľ je oprávnený požadovať a objednávateľ je povinný poskytnúť pri replikácii závady potrebnú súčinnosť. Lehota na odstránenie závady sa predlžuje o dobu omeškania objednávateľa s poskytnutím súčinnosti.
2. Objednávateľ je povinný oznámiť vady bez zbytočného odkladu po ich zistení.
3. Poskytovateľ sa zaväzuje, že predmet zmluvy bude spĺňať minimálne požiadavky v zmysle Prílohy č. 1 k tejto zmluve.
4. Poskytovateľ sa zaväzuje garantovať dostupnosť špecialistov podľa prílohy č. 1 Špecifikácia predmetu zmluvy.
5. Zmluvné strany sa zaväzujú:
   a) zachovávať mlčanlivosť o všetkých skutočnostiach obchodného tajomstva, o ktorých sa dozvedia v súvislosti s plnením predmetu tejto zmluvy,
   b) neposkytovať žiadne informácie alebo dokumenty prípadne ich kópie tretím osobám,
   c) v zmysle Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a ustanovenia zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov zachovať mlčanlivosť o všetkých osobných údajoch, s ktorými prídu do styku v súvislosti s plnením tejto zmluvy. Povinnosť zachovať mlčanlivosť trvá aj po zániku zmluvného vzťahu, ktorý je predmetom tejto zmluvy.
6. Objednávateľ sa zaväzuje, že neprevedie, čo i len čiastočne licenciu alebo právo na používanie predmetu zmluvy (sublicencia) na tretiu stranu bez predchádzajúceho písomného súhlasu poskytovateľa.
7. Objednávateľ sa zaväzuje, že bude dodržiavať všetky zákonné predpisy a opatrenia, aby nedošlo k takému rozširovaniu licencií, ktoré by mohlo poškodiť' výkon majetkových práv poskytovateľa alebo jeho partnerských spoločností.
8. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto zmluvy.
9. Objednávateľ sa zaväzuje, že bude s poskytovateľom bez zbytočného odkladu rokovať o všetkých otázkach, ktoré by mohli negatívne ovplyvniť dodanie predmetu zmluvy podľa tejto zmluvy a že mu bude oznamovať všetky okolnosti, ktoré by mohli ohroziť dohodnutý termín pre dodanie predmetu zmluvy v zmysle tejto zmluvy.
10. Poskytovateľ sa zaväzuje najneskôr ku dňu podpisu zmluvy predložiť objednávateľovi kontaktné údaje osoby/osôb zodpovednej za riadne plnenie predmetu zmluvy v rozsahu:

meno, priezvisko, telefónne číslo a e-mail a zároveň predloží aj telefónne číslo a e-mailovú adresu na hlásenie servisných požiadaviek objednávateľom.

11. Poskytovateľ nie je oprávnený navýšiť cenu o žiadne položky mimo zmluvnej ceny (doprava, náhradné diely a pod.).
12. Poskytovateľ najneskôr ku dňu podpisu zmluvy preukáže, že disponuje vlastným systémom na nahlasovanie porúch v režime 24x7 a to minimálne telefonicky, e-mailom s centrálnou adresou monitorovanou počas poskytovania podpory, prípadne možnosťou integrácie na centrálny dispečing objednávateľa.
13. Poskytovateľ sa zaväzuje v primeranej miere vykonať aj práce súvisiace s migráciou, implementáciou, optimalizáciou systémov a zaškolenia personálu určeného Objednávateľom v zmysle Prílohy č. 1.

Článok IX.
TRVANIE A ZÁNIK ZMLUVY

1. Táto zmluva sa uzatvára na dobu 12 mesiacov odo dňa nadobudnutia jej účinnosti. Zmluva nadobúda platnosť dňom jej podpisu oprávnenými zástupcami zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v zmysle ustanovenia § 47a Občianskeho zákonníka v znení neskorších predpisov a ustanovenia § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov v Centrálnom registri zmlúv, vedenom Úradom vlády Slovenskej republiky na webovom sídle www.crz.gov.sk. Ak sa do troch mesiacov od uzavretia zmluvy zmluva nezverejní, platí, že k uzavretiu zmluvy nedošlo.
2. Táto Zmluva je povinne zverejňovanou zmluvou v zmysle § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov a obidve Zmluvné strany súhlasia s jej zverejnením v Centrálnom registri zmlúv.
3. Zmluvné strany sa dohodli, že zmluva zaniká:
   a) písomnou dohodou obidvoch zmluvných strán k dohodnutému termínu,
   b) odstúpením od zmluvy zo strany objednávateľa alebo poskytovateľa z dôvodov dohodnutých v tomto článku zmluvy,
   c) uplynutím doby, na ktorú je táto zmluva uzatvorená,
   d) písomnou výpoveďou ktorejkoľvek zmluvnej strany bez udania dôvodu s 3-mesačnou výpovednou lehotou. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane,
4. V prípade podstatného porušenia zmluvy je odstupujúca zmluvná strana oprávnená od zmluvy odstúpiť, ak to písomne oznámi druhej zmluvnej strane bez zbytočného odkladu potom, čo sa o tomto porušení dozvedela.
5. Za podstatné porušenie zmluvy sa považuje najmä:

a) ak je poskytovateľ v omeškaní s dodaním predmetu zmluvy dohodnutým podľa tejto zmluvy o viac ako 10 kalendárnych dní,

b) ak objednávateľ neuhradí riadne vystavenú a preukázateľne doručenú faktúru ani do 30 kalendárnych dní po uplynutí jej splatnosti.

5. V prípade odstúpenia od zmluvy – oznámenie o odstúpení od tejto zmluvy musí byť podpísané štatutárnym zástupcom odstupujúcej zmluvnej strany a nadobúda účinnosť dňom jeho preukázateľného doručenia druhej zmluvnej strane.

6. Zmluvné strany sa dohodli, že ukončením zmluvy sa táto zmluva neruší od začiatku, ale zaniká ku dňu účinnosti odstúpenia od tejto zmluvy.

7. Odstúpenie od zmluvy sa nedotýka nároku na náhradu škody a nároku na zaplatenie zmluvnej pokuty, ktoré vznikli pred odstúpením od zmluvy z dôvodu porušenia zmluvnej povinnosti.

Článok X.
ZÁVEREČNÉ USTANOVENIA

1. Právne vzťahy touto zmluvou výslovne neupravené sa riadia ustanoveniami Obchodného zákonníka, Autorského zákona a ostatnými platnými právnymi predpismi Slovenskej republiky.

2. Zmluvné strany berú na vedomie, že táto zmluva podlieha zverejneniu podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov a s jej zverejnením vyjadrujú súhlas. Zverejnenie tejto zmluvy v Centrálnom registri zmlúv sa nepovažuje za porušenie ani za ohrozenie obchodného tajomstva.

3. V prípade akéhokoľvek nedorozumenia, sporu alebo sporného nároku sa obe zmluvné strany zaväzujú riešiť ich prednostne cestou vzájomnej dohody. Pokiaľ nedôjde k vyriešeniu sporov cestou vzájomnej dohody, je každá zo zmluvných strán oprávnená riešiť spor súdnou cestou na príslušnom všeobecnom súde Slovenskej republiky.

4. Zmluva môže byť doplnená alebo zmenená len písomnými dodatkami k zmluve, podpísanými obidvoma zmluvnými stranami v súlade s ustanovením § 18 zákona o verejnom obstarávaní.

5. Pokiaľ akékoľvek z ustanovení tejto zmluvy je alebo sa stane neplatným, protiprávnym alebo neúčinným, zaväzujú sa zmluvné strany toto ustanovenie bezodkladne nahradiť ustanovením novým, ktorého zmysel sa bude čo možno najviac blížiť zmyslu a hospodárskemu účelu nahradzovaného ustanovenia tak, že by bolo možné predpokladať, že by ho strany boli použili, keby vedeli o neplatnosti, protiprávnosti alebo neúčinnosti ustanovenia nahradzovaného. Neplatnosť, protiprávnosť alebo neúčinnosť ustanovenia zmluvy sa nebude dotýkať ostatných ustanovení tejto zmluvy, pričom táto zmluva sa bude vykladať tak, ako keby v nej nebolo neplatné, protiprávne alebo neúčinné ustanovenia nikdy obsiahnuté.

