

ZMLUVA o dodaní riešení na zabezpečenie opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti

uzavretá podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník
v znení neskorších predpisov (ďalej len „Obchodný zákonník“),
§ 65 a nasl. zákona č. 185/2015 Z. z. 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 „ZVO“)
medzi zmluvnými stranami
(ďalej len „zmluva“)

Článok I. ZMLUVNÉ STRANY

Objednávateľ:

Názov:	Slovenská poľnohospodárska univerzita v Nitre
Sídlo:	Trieda Andreja Hlinku 2, 949 76 Nitra, Slovenská republika
Štatutárny orgán:	doc. Ing. Klaudia Halászová, PhD., rektorka
IČO:	00397482
DIČ:	2021252827
IČ DPH:	SK2021252827
Bankové spojenie:	Štátna pokladnica
Kontaktná osoba:	Ing. Ľuboš Határ
e-mail:	lubos.hatar@uniag.sk
Tel. č.:	+421 37 641 4864

(ďalej len „objednávateľ“)

a

Dodávateľ:

Názov	iServices s.r.o.
Sídlo:	Strojnícka 2979/34, 821 05 Bratislava
Štatutárny orgán:	Ing. Pavol Šimák, konateľ
IČO:	43 872 930
IČ DPH:	SK2022500524
Zapísaný:	v OR Mestského súdu Bratislava III, oddiel Sro, vložka č. 49450/B
Bankové spojenie:	Tatra banka, a.s.
IBAN:	
Kontaktná osoba:	Ing. Pavol Šimák
e-mail:	
Tel. č.:	

(ďalej len „dodávateľ“)

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

Článok II. ÚVODNÉ USTANOVENIE

1. Táto zmluva je výsledkom zadávania nadlimitnej zákazky postupom verejnej súťaže podľa § 91 v spojení s §66 ods. 7 písm. b) zákona č. 343/2015 Z.z. o verejnom obstarávaní na predmet zákazky pod názvom: „**Zvýšenie úrovne informačnej a kybernetickej bezpečnosti na SPU v Nitre**“, ktorej úspešným uchádzačom sa stal dodávateľ.
2. Predmet plnenia bude financovaný z nenávratného finančného príspevku poskytnutého objednávateľovi Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „Poskytovateľ NFP“), pre projekt „Podpora v oblasti kybernetickej a

informačnej bezpečnosti na regionálnej úrovni - SPU NR“, kód projektu 401101FNJ2, na základe Zmluvy o poskytnutí nenávratného finančného príspevku č. NFP401101FMJ2 (ďalej len „Zmluva o NFP“).

Článok III. PREDMET ZMLUVY

1. Dodávateľ sa zaväzuje za podmienok uvedených v tejto zmluve dodať objednávateľovi plnenie špecifikované v Prílohe č. 1 (ďalej aj ako „Predmet plnenia“) za podmienok uvedených v tejto zmluve a záväzok objednávateľa zaplatiť dodávateľovi spôsobom a za podmienok dohodnutých v tejto zmluve cenu dohodnutú v tejto zmluve .
2. Podrobný opis Predmetu plnenia ako aj osobitné požiadavky na plnenie sú uvedené v Prílohe č. 1 tejto zmluvy – Špecifikácia predmetu plnenia.
3. Dodávateľ týmto vyhlasuje, že je oprávnený v prípade dodania licencie 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 dodávateľovi ako tretej osobe súhlas na použitie programu ako autorského diela v rozsahu udelenej licencie (tzn. oprávnenie udeliť právo ďalej poskytovať sublicenciu k programu).

Článok IV. MIESTO PLNENIA

1. Miestom plnenia predmetu zmluvy je miesto sídla objednávateľa v Nitre, Trieda A. Hlinku 2, ak sa zmluvné strany nedohodnú inak.

Článok V. TERMÍN A SPÔSOB PLNENIA

1. K licenciám dodaným podľa tejto zmluvy špecifikovaným v Prílohe č. 1 poskytne dodávateľ 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 EDR/XDR a nástroja na riadenie kapacít prostredníctvom internetu.
2. Predmet zmluvy sa dodáva na dobu platnosti a účinnosti tejto zmluvy na základe prílohy č.1 – Špecifikácia predmetu zmluvy.
3. Lehota plnenia pre každú položku tvoriacu predmet plnenia je uvedená v prílohe č. 1 zmluvy.
4. Dodávateľ dodá predmet plnenia formou uvedenou v Prílohe č. 1 . V prípade položiek vyžadujúcich dodanie licenčných kľúčov doručí tieto dodávateľ na e-mailovú adresu objednávateľa: lubos.hatar@uniag.sk .