6. Zmluva sa vyhotovuje v 2 (dvoch) rovnopisoch, každý s platnosťou originálu, pričom objednávateľ obdrží 1 (jeden) rovnopis a poskytovateľ obdrží 1 (jeden) rovnopis.
7. Zmluvné strany prehlasujú, že si zmluvu prečítali, obsahu, ktorý považujú za určitý a zrozumiteľný, porozumeli a tento vyjadruje ich slobodnú a vážnu vôľu zbavenú akýchkoľvek omylov, na dôkaz čoho pripájajú svoje podpisy.
8. Neoddeliteľnou súčasťou tejto zmluvy je:
   8.1 Príloha č. 1 – Špecifikácia predmetu zmluvy
   8.2 Príloha č. 2 – Cenník
   8.3 Príloha č. 3 – Dohoda o utajení
   8.4 Príloha č. 4 – Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Príloha č. 1

Špecifikácia predmetu zmluvy

Predmetom zákazky je povýšenie kybernetickej bezpečnosti organizácie obstaraním licencií Safetica (180 ks) a ESET PROTECT Elite (220 ks), inštalácia serverového riešenia ESET XDR s aktívnym monitoringom XDR platformy na licenčné obdobie 12 mesiacov s konzultačnou a aplikačnou podporou (SLA) pre obe riešenia

Technická špecifikácia- Safetica

Popis existujúceho riešenia obstarávateľa:
nasadená a funkčná Safetica vo verzii 10.5.76 na VM Windows Server 2019
Požiadavky na dodávateľa:
1. Dodanie licencií Safetica PRO s aktualizáciou na 12 mesiacov pre 180 zariadení (PC, notebooky)
2. Podpora SAFETICA, SLA - dostupnosť helpdeskového portálu a garantovaná dostupnosť špecialistu na IT bezpečnosť

Pod bodom 2. „Podpora SAFETICA, SLA" sa rozumie:
- poskytovanie služieb rozšírenej servisnej podpory formou SLA s monitoringom v trvaní 12 mesiacov vzdialenou off-site formou
- SLA 8x5 v prac. dňoch v čase 08:00-16:00 hod., potvrdenie prijatia požiadavky na servisný zásah do 60 min., nástup na riešenie najneskôr do 6 hod. od nahlásenia incidentu.
- aktualizácia servera a inštalácia klientov na najnovšiu verziu; pomoc pri inštalácii nových klientov a riešenie problémov pri inštalácii / aktualizácii klientov

Požadované proaktívne činnosti pre oblasť podpory:
- komplexná starostlivosť a prevádzka DLP riešenia vrátane podpory a pravidelných aktualizácií riešenia (aktualizácia aplikačného vybavenia v zmysle odporúčaní výrobcom)
- proaktívne riešenie vznikajúcich problémov
- proaktívny monitoring vybraných parametrov aplikačného riešenia DLP určených s prevádzkou a dostupnosťou DLP služieb
- aktívny monitoring DLP pravidiel s príslušným notifikačným mechanizmom
- pravidelné vyhodnocovanie DLP incidentov na mesačnej báze s príslušným návrhom opatrení a reštrikcií
- kontrola logov
- dodanie informácií o známych bezpečnostných chybách a aplikovanie náprav
- evidencia DLP incidentov na on-line portáli/HelpDesku.
- tvorba natívnych reportov a ad-hoc vyhodnocovanie incidentov s príslušným návrhom na zmenu nastavenia Safetica riešenia

Ďalšia oblasť podpory Safetica:

- riadené používateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia
- ochrana proti zmene nastavenia na koncovej stanici
- možnosť pracovať s historickými dátami
- automatické generovanie emailových varovaní v prípade incidentov, možnosť zmeniť citlivosť a špecifikáciu incidentu.
- automatické generovanie emailových reportov s možnosťou úprav obsahu (množstvo informácií, množina uzlov, frekvencie odosielanie, príjemcovia).

Správa zariadení:

- reštrikcie pre USB mass storage zariadenia, pripojenie mobilných telefónov, pamäťové karty, Bluetooth prenosy súborov, optické disky či FireWire.
- možnosť vynútenia režimu Iba na čítanie u pripojených zariadení.
- zaznamenávanie všetkých pripojených zariadení vrátane monitorov, myší a klávesníc.
- schopnosť blokovať iba prenosy dát cez Bluetooth, ale povoliť pripojenie a voľné použitie ďalších Bluetooth zariadení (napr. slúchadiel).
- klasifikované dáta je možné chrániť pred skopírovaním na chytré telefóny pripojené cez Multimedia Transfer Protocol, tieto zariadenia je možné ale inak neobmedzene používať s necitlivými dátami.

Správa aplikácií:

- monitoring využívania aplikácií naprieč organizáciou a možnosť riadiť, ktoré aplikácie je možné a ktoré nemožno spúšťať.
- monitoring navštevovania webových stránok naprieč organizáciou a možnosť riadiť, ktoré webové stránky je možné a ktoré nemožno navštevovať.

Ochrana údajov:

- definícia kategórií citlivých dát dovoľuje obmedzenie pohybu a práce s týmito dátami; určuje, ktoré médiá môžu byť použité pre prenos, ktoré siete môžu byť použité pre prenos dát, na ktoré emailové adresy môžu byť dáta odoslané, ktoré aplikácie môžu s dátami pracovať.
- možnosť úplnej blokácie používateľských akcií, používateľského schválenia operácie, informatívne notifikácie používateľa a zaznamenanie používateľských akcií
- možnosť aplikácie politík pre konkrétne aplikácie – definícia zdroja a cieľa (prístup na externé zariadenie, sieť, tlač, virtuálnu tlač) a správa používateľských operácií (použitie schránky, snímanie obrazovky).
- možnosť správy nepovolených cloudových úložísk.
- funkcionalita „shadow copy" umožňujúca administrátorovi prezeranie súborov, ktoré boli súčasťou bezpečnostných incidentov. Funkcia musí sprístupniť súbory, ktoré používateľ odoslal, aj tie, ktoré DLP riešenie zablokovalo.
- možnosť nastavenia počtu výskytov citlivých údajov. Dynamické reštrikcie nad súbormi a aplikáciami, pokiaľ je detegovaný citlivý obsah.

- blokácia odoslania dát s citlivým obsahom mimo koncovú stanicu – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenie, IM komunikačné nástroje, synchronizácia s cloudovými aplikáciami.

Ochrana citlivých údajov:

- detekcia citlivých dát v dokumentoch
- možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov.
- možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov.
- možnosť importu vlastných slovníkov a kľúčových slov.
- možnosť nastavenia počtu výskytov citlivých údajov.
- možnosť klasifikácie citlivých dát podľa kontextových podmienok, napr. pôvod alebo umiestnenie dát.
- možnosť klasifikácie kompatibilných typov súborov pomocou perzistentných súborových metadát.
- blokovanie odoslania dát s citlivým obsahom mimo koncovej stanice – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenia, IM komunikačné nástroje, synchronizácia s cloudovými aplikáciami.
- detekcia dát obsahujúcich citlivý obsah, uložených na koncovej stanici alebo na zdieľanom sieťovom disku. Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.
- reštrikcie pre USB zariadenia, pamäťové karty, Bluetooth zariadení, optické disky či FireWire.
- možnosť vynútenia režimu iba na čítanie u pripojených zariadení.
- centrálna správa aplikácií, prehľad jednotlivých verzií aplikácii.

Pravidelné zasielanie - dátový audit:

- detailné informácie o aplikáciách, ako čas spustenia a ich aktívnom využití. Aplikácie sú rozdelené do kategórií pre prehľadnú správu.
- detailné informácie o weboch, ako ich aktívne využitie, informáciách o URL, použitom protokole, hlavičky webu, a to bez ohľadu na použitý prehliadač. Weby sú rozdelené do kategórií pre prehľadnú správu.
- detailné informácie o práci so súbormi, ako prehľad používateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové atď.).
- lokálne súborové operácie – kopírovanie, presúvanie, sťahovanie z webu, FTP, mazanie, vytvorenie, otvorenie, a to vrátanie zdrojovej a cieľovej identifikácie: cesta, typ zariadenia, jedinečný identifikátor,
- -logovanie tlačových úloh a možnosť exportu reportov do XLS, PDF.

Zaznamenávanie komunikácie:

- podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania.
- podpora desktopových emailových klientov MS Outlook, Mozilla Thunderbird a pod. - riešenie je schopné zaznamenávať emaily nezávisle od použitej aplikácie.
- podpora zaznamenávania súborov odoslaných cez web mailových klientov.

- podpora zaznamenávania súborov odoslaných cez IM komunikačné nástroje

Sieťová aktivita:

- monitorovanie množstva odoslaných/stiahnutých dát.
- Pod „garantovaná dostupnosť špecialistu na IT bezpečnosť" sa rozumie:
- Dodávateľ sa zaväzuje garantovať dostupnosť špecialistov na riešenie v pracovnom čase 08:00 – 16:00 hod. s reakčnosťou do 6 hodín:
- min. 1 špecialista Tier 1 určených na riešenie prevádzkových incidentov, diagnostiky pre DLP riešenie
- min. 1 špecialista Tier 2 určených na riešenie incidentov v oblasti DLP problematiky, definovanie DLP pravidiel v zmysle požiadaviek, aktívny reporting odporúčaní, poskytovanie konzultácií

Objednávateľ považuje za nevyhnutné na riadne poskytnutie plnenia predmetu zmluvy a dodávateľ je povinný pred uzatvorením zmluvy preukázať objednávateľovi splnenie požiadaviek:

- disponovanie certifikátmi ISO/IEC 27001 (systém manažérstva informačnej bezpečnosti), ISO 22301 (systém manažérstva kontinuity podnikania), ISO 10006 (systém manažérstva kvality v projektoch) a ISO/IEC 27017(systém manažérstva informačnej bezpečnosti na zabezpečenie cloudových služieb)
- disponovanie certifikátom partner Safetica (pokiaľ nie je dodávateľom priamo výrobca, alebo Distribútor)
- disponovanie min. 1 špecialistom s certifikáciou CySA+
- disponovanie min. 1 certifikovaným projektovým manažérom s platným certifikátom projektového riadenia PRINCE2 alebo IPMA a súčasne s platným certifikátom ITIL Foundation alebo ekvivalent

Osobitné požiadavky na plnenie:

Dodávateľ do 3 dní od nadobudnutia účinnosti Zmluvy preukáže, že disponuje vlastným systémom na nahlasovanie porúch v režime 24x7 a to telefonicky, alebo e-mailom s centrálnou adresou monitorovanou počas poskytovania podpory.

Dodávateľ sa zaväzuje do 3 pracovných dní od účinnosti zmluvy predložiť objednávateľovi kontaktné údaje osoby/osôb zodpovednej za riadne plnenie predmetu zmluvy v rozsahu: meno, priezvisko, telefónne číslo a e-mail a zároveň predloží aj telefónne číslo a e-mailovú adresu na hlásenie servisných požiadaviek objednávateľom.

Zmluvná cena „Podpora Safetica" bude rovnomerne rozdelená medzi 12 mesiacov a fakturovaná v pravidelných mesačných platbách počas doby trvania Zmluvy na základe faktúr zasielaných Dodávateľom.

Špecifikácia ESET Protect Elite

Popis existujúceho riešenia:

OS CentOS 7, Eset Protect Virtual Appliance, on premis

Požiadavky na dodávateľa:

1. Dodanie licencií ESET PROTECT Elite na obdobie 12 mesiacov v počte 220 ks.
Bližšia špecifikácia bodu 1:
- upgrade existujúcich licencií na nový typ licencií ESET PROTECT Elite v počte 220 ks., poskytovanie aktualizácií (update), nových verzií (upgrade) a podpory dodaných licencií na obdobie 12 mesiacov

2. Inštalácia cloudového serverového riešenia ESET XDR, migračné, implementačné, konfiguračné a optimalizačné práce ESET PROTECT pre 220 Endpointov
Popis hlavných činností bodu 2:
- inštalácia cloudového serverového riešenia, inštalácia centrálnej konzoly ESET, nastavenie 2 faktorovej autentifikácie
- analýza aktuálneho stavu on-premis riešenia, migrácia existujúceho riešenia do Cloudu:
- migrácia existujúcich pracovných staníc (počítače, notebooky, servery)
- kontrola existujúcich pravidiel a politík, ich migrácia a optimalizácia
- implementačné a optimalizačné práce pre prostredie ESET Protect a ESET Inspect
- implementácia a konfigurácia sandbox funkcionality na endpointoch
- hodnotiaca správa výsledkov migrácie do cloudu

3. Technické školenie administrátorov na nástroj ESET Inspect v rozsahu min. 1 deň (1 MD)
Bližšia špecifikácia bodu 3:
- on-line školenie rozdelené minimálne do dvoch súvislých a súvisiacich častí
- poskytnutie / vytvorenie manuálov a postupov na nasadenie a správu politik ochrany, manuál pre prípady podozrenia na kompromitáciu endpointu, ako aj potvrdenej kompromitácie endpointu a pod.

4. Technické školenie administrátorov na nástroj ESET Protect v rozsahu min. 1 deň (1MD)
Bližšia špecifikácia bodu 4:
- on-line školenie rozdelené minimálne do dvoch súvislých a súvisiacich častí
- poskytnutie / vytvorenie manuálov napr. na reakciu na všeobecné bezpečnostné udalosti, manuál na správu aktualizácií a kontrolu kompatibility softvéru

5. Poskytovanie služieb rozšírenej servisnej podpory pre XDR platformu s aktívnym monitoringom počas 12 mesiacov, ktoré sú zamerané na detekciu a reakciu na hrozby na koncových zariadeniach
Bližšia špecifikácia služieb bodu 5:
- komplexná starostlivosť o prevádzku XDR platformy

- podpora poskytovaná 8x5, v prac. dňoch v čase 8:00-16:00 h, potvrdenie prijatia požiadavky na servisný zásah do min. 60 minút, nástup na riešenie najneskôr do 4 h od nahlásenia incidentu
- nástup na riešenie najneskôr do 4 hodín od nahlásenia incidentu, ktorý sa vzťahuje na ESET PROTECT a ESET Inspect prostredia
- proaktívne činnosti pre oblasť podpory: proaktívne riešenie vznikajúcich problémov. V rámci tejto aktivity sú požadované minimálne nasledovné činnosti pre riešenie:
- proaktívny monitoring vybraných parametrov a dostupnosť všetkých služieb aplikačného riešenia EDR/XDR serverového systému.
- aktívny monitoring EDR/XDR pravidiel s príslušným notifikačným mechanizmom
- nastavovanie pravidelných reportov podľa požiadaviek objednávateľa v celkom rozsahu 2 reporty za mesiac

Security podpora pre ESET Inspect endpointové produkty:

- Malware: chýbajúca detekcia
- Malware: problém s liečením
- Malware: infekcia ransomvérom
- Zachytenie False positive
- Vyšetrenie podozrivého správania
- Vyšetrenie malware incidentu a odozva na vzniknutý malware incident:
- Základná analýza zaslaného súboru
- Detailná analýza zaslaného súboru
- Analýza a vyšetrenie odovzdaných súvisiacich dát
- Asistencia pri odozve/protiopatreniach na malware incident

Podpora pre riešenie bezpečnostných incidentov v prostredí XDR:

- Podpora s vytváraním XDR pravidiel
- Podpora s vytváraním XDR výnimiek
- ESET Inspect operatívna optimalizácia prostredia
- ESET Inspect služba Threat Hunting (poskytovaná na požiadanie zo strany objednávateľa)
- pravidelné vyhodnocovanie XDR incidentov na mesačnej báze s príslušným návrhom opatrení a reštrikcií
- v mesačnej správe je zahrnuté aj vyhotovenie úplného ročného analytického reportu, ktorý bude sumarizovať všetky zistenia a odporúčania za ročné sledované obdobie
- kontrola logov
- napojenie na SIEM a zadefinovanie parametrov (poskytovaná na požiadanie zo strany objednávateľa)
- aktualizácia aplikačného vybavenia v zmysle odporúčaní výrobcom
- dodanie informácií o známych bezpečnostných chybách a aplikovanie náprav
- evidencia XDR incidentov a úprav na on-line portáli/HelpDesku
- v prípade potreby zabezpečenie možnosti porovnávať bezpečnostné výstupy z riešení ESET a Safetica pri podozrení na bezpečnostný incident s cieľom zvýšiť efektívnosť analýzy a reakcie na hrozby

Ďalšia minimálna technická špecifikácia na softvérové riešenie pre prostredie ESET - XDR:
Antivírusové riešenie pre koncové body a servery:

- podporované klientske platformy OS - Windows, Linux, MacOS všetko v slovenskom alebo českom jazyku, natívna podpora architektúr pre platformy Windows a MacOS: x86, x64, ARM64
- antimalware, antiransomware, antispyware a anti-phishing na aktívnu ochranu pred všetkými typmi hrozieb
- personálny firewall pre zabránenie neautorizovanému prístupu k zariadeniu so schopnosťou automatického prebratia pravidiel z brány Windows Firewall
- modul pre ochranu operačného systému a elimináciu aktivít ohrozujúcich bezpečnosť zariadenia s možnosťou definovať pravidlá pre systémové registre, procesy, aplikácie a súbory
- ochrana pred neautorizovanou zmenou nastavenia
- aktívna aj pasívna heuristická analýza pre detekciu doposiaľ neznámych hrozieb
- systém na blokáciu exploitov zneužívajúcich zero-day zraniteľností, ktorý pokrýva najpoužívanejšie vektory útoku: min. sieťové protokoly, Flash Player, Java, Microsoft Office, webové prehliadače, emailových klientov, PDF čítačky
- systém na detekciu malwaru už na sieťovej úrovni poskytujúci ochranu aj pred zneužitím zraniteľností na sieťovej vrstve
- kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).
- Anti-phishing so schopnosťou detekcie homoglyph útokov
- kontrola RAM pamäte pre lepšiu detekciu malwaru využívajúcu silnú obfuskáciu a šifrovanie
- cloud kontrola súborov pre urýchlenie skenovania fungujúce na základe reputácie súborov.
- kontrola súborov v priebehu sťahovania pre zníženie celkového času kontroly
- kontrola súborov pri zapisovaní na disku a extrahovaní archivačných súborov
- detekcia s využitím strojového učenia
- funkcia ochrany proti zapojeniu do botnetu pracujúcej s detekciou sieťových signatúr
- ochrana pred sieťovými útokmi skenujúca sieťovú komunikáciu a blokujúca pokusy o zneužitie zraniteľností na sieťovej úrovni
- kontrola s podporou cloudu pre odosielanie a online vyhodnocovanie neznámych a potenciálne škodlivých aplikácií.
- lokálny sandbox
- modul behaviorálnej analýzy pre detekciu správania nových typov ransomwaru
- reputačný systém na získavanie informácií o bezpečnosti súborov a URL adries
- cloudový systém na detekciu nového malwaru ešte nezaneseného v aktualizáciách signatúr
- technológia na detekciu rootkitov obvykle maskujúcich sa za súčasti operačného systému
- skener firmvéru BIOSu a UEFI
- skenovanie súborov v cloude OneDrive
- funkcionalita pre MS Windows v min. rozsahu: Antimalware, Antispyware, Personal Firewall, Personal IPS, Application Control, Device control, Security Memory, kontrola integrity systémových komponentov

- funkcionalita pre MacOS v min. rozsahu: Personal Firewall, Device control, autoupgrade
- možnosť aplikovania bezpečnostných politík aj v off-line režime na základe definovaných podmienok
- ochrana proti pokročilým hrozbám (APT) a 0-day zraniteľnostiam
- podpora automatického vytvárania dump súborov na stanici na základe nálezov
- okamžité blokovanie/mazanie napadnutých súborov na stanici (s možnosťou stiahnutia administrátorom na ďalšiu analýzu)
- duálny aktualizačný profil pre možnosť sťahovania aktualizácií v lokálnej sieti a zároveň vzdialených serverov pri nedostupnosti lokálneho
- možnosť definovať webové stránky, ktoré sa spustia v chránenom režime prehliadača, pre bezpečnú prácu s kritickými systémami alebo internetovým bankovníctvom
- aktívna ochrana pred útokmi hrubou silou na protokol SMB a RDP
- možnosť zablokovania konkrétnej IP adresy po sérii neúspešných pokusov o prihlásenie pre protokoly SMB a RDP s možnosťou výnimiek vo vnútorných sieťach
- automatické aktualizácie bezpečnostného softvéru s možnosťou odloženia reštartu stanice.
- "Zmrazenie" na požadovanej verzii – produkt je možné nakonfigurovať tak, aby nedochádzalo k automatickému povyšovaniu majoritných a minoritných verzií najmä na staniciach, kde sa vyžaduje vysoká stabilita

Integrovaná cloudová analýza neznámych vzoriek:

- funkcia cloudového sandboxu je integrovaná do produktu pre koncové a serverové zariadenia, tzn. Cloudový sandbox nemá vlastného agenta, nevyžaduje inštaláciu ďalšie komponenty či už v rámci produktu alebo implementácie HW prvku do siete
- sandbox umožňujúci spustenie vzoriek malwaru pre Windows, Linux
- možnosť využitia na koncových bodoch a serveroch pre aktívnu detekciu škodlivých súborov
- analýza neznámych vzoriek v rade jednotiek minút
- optimalizácia pre znemožnenie obídenia anti-sandbox mechanizmy
- schopnosť analýzy rootkitov a ransomvéru
- schopnosť detekcie a zastavenie zneužitia alebo pokusu o zneužitie zero day zraniteľnosti
- riešenie pracuje s behaviorálnou analýzou
- kompletný výsledok o zanalyzovanom súbore vrátane informácie o nájdenom i nenájdenom škodlivom správaní daného súboru
- manuálne odoslanie vzorky do sandboxu
- možnosť proaktívnej ochrany, kedy je potenciálna hrozba blokovaná, pokiaľ nie je známy výsledok analýzy zo sandboxu
- neobmedzené množstvo odosielaných súborov
- všetka komunikácia prebieha šifrovaným kanálom
- okamžité odstránenie súboru po dokončení analýzy v cloudovom sandboxe
- možnosť voľby, aké kategórie súborov do cloudového sandboxu budú odchádzať (spustiteľné súbory, archívy, skripty, pravdepodobný spam, dokumenty atp.)
- veľkosť odoslaných súborov do cloudového sandboxu môže dosahovať až 64MB

- výsledky analyzovaných súborov sú dostupné a automatizovane distribuované všetkým serverom a staniciam naprieč organizáciou, tak aby nedochádzalo k duplicitnému testovaniu

Šifrovanie celých diskov:

- podpora platforiem Windows a MacOS
- správa cez jednotný centrálny manažment
- unikátna technológia pre platformu Windows (nevyužíva sa BitLocker)
- podpora Pre-Boot autentizácia
- podpora TMP modulu
- podpora Opal samošifrovacích diskov
- možnosť definovať: počet chybne zadaných pokusov, zložitosť a dĺžku autentizačného hesla
- možnosť obmedziť platnosť autentizačného hesla
- podpora okamžitého zmazania šifrovacieho kľúča a následné uzamknutie počítača
- recovery z centrálnej konzoly

XDR riešenie:

- prevádzka centrálneho servera v Cloude
- webová konzola pre správu a vyhodnotenie
- možnosť prevádzky s databázami: Microsoft SQL, MySQL
- možnosť prevádzky v offline prostredí
- autonómne správanie so schopnosťou vyhodnotiť podozrivú/ škodlivú aktivitu a zareagovať na ňu aj bez aktuálne dostupného riadiaceho servera alebo internetového pripojenia
- logovanie činností administrátora
- podpora EDR pre systémy Windows, Windows server, MacOS a Linux
- možnosť autentizácie do manažmentu EDR pomocou 2FA
- možnosť riadenia manažmentu EDR prostredníctvom API, a to ako pre: Prijímanie informácií z EDR serverov aj Zasielanie príkazov na EDR servery
- integrovaný nástroj v EDR riešení pre vzdialené zasielanie príkazov priamo z konzoly
- možnosť izolácie zariadenia od siete
- možnosť tvorby vlastných IoC
- možnosť škálovania množstva historických dát vyhodnotených v EDR min. 3 mesiace pre raw-data a min. 3 roky pre detegované incidenty.
- „učiaci režim“ pre automatizované vytváranie výnimiek k detekčným pravidlám
- indikátory útoku pracujúce s behaviorálnou detekciou
- indikátory útoku pracujúce s reputáciou
- riešenie umožňuje analýzu vektorov útoku
- schopnosť detekcie: min. škodlivých spustiteľných súborov: skriptov, exploitov, rootkitov, sieťových útokov, zneužitie WMI nástrojov, bezsúborového malwaru, škodlivých systémových ovládačov - kernel modulov, pokusov o dump prihlasovacích údajov užívateľa
- schopnosť detegovať laterálny pohyb útočníka