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. Celková cena za celý predmet plnenia podľa ponuky dodávateľa predložená vo verejnom obstarávaní v rámci zákazky je:

Cena v € bez DPH	320 364,50
DPH:	73 683,83
Cena v € s DPH	394 048,33

3. Cenník jednotlivých položiek tvoriacich predmet plnenia sa nachádza v Prílohe č. 2 k tejto zmluve.
4. Objednávateľ neposkytuje preddavky ani zálohové platby.
5. Objednávateľ sa zaväzuje zaplatiť dohodnutú cenu po dodaní predmetu plnenia na základe faktúry vystavenej Dodávateľom. Lehota splatnosti faktúry je tridsať (30) dní od jej doručenia objednávatel'ovi. Prílohou faktúry bude dodací list potvrdený objednávatel'om, preukazujúci dodanie predmetu zmluvy.
6. V prípade časti plnenia UPGRADE ANTIVÍRUSOVÉHO SOFTVÉRU ESET A SLUŽBY ROZŠÍRENEJ PODPORY KYBERNETICKEJ BEZPEČNOSTI S AKTÍVNYM MONITORINGOM XDR PLATFORMY bude mesačne uhrádzané čiastka za „Poskytovanie služieb rozšírenej servisnej on-site podpory pre XDR platformu“ a to v 12 mesačných platbách v jednotkovej cene podľa prílohy č. 1a.
7. Platby sa budú uskutočňovať na základe faktúr zasielaných Dodávateľom prostredníctvom elektronického alebo poštového styku. Dodávateľ nie je oprávnený navýšiť cenu o žiadne položky mimo zmluvnej ceny (doprava, náhradné diely a pod.). Lehota splatnosti faktúry je tridsať (30) dní od jej doručenia objednávatel'ovi
8. Objednávateľ umožňuje predložiť aj zaručenú elektronickú faktúru, ktorú dodávateľ zašle na emailovú adresu lubos.hatar@uniag.sk. V prípade nevyužitia možnosti predložiť zaručenú elektronickú faktúru, dodávateľ zašle originál faktúry na adresu objednávatel'a:
9. Faktúra musí obsahovať všetky náležitosti daňového dokladu v zmysle platných právnych predpisov, najmä:
 - označenie objednávatel'a a obchodné meno dodávateľ'a vrátane sídla,
 - názov a číslo zmluvy,
 - číslo faktúry,
 - deň odoslania a deň splatnosti faktúry,
 - označenie peňažného ústavu a číslo účtu, na ktorý sa má platiť fakturovaná suma, konštantný a variabilný symbol,
 - rozpis fakturovaných čiastok,
 - pečiatka a podpis oprávnenej osoby dodávateľ'a.
10. V prípade, že faktúra nebude obsahovať všetky príslušné náležitosti, objednávateľ faktúru dodávateľovi vráti na doplnenie a lehota splatnosti začne plynúť až dňom doručenia opravenej faktúry objednávatel'ovi, ktorá má všetky náležitosti vyžadované právnymi predpismi. Za správne vyhotovenie faktúry zodpovedá v plnom rozsahu dodávateľ.
11. Za uhradenie faktúry sa považuje deň, v ktorom bude fakturovaná suma odpísaná z účtu objednávatel'a v prospech účtu dodávateľ'a. V prípade, že splatnosť faktúry pripadne na deň pracovného voľna alebo pracovného pokoja, bude sa za deň splatnosti považovať najbližší nasledujúci pracovný deň.
12. 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 dodávateľ v plnom rozsahu.

Článok VII.

ZMLUVNÁ POKUTA A ÚROK Z OMEŠKANIA

1. Ak je dodávateľ 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 dodávateľ právo uplatniť úrok z omeškania za každý aj začatý deň omeškania z dlžnej sumy vo výške určenej Nariadením vlády Slovenskej republiky č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení neskorších predpisov.