- analýza procesov, všetkých spustiteľných súborov a DLL knižníc.
- náhľad na spustené skripty použité pri detegovanej udalosti
- možnosť zabezpečeného vzdialeného spojenia cez servery výrobcu do konzoly EDR
- schopnosť automatizovaného response úkonu pre jednotlivé detekčné pravidlá v podobe: izolácia stanice, blokácia hash súboru, blokácia a vyčistenie siete od konkrétneho súboru, ukončení procesu, reštart počítača, vypnutie počítača
- možnosť automatického vyriešenia incidentu administrátorom
- -prioritizácia vzniknutých incidentov
- -možnosť stiahnutia spustiteľných súborov zo staníc pre bližšiu analýzu vo formáte archívu opatreným heslom
- integrácia a zobrazenie detekcií vykonaných antimalware produktom
- riešenie je schopné generovať tzv. forest/full execution tree model
- vyhľadávanie pomocou novo vytvorených IoC nad historickými dátami
- previazanie s technikami popísanými v knowledge base MITRE ATT&CK
- integrovaný vyhľadávač VirusTotal s možnosť rozšírenia o vlastné vyhľadávače
- oprava po útoku ransomvérom - obnova zašifrovaných súborov (Ransomware Remediation)

Management konzola pre správu všetkých riešení v rámci ponúkaného balíka v rozsahu:

- možnosť prevádzkovať jednotnú management konzolu na správu týchto riešení v cloudovom nasadení
- webová konzola
- možnosť inštalácie na Windows aj Linux
- možnosť prebudenia klientov pomocou Wake On Lan
- vzdialené vypnutie, reštart počítača alebo odhlásenie všetkých užívateľov
- možnosť konfigurácie virtual appliance cez užívateľsky prívetivé webové rozhranie Webmin
- nezávislí manažment agent pre platformy Windows, Linux a MacOS
- management agent pre architektúry na platformy Windows a MacOS: x86, x64, ARM64
- nezávislý agent (pracuje aj offline) vzdialenej správy pre zabezpečenie komunikácie a ovládania operačného systému verejného obstarávateľa
- Off-line uplatňovanie politík a spúšťanie úloh pri výskyte definovanej udalosti (napríklad: odpojenie od siete pri nájdení škodlivého kódu).
- administrácia v slovenčine
- široké možnosti konfigurácie oprávnení administrátorov (napríklad možnosť správy iba časti infraštruktúry, ktoré konkrétnemu administrátorovi podlieha)
- zabezpečenie prístupu administrátorov do vzdialenej správy pomocou 2FA
- podpora štítkov a tagovania pre jednoduchšiu správu a vyhľadávanie
- správa karantény s možnosťou vzdialeného vymazania / obnovenia / obnovenia a vylúčenia objektu z detekcie
- vzdialené získanie zachyteného škodlivého súboru
- detekcia nespravovaných (rizikových) počítačov komunikujúcich na sieti.
- podpora pre inštalácie a odinštalácie aplikácií 3.strán, vyčítanie informácií o verziách softvéru 3. strán

- možnosť vyčítať informácie o hardvéri na spravovaných zariadeniach: CPU, RAM, diskové jednotky, grafické karty a pod., možnosť vyčítať sériové číslo zariadenia, možnosť vyčítať voľné miesto na disku
- detekcia aktívneho šifrovania BitLocker na spravovanej stanici
- zobrazenie časovej informácie o poslednom boote stanice
- odoslanie správy na počítač, ktoré sa následne zobrazí užívateľovi na obrazovke
- vzdialené odinštalovanie antivírusového riešenia 3. strany
- vzdialené spustenie akéhokoľvek príkazu na cieľovej stanici pomocou Príkazového riadka
- dynamické skupiny pre možnosť definovania podmienok, za ktorých dôjde k automatickému zaradeniu klienta do požadovanej skupiny a automatickému uplatneniu klientskej úlohy
- automatické zasielanie upozornení pri dosiahnutí definovaného počtu alebo percent ovplyvnených klientov
- podpora SNMP Trap, Syslogu a qRadar SIEM
- podpora formátov pre Syslog správy: CEF, JSON, LEEF
- podpora inštalácie skriptom - *.bat, *.sh, *.ini (GPO, SSCM…)
- rýchle pripojenie na klienta pomocou RDP z konzoly pre vzdialenú správu
- reportovanie stavu klientov chránených inými bezpečnostnými programami
- schopnosť zaslať reporty a upozornenia na e-mail
- konzola podporuje multidoménové a multitenantné prostredie
- podpora VDI prostredia: Citrix, VMware, SCCM, a pod.
- podpora klonovania počítačov pomocou golden image
- podpora inštanciách klonov
- podpora obnovy identity počítača pre VDI prostredie na základe FQDN
- možnosť definovať viacero menných vzorov klonovaných počítačov pre VDI prostredie
- pridanie zariadenia do vzdialenej správy pomocou: synchronizácia s Active Directory, ručné pridanie pomocou podľa IP adresy alebo názvu zariadenia, pomocou sieťového skenu nechránených zariadení v sieti, Import cez csv súbor

Správa zraniteľností a patchov aplikácií tretích strán:

- automatizované kontroly podľa vlastného harmonogramu na základe prispôsobiteľných pravidiel
- filtrovanie, zoskupovanie a triedenie zraniteľností podľa ich závažnosti
- možnosť manuálnych alebo automatických opráv
- prispôsobiteľné politiky záplat
- podpora multitenant v komplexných sieťových prostrediach - prehľad zraniteľností v konkrétnych častiach organizácie
- databáza zraniteľností, CVSS 2.0 a CVSS 3.1

Osobitné požiadavky na plnenie:

Objednávateľ považuje za nevyhnutné na riadne poskytnutie plnenia predmetu zmluvy a dodávateľ je povinný pred uzatvorením zmluvy preukázať objednávateľovi:

- doklad preukazujúci, že dodávateľ je oficiálnym partnerom spoločnosti ESET minimálne v kategórii „Zlatý partner". Úroveň partnerstva musí byť verifikovateľná z verejných zdrojov (napr. webstránka výrobcu), alebo takéto partnerstvo je preukázané dokladom
- doklad preukazujúci, že dodávateľ disponuje vlastným systémom na nahlasovanie vád v režime 24x7 a to telefonicky alebo e-mailom s centrálnou adresou monitorovanou počas poskytovania podpory.
- dodávateľ preukáže, že disponuje certifikáciou:
- ISO/IEC 27001 - Systém manažérstva informačnej bezpečnosti ISO 22301 - Systém manažérstva kontinuity podnikania
- ISO/IEC 27017 - Systém manažérstva informačnej bezpečnosti pre zabezpečenie cloudových služieb ISO 10006 - Systém manažérstva kvality v projektoch
- dodávateľ preukáže dokladom (napr. certifikát osoby), že disponuje min. 1 špecialistom (ESET Optimization Specialist), ktorý bude v rámci plnenia predmetu zákazky k dispozícii na riešenie bezpečnostných, prevádzkových incidentov a diagnostiky pre EDR/XDR platformu.
- dodávateľ preukáže dokladom (napr. certifikát osoby), že disponuje minimálne 1 certifikovanou osobou/špecialistom v nasledovných oblastiach:
- 11
- základné technické znalosti ESET riešení, základná technická certifikácia ESMC, pokročilá technická certifikácia ESMC, produktová technická certifikácia na ESET Endpoint Encryption
- projektového manažéra s platným certifikátom projektového riadenia PRINCE2 Practitioner a súčasne s platným certifikátom ITIL Foundation alebo ekvivalent
- s certifikáciou CySA+
- Manažér kybernetickej bezpečnosti

Príloha č. 2

Cenník

P.č	Položka	Merná jednotka	Množstvo	Jednotková cena v EUR bez DPH	Cena celkom v EUR bez DPH
1	*Safetica PRO s aktualizáciou na 12 mesiacov*	ks	180	55,25	9 945,00
2	*SLA – dostupnosť helpdesk portálu 24x7 pre nahlásenie požiadavky na podporu.* *Garantovaná dostupnosť špecialitu na IT bezpečnosť v čase 08:00 – 17:00 hod. s reakčným časom do 6 hodín*	mesiac	12	405,00	4 860,00
3	*Dodanie licencií ESET PROTECT Elite na obdobie 12 mesiacov*	ks	220	36,00	7 920,00
4	*Inštalácia cloudového serverového riešenia ESET XDR; migračné, implementačné a optimalizačné práce ESET PROTECT pre 220 Endpointov*	-	1	5 040,00	5 040,00
5	*Technické školenie administrátorov na nástroj ESET Inspect v rozsahu min. 1 deň (1 MD)*	MD	1	450,00	450,00
6	*Technické školenie administrátorov na nástroj ESET Protect v rozsahu min. 1 deň (1MD)*	MD	1	450,00	450,00
7	*Poskytovanie služieb rozšírenej servisnej on-site podpory pre XDR platformu s aktívnym monitoringom*	mesiac	12	627,75	7 533,00
		Cena celkom			36 198,00

DOHODA O UTAJENÍ

podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník

---

medzi:

Záchranná zdravotná služba Bratislava
Antolská 11, 850 07 Bratislava 57
IČO: 17 336 210
Zastúpená: Mgr. Slavomír Gruška, MBA, riaditeľ

a

iServices s. r. o.
Strojnícka 2979/34, 821 05 Bratislava
IČO: 43 872 930
Zastúpená: Ing. Pavol Šimák, konateľ
zapísaná v: Obchodnom registri Mestského súdu Bratislava III, Oddiel: Sro, Vložka č.: 49450/B

1. Predmet dohody

1.1. Predmetom dohody je synalagmatický záväzok strán dohody o dodržiavaní povinnosti mlčanlivosti o dôverných informáciách medzi stranami dohody.