3. Rozhodnutie požadovať zaplatenie zmluvnej pokuty/úroku z omeškania oznámi oprávnená strana dorúčením penalizačnej faktúry druhej zmluvnej strane.
4. V prípade, že je dodávateľ podľa prílohy č. 1 pri niektorej z položiek tvoriacich predmet plnenia povinný dodržať garanciu dostupnosti špecialistov, v pracovnom čase od 08:00 – 16:00 s nedodržaním reakcie do 4 hodín od nahlásenia incidentu v zmysle čl. 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. Dodávateľ sa zaväzuje poskytnúť okamžitú súčinnosť pri riešení závažných väd programu brániacim ich riadnemu užívaniu po ich nahlásení. Bežné vady softvéru dodávateľ 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. Dodávateľ je oprávnený požadovať a objednávateľ je povinný poskytnúť pri replikácii vady potrebnú súčinnosť. Lehota na odstránenie vady sa predlžuje o dobu omeškania objednávateľa s poskytnutím súčinnosti.
2. Objednávateľ je povinný oznámiť vady bez zbytočného odkladu po ich zistení.
3. Dodávateľ sa zaväzuje, že predmet zmluvy bude spĺňať minimálne požiadavky v zmysle Prílohy č. 1 k tejto zmluve.
4. Dodávateľ 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 Nariadenia 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 dodávateľa.
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 dodávateľa 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 dodávateľom 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. Dodávateľ sa zaväzuje najneskôr k podpisu tejto 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. Dodávateľ nie je oprávnený navýšiť cenu o žiadne položky mimo zmluvnej ceny (doprava, náhradné diely a pod.).
12. Dodávateľ najneskôr k podpisu tejto 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. Dodávateľ sa zaväzuje v primeranej miere vykonať aj práce súvisiace s migráciou, implementáciou, optimalizáciou systémov a zaškolenia personálu určeného objednávateľom v zmysle Prílohy č. 1 k tejto zmluve.
14. Z dôvodu, že predmet zmluvy bude financovaný z prostriedkov poskytnutých objednávateľovi na základe Zmluvy o NFP, zaväzuje sa poskytovateľ strpieť výkon kontroly/auditú súvisiaceho s predmetom tejto zmluvy kedykoľvek počas platnosti a účinnosti Zmluvy o NFP, a to oprávnenými osobami na výkon tejto kontroly/auditú a poskytnúť im všetku súčinnosť. Objednávateľ má právo bez akýchkoľvek sankcií odstúpiť od tejto zmluvy s dodávateľom v prípade, kedy ešte nedošlo k plneniu z tejto zmluvy a výsledky finančnej kontroly Poskytovateľa NFP neumožňujú financovanie výdavkov podľa tejto zmluvy.
15. Dodávateľ je oprávnený kedykoľvek počas trvania Zmluvy vymeniť ktoréhokoľvek subdodávateľa, spôsobom podľa bodu 17 tohto článku zmluvy.
16. Dodávateľ je povinný oznámiť verejnému obstarávateľovi akúkoľvek zmenu údajov o každom subdodávateľovi počas plnenia predmetu zákazky a to bezodkladne, najneskôr v deň nasledujúcom po dni, kedy k zmene došlo.
17. V prípade zmeny subdodávateľa počas trvania Zmluvy medzi verejným obstarávateľom a úspešným uchádzačom, pričom zmenou sa rozumie výmena pôvodne navrhnutého subdodávateľa alebo vstup ďalšieho nového subdodávateľa, je povinný úspešný uchádzač najneskôr v deň, ktorý predchádza dňu, v ktorom má zmena subdodávateľa nastať, oznámiť verejnému obstarávateľovi zmenu subdodávateľa a v tomto oznámení uviesť min. nasledovné: %-ný podiel zákazky, ktorý má v úmysle zadať tretím osobám, navrhovaných nových subdodávateľov, predmety plnenia.

Článok IX. ZÁNIK ZMLUVY

1. Zmluvné strany sa dohodli, že zmluva zaniká:
 - a) písomnou dohodou obidvoch zmluvných strán k dohodnutému termínu,
 - b) odstúpením od zmluvy zo strany objednávateľa alebo Dodávateľa 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,
2. 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.
3. Za podstatné porušenie zmluvy sa považuje najmä:

- a) ak je Dodávateľ v omeškaní s dodaním predmetu zmluvy dohodnutým podľa tejto zmluvy o viac ako 10 kalendárnych dní,
 - b) porušenie povinností dodávateľa, uvedených v osobitných požiadavkách na plnenie uvedené v prílohe č. 1 zmluvy sa považuje za podstatné porušenie zmluvy zo strany dodávateľa, zakladajúce právo objednávateľa odstúpiť od zmluvy a o dodávateľovi bude podaná negatívna referencia.
 - c) ak objednávateľ neuhradí riadne vystavenú a preukázateľne doručenú faktúru ani do 30 kalendárnych dní po uplynutí jej splatnosti.
- 4. 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.
 - 5. Zmluvné strany sa dohodli, že ukončením zmluvy sa táto zmluva neruší od začiatku, ale zaniká ku dňu účinnosti odstúpenia od tejto zmluvy.
 - 6. 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.
 - 7. V prípade predčasného ukončenia tejto zmluvy niektorým z vyššie uvedených spôsobov, zmluvné strany sú povinné vysporiadať všetky svoje vzájomné záväzky, ktoré medzi nimi