2. Účel dohody

2.1. Účelom tejto dohody je zabezpečiť mlčanlivosť zmluvných strán o všetkých dôverných informáciách poskytnutých zmluvnými stranami navzájom, vymedzených v článku 3. dohody,

v súvislosti s realizáciou zákazky „Nákup licencií Safetica a ESET PROTECT Elite vrátane SLA“ (ďalej ako „projekt“).

3. Dôverné informácie

3.1. Dôvernými informáciami, ktoré sú predmetom ochrany v zmysle dohody, sú akékoľvek poskytnuté informácie, ktoré nie sú inak verejne prístupné a s ktorými sa má nakladať vzhľadom na okolnosti známe druhej strane pri poskytnutí informácií, ako s dôvernými (ďalej len „dôverné informácie“).

3.2. Dôverné informácie sú aj akékoľvek informácie, špecifikácie, plány, náčrty, modely, vzorky, dáta, počítačové programy, softwér, alebo dokumentácia v akejkoľvek podobe či už zachytené hmotne alebo ústne, ktoré boli poskytnuté jednou zmluvnou stranou (ďalej len „poskytovateľ“) druhej zmluvnej strane (ďalej len „prijímateľ“).

3.3. Dôvernými informáciami nie sú informácie,

3.3.1. ktoré sú, alebo sa stanú verejne dostupnými inak, ako porušením povinností zmluvnej strany podľa tejto dohody alebo

3.3.2. ktoré boli pred uzavretím tejto dohody známe bez akejkoľvek povinnosti dodržiavať ich dôvernosť, alebo

3.3.3. ktoré boli získané od tretej osoby, ktorá je oprávnená šíriť tieto informácie.

4. Povinnosti zmluvných strán

4.1. Každá zo zmluvných strán sa týmto zaväzuje, že:

4.1.1. bude zachovávať mlčanlivosť o všetkých dôverných informáciách poskytovateľa v každom štádiu realizácie projektu bez ohľadu na skutočnosť, že napokon dôjde k jeho naplneniu a uskutočneniu

4.1.2. bude chrániť dôverné informácie poskytnuté poskytovateľom minimálne v rozsahu, ako dôverné informácie vlastné, a za tým účelom bude prijímať potrebné opatrenia na ich ochranu,

4.1.3. bude vyhotovovať kópie dokumentov obsahujúcich dôverné informácie len s písomným súhlasom poskytovateľa,

4.1.4. poskytne dôverné informácie tretej osobe len s písomným súhlasom poskytovateľa,

4.1.5. poskytne dôverné informácie svojim zamestnancom, riaditeľom, poverencom a zástupcom, pokiaľ takéto osoby boli náležite poučené o záväzku zachovávať mlčanlivosť o dôverných informáciách podľa tejto dohody,

4.1.6. bude používať dôverné informácie len v konkrétnej a priamej súvislosti s projektom,

4.1.7. vráti poskytovateľovi na jeho požiadanie všetky dokumenty obsahujúce dôverné informácie a to rovnako originály nosičov dôverných informácii ako aj kópie týchto nosičov v akejkoľvek technickej podobe.

4.1.8. oznámi poskytovateľovi neoprávnené použitie, poskytnutie alebo zverejnenie dôverných informácií, a to ihneď po tomto zistení a bude spolupracovať pri znovuobnovení ochrany dôverných informácií a zabránení ich ďalšiemu neoprávnenému použitiu.

4.1.9. bude niesť zodpovednosť za škodu spôsobenú tým, že porušil niektorú z povinností podľa bodu 4.1.1. až 4.1.8. Rovnako zmluvná strana zodpovedá v prípade, že svojim zavineným konaním umožnila, čo aj nepriamo, porušenie ochrany dôverných informácií tretej osobe.

5. Zmluvné pokuty

5.1. Porušením povinností niektorého účastníka Dohody, týkajúcich sa ochrany dôverných informácií a skutočností tvoriacich obchodné tajomstvo podľa tejto Dohody, vzniká druhej strane právo požadovať zaplatenie zmluvnej pokuty.

5.2. Výška zmluvnej pokuty je dohodnutá na sumu 10.000,- € (slovom desaťtisíc eur).

5.3. Zmluvná pokuta, na ktorú vznikne poškodenej strane podľa tejto Dohody nárok, je druhá strana povinná uhradiť do pätnástich (15) kalendárnych dní odo dňa doručenia výzvy na jej úhradu.

5.4. Každý z účastníkov tejto Dohody zodpovedá za škodu, ktorá vznikne druhej strane porušením povinností podľa tejto Dohody. Poškodená strana je oprávnená domáhať sa náhrady vzniknutej škody samostatne, popri zmluvnej pokute.

5.5. Účastníci Dohody sú si vedomí, že na ochranu svojich oprávnených záujmov môžu použiť prostriedky právnej ochrany proti nekalej súťaži podľa § 53 Obchodného zákonník a § 373 a nasl. Obchodného zákonníka, na účely uplatnenia náhrady škody.

6. Zodpovednosť za škodu

6.1. Prijímateľ zodpovedá za škodu, ktorá vznikne Poskytovateľovi porušením povinností podľa tejto dohody.

6.2. Prijímateľ si je vedomý, že na ochranu svojich oprávnených záujmov môže Poskytovateľ použiť prostriedky právnej ochrany proti nekalej súťaži podľa § 53 Obchodného zákonníka a § 373 a nasl. Obchodného zákonníka, na účely uplatnenia náhrady škody.

7. Nakladanie s dôvernými informáciami a ich nosičmi

7.1. Dôverné informácie podľa tejto zmluvy, ktoré sa týkajú druhej zmluvnej strany, a s ktorými bola zmluvná strana oboznámená alebo ktoré získala, nesmie zmluvná strana využívať v rozpore so záujmami druhej zmluvnej strany, a to ani pre svoj prospech a ani pre prospech tretích osôb, a ani po skončení trvania tejto zmluvy.

7.2. Každá zo zmluvných strán je oprávnená poskytnúť dôverné informácie:

7.2.1. súdu alebo inému orgánu verejnej moci v súvislosti so súdnym alebo iným úradným konaním vzniknutým a vedeným v súvislosti s obchodnými vzťahmi medzi zmluvnými stranami, alebo

7.2.2. ak je okrem prípadov podľa bodu 7.2.1 ich poskytnutie požadované príkazom súdu alebo iného orgánu verejnej moci, či už v konaní alebo mimo neho, alebo

7.2.3. v prípade, že povinnosť zmluvnej strany takto konať je stanovená zákonom, či iným všeobecne záväzným predpisom, alebo

7.2.4. vládnej, bankovej, daňovej alebo inej inštitúcii či osobe, ktorá je oprávnená ich vyžadovať podľa platných a účinných právnych predpisov Slovenskej republiky.

7.3. V týchto prípadoch podľa bodu 7.2 je prijímateľ povinný o tejto skutočnosti bezodkladne informovať poskytovateľa.

7.4. Dôverné informácie sú a vždy budú vlastníctvom poskytovateľa. Poskytnutím dôverných informácií poskytovateľ nedáva právo, licenciu alebo iné oprávnenie prijímateľovi.

7.5. Pri manipulácii s dôvernými informáciami poskytovateľa je zmluvná strana povinná počínať si s primeranou starostlivosťou nevyhnutnou na zabezpečenie ochrany dôverných informácií v súlade s účelom tejto dohody.

8. Záverečné ustanovenia

8.1. Právne vzťahy zmluvných strán touto dohodou neupravené sa riadia ustanoveniami Obchodného zákonníka a právnym poriadkom SR.

8.2. Dohoda je vyhotovená v dvoch rovnopisoch, po jednom pre každú zmluvnú stranu.

8.3. Zmluvné strany sa dohodli, že táto dohoda nadobúda platnosť podpisom zmluvných strán, jej účinnosť nie je časovo obmedzená a ani viazaná na uzavretie zmluvy na projekt.

8.4. Zmluvné strany prehlasujú, že zmluvu uzavreli slobodne, vážne, jej obsahu porozumeli a súhlasia s jej znením, čo potvrdzujú podpismi tejto dohody.

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník a § 19 ods. 2 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti (ďalej len „**Zmluva**") medzi :

1/Dodávateľ:

Obchodné meno:	**iServices s. r. o.**
Sídlo:	Strojnícka 2979/34, Bratislava - mestská časť Ružinov 821 05
V zastúpení:	Ing. Pavol Šimák, konateľ
IČO:	43 872 930
DIČ:	2022500524
IČ DPH:	SK2022500524
IBAN:	SK44 1100 0000 0026 2281 9087
Zapísaný:	v Obchodnom registri Mestského súdu Bratislava III Vl. č.: 49450/B

(ďalej len „Dodávateľ")

a

2/ Prevádzkovateľ základnej služby:

Obchodné meno:	Záchranná zdravotná služba Bratislava
Sídlo:	Antolská 11, 850 07 Bratislava 57
V zastúpení:	Ing. Slavomír Gruška, MPH, riaditeľ
IČO:	17 336 210
DIČ:	2020845827
IČ DPH:	nie je platiteľom DPH
IBAN:	SK85 8180 0000 0070 0028 7955
Zriadený:	zriaďovacou listinou MZ SR č. 3724/1991 – A/XXI-3 s účinnosťou od 01. 01. 1992 v znení neskorších zmien

(ďalej len „Odberateľ")
Odberateľ a Dodávateľ spolu ďalej ako „Zmluvné strany" a každý samostatne ako „Zmluvná strana".

Článok 1
Úvodné ustanovenia

1. Zmluvné strany uzatvárajú túto Zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na Rámcovú dohodu na nákup licencií Safetica a ESET PROTECT Elite vrátane SLA uzatvorenú medzi Zmluvnými stranami dňa ....., č. .... (ďalej len „Osobitná zmluva").

2. Odberateľ je prevádzkovateľom základnej služby v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších zmien (ďalej ako „zákon o kybernetickej bezpečnosti").

3. Odberateľ vyhlasuje, že si je vedomý svojich zmluvných a zákonných povinností, prijal všetky

potrebné bezpečnostné opatrenia, ktoré bude počas platnosti tejto Zmluvy udržiavať, má zodpovedajúce materiálne, technické a personálne vybavenie a zaväzuje sa poskytnúť Dodávateľovi potrebnú súčinnosť a informácie, aby mohol efektívne napĺňať účel a predmet tejto Zmluvy.

4. Dodávateľ prehlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tejto Zmluvy.

5. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve a príslušných právnych predpisov tak, aby bol naplnený účel tejto Zmluvy.

6. Dodávateľ sa zaväzuje vykonávať všetky činnosti definované v tejto Zmluve v súlade s platnými právnymi predpismi. Zmluvne strany zhodne prehlasujú, že nič v tejto Zmluve nezbavuje Zmluvné strany zodpovednosti za plnenie vlastných povinností, ktoré im vyplývajú z právnych predpisov vydaných v súlade so zákonom o kybernetickej bezpečnosti a zákona o kybernetickej bezpečnosti.

7. Pojmy uvedené v tejto Zmluve sa zhodujú s pojmami definovanými zákonom o kybernetickej bezpečnosti a v prípade ich slovnej nezhody sa použijú ustanovenia zákona o kybernetickej bezpečnosti, ktoré sú im významom najbližšie.

8. Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia Osobitnou zmluvou alebo inými právnymi predpismi vydanými v súlade so zákonom o kybernetickej bezpečnosti a zákonom o kybernetickej bezpečnosti.

9. V prípade vzniku nákladov na strane Dodávateľa v súvislosti s plnením povinností podľa tejto Zmluvy ako aj zákona o kybernetickej bezpečnosti, tieto náklady znáša Dodávateľ.

10. Zmluva stanovuje základné úlohy a princípy spolupráce Zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Odberateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Odberateľa a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany Odberateľa (ďalej len „účel"), a to aj v spolupráci s Dodávateľom.

Článok 2
Predmet zmluvy

1. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Odberateľovi dodržiavanie bezpečnostných požiadaviek a opatrení, ktoré sú kladené na tretie strany v zmysle § 19 zákona o kybernetickej bezpečnosti a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška NBÚ").

2. Miestom plnenia tejto Zmluvy sú najmä pracovisko alebo sídlo Odberateľa, pracovisko alebo sídlo Dodávateľa, alebo pracoviská a sídla subdodávateľov v zmysle Osobitnej zmluvy. V prípade zmeny alebo doplnenia sídla alebo pracoviska zo strany Zmluvných strán, vykonajú tak Zmluvné strany oznamom zaslaným e-mailom na kontaktné osoby uvedené v Článku 9 tejto Zmluvy, najneskôr do 30 dní od vykonania tejto zmeny.

3. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu

nadobudnutia účinnosti tejto Zmluvy až do skončenia platnosti Osobitnej zmluvy, pokiaľ z právnych predpisov uvedených v tejto Zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti Osobitnej zmluvy.

Článok 3
Práva a povinnosti Dodávateľa

1. Odberateľ je povinný bezodkladne po uzavretí Zmluvy oboznámiť Dodávateľa s bezpečnostnou politikou informačných systémov upravenou v aktuálnych vnútorných predpisoch Odberateľa. Dodávateľ sa zaväzuje oboznámiť sa a dodržiavať bezpečnostnú politiku informačných systémov Odberateľa v časti, v ktorej je služba Dodávateľa pripojená k sieti základnej služby alebo informačného systému základnej služby (ďalej ako „bezpečnostná politika") a súčasne s ňou Dodávateľ vyjadruje svoj súhlas. O oboznámení sa s bezpečnostnou politikou a vyjadrení súhlasu s ňou si Zmluvné strany vydajú písomné potvrdenie.

2. Dodávateľ súhlasí s tým, že bezpečnostná politika Odberateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Odberateľa a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Odberateľa. Odberateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne písomne potvrdí, že sa so zmenami bezpečnostnej politiky oboznámil a súhlasí s nimi.

3. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Odberateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.

4. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Odberateľom pri zabezpečovaní požiadaviek kladených na Odberateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky NBÚ, a to zaslaním e-mailu na kontaktnú osobu Odberateľa uvedenú v tejto Zmluve.

5. Dodávateľ sa zaväzuje hlásiť všetky informácie, ktoré majú vplyv na túto Zmluvu zaslaním e-mailu na kontaktnú osobu Odberateľa uvedenú v tejto Zmluve.

6. V oblasti technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 9 vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Odberateľovi a ktoré toto poskytovanie služieb Odberateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

6.1. Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb.
6.2 Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb.
6.3 Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

7. Dodávateľ je ďalej povinný :

7.1 zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Odberateľa,
7.2 sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Odberateľa („incidenty"),

7.3 zasielať Odberateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak, a

7.4 spolupracovať s Odberateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Odberateľa,

7.5 po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má Dodávateľ počas trvania Osobitnej zmluvy s Odberateľom prístup.

7.6 okrem už uvedeného prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. d), e) f), g) h), j), k), m) a p) zákona o kybernetickej bezpečnosti v rozsahu podľa§ 8, 10, 12, 14 a 15 vyhlášky NBÚ, a v rozsahu špecifikovanom v bezpečnostnej politike Odberateľa.

8. Dodávateľ môže zapojiť do poskytovania služieb na základe Osobitnej zmluvy ďalšieho dodávateľa, ak mu to vyplýva z ustanovení Osobitnej zmluvy.

Článok 4
Reaktivita pri riešení incidentov

1. Dodávateľ je povinný bezodkladne nahlásiť Odberateľovi každý incident a informovať ho o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti, o ktorých sa dozvie, a to spôsobom určeným touto Zmluvou. Dodávateľ následne určí závažnosť incidentu.

2. Ak v čase hlásenia incidentu stále trvajú prejavy incidentu, Dodávateľ odošle Odberateľovi neúplné hlásenie aj s odkazom, že ide o neúplné hlásenie. Dodávateľ neúplné hlásenie bez zbytočného odkladu doplní po obnove riadnej a úplnej prevádzky siete a všetkých informačných systémov Odberateľa.

3. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou incidentov (ďalej len „Reakčné opatrenia"), a to ako na výzvu Odberateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie.

4. Dodávateľ pri reakciách na incidenty spolupracuje s Odberateľom, NBÚ a inými príslušnými orgánmi a za týmto účelom poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami a ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.

5. Dodávateľ bez zbytočného odkladu oznámi Odberateľovi implementáciu Reakčných opatrení. Ak o to Odberateľ požiada, po úspešnej implementácii Reakčného opatrenia Dodávateľ predloží návrh bezpečnostných opatrení a postupov, ktoré zabezpečia, že nedôjde k opakovaniu, pokračovaniu či šíreniu incidentu (ďalej len „Ochranné opatrenie"). Ak Dodávateľ Ochranné opatrenie nenavrhne alebo ak Ochranné opatrenie neprinesie požadovaný efekt, Dodávateľ vypracuje a predloží iné Ochranné opatrenie. S povolením Odberateľa Dodávateľ implementuje Ochranné opatrenie a spíše záznam o efektívnosti jeho implementácie.

Článok 5
Zodpovednosť

Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto Zmluvy môže spôsobiť Odberateľovi škody, pričom v prípade škôd ako dôsledkov incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Dodávateľa podľa tejto Zmluvy neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá Odberateľovi v plnom rozsahu (zodpovednosť za výsledok).

Článok 6
Audit kybernetickej bezpečnosti

1. Odberateľ je oprávnený vykonať u Dodávateľa audit kybernetickej bezpečnosti (ďalej len „audit") zameraný na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy a to prostredníctvom svojich zamestnancov alebo poverenej osoby. Výdavky Odberateľa spojené s vykonaním auditu znáša Odberateľ.

2. Dodávateľ sa zaväzuje, že Odberateľovi umožní kedykoľvek vykonať audit, ktorý okrem bodu 1 tohto článku bude tiež zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.

3. Akékoľvek nedostatky alebo pochybenia zistené auditom je Dodávateľ povinný odstrániť bezodkladne, avšak najneskôr do 60 (slovom: šesťdesiatich) kalendárnych dní.

4. Dodávateľ je povinný pri audite spolupracovať s Odberateľom a v prípade potreby umožniť zamestnancom alebo poverenej osobe Odberateľa voľný vstup do svojich priestorov , zabezpečiť im dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.

5. Odberateľ je povinný oznámiť e-mailom na kontaktnú osobu Dodávateľa uvedenú v Zmluve, najmenej 10 (slovom: desať) pracovných dní vopred, že chce u Dodávateľa vykonať audit.

6. Odberateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Odberateľ a jeho zamestnanci pri vstupe do priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „BOZP") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO"), s ktorými boli oboznámení podľa štvrtej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Odberateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne informovať zamestnancov Odberateľa o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

Článok 7
Mlčanlivosť

1. Zmluvné strany sa zaväzujú zachovávať mlčanlivosť o podmienkach spolupráce podľa tejto Zmluvy, ako aj o všetkých skutočnostiach týkajúcich sa druhej Zmluvnej strany (najmä, nie však výlučne obchodnej povahy), ktoré im boli sprístupnené počas trvania tejto Zmluvy alebo ktoré sa im stali iným spôsobom známe. Uvedené sa týka najmä skutočností týkajúcich sa kybernetickej bezpečnosti a osobných údajov. Povinnosť mlčanlivosti trvá aj po skončení tejto Zmluvy alebo Osobitnej zmluvy bez časového obmedzenia.

2. Výnimky z povinností podľa tohto článku tejto Zmluvy upravujú najmä Zákon o kybernetickej bezpečnosti a iné príslušné právny predpisy.

3. Dodávateľ je povinný doručiť Odberateľovi zoznam pracovných rolí Dodávateľa, ktoré sa budú podieľať na plnení Osobitnej zmluvy a tejto Zmluvy a/alebo majú prístup k informáciám a údajom Odberateľa a ktorý sa jeho doručením Odberateľovi stane súčasťou tejto Zmluvy. Tieto osoby sú povinné zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti a Dodávateľ je povinný oznámiť Odberateľovi každú zmenu v personálnom obsadení.

Článok 8
Kontaktné osoby

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto Zmluvy s Odberateľom emailom na kontaktné údaje zmluvných strán, alebo iným vhodným spôsobom, pričom vo všetkých prípadoch musí byť prenos informácií uskutočnený za podmienok umožňujúcich chránený prenos informácií.

2. Odberateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti: [redacted]

3. Dodávateľ určuje nasledovnú kontaktnú osobu na úseku kybernetickej bezpečnosti pre komunikáciu s Odberateľom: [redacted]

4. Kontaktná osoba Dodávateľa plní úlohy pri zabezpečovaní reaktivity podľa čl. 4 tejto Zmluvy. Kontaktná osoba plní notifikačné povinnosti prostredníctvom na to povereného organizačného útvaru Dodávateľa.

5. Kontaktné osoby podľa odsekov 2 alebo 3 tohto článku môže príslušná Zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej Zmluvnej strane v písomnej forme. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia Zmluvy o doručovaní, pričom nie je potrebné uzatvoriť dodatok k Zmluve. V prípade, ak kontaktné osoby majú prístup k informáciám a údajom Odberateľa sú povinné zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

Článok 9
Záverečné ustanovenia

1. Táto zmluva sa uzatvára na dobu určitú, do ukončenia Osobitnej zmluvy.

2. Odberateľ je oprávnený od tejto Zmluvy odstúpiť v prípadoch, ak Dodávateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy, pričom odstúpenie je účinné dňom doručenia odstúpenia Dodávateľovi.

3. Odstúpenie od tejto Zmluvy sa musí urobiť písomne, inak sa na neho neprihliada. Povinnosť doručiť odstúpenie od tejto Zmluvy sa považuje za splnenú dňom prevzatia odstúpenia od tejto Zmluvy alebo dňom odmietnutia prevziať odstúpenie od tejto Zmluvy.

4. Ukončenie tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po ukončení tejto Zmluvy, a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy, ku ktorému dôjde do ukončenia tejto Zmluvy.

5. S ohľadom na § 8 ods. 2 písm. p) vyhlášky NBÚ, po ukončení tejto Zmluvy je Dodávateľ povinný

udeliť, poskytnúť, previesť alebo postúpiť na Odberateľa všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby Odberateľom, tento záväzok Dodávateľa ostáva v platnosti najmenej po dobu piatich rokov po ukončení tejto Zmluvy.

6. Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov týkajúcich sa tejto Zmluvy.

7. Táto Zmluva sa môže meniť alebo ukončiť iba dohodou Zmluvných strán v písomnej forme.

8. V prípade, že niektoré ustanovenia Zmluvy sú alebo sa z akéhokoľvek dôvodu stanú neplatné, neúčinné alebo nevynútiteľné, nemá to a ani nebude mať za následok neplatnosť, neúčinnosť alebo nevynútiteľnosť ostatných ustanovení Zmluvy. Zmluvné strany sú povinné v dobrej viere rokovať, aby bolo neplatné, neúčinné alebo nevynútiteľné ustanovenie písomne nahradené iným ustanovením, ktorého vecný obsah bude zhodný alebo čo najviac podobný ustanoveniu, ktoré je nahradzované, pričom účel a zmysel Zmluvy musí byť zachovaný.

9. Písomnosti si budú Zmluvné strany doručovať na adresu sídla uvedenú v tejto Zmluve. Zmenu sídla je Zmluvná strana povinná bezodkladne písomne oznámiť druhej Zmluvnej strane. Zmluvné strany sa dohodli, že v prípade vrátenia zásielky odosielateľovi z akéhokoľvek dôvodu platí, že písomnosť bola doručená adresátovi dňom vrátenia zásielky odosielateľovi, aj keď sa o tom adresát nedozvedel.

10. Táto Zmluva bola vyhotovená v dvoch rovnopisoch, jedno vyhotovenie pre Odberateľa, jedno pre Dodávateľa.

11. Zmluva nadobúda platnosť dňom podpisu oboma Zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv.

12. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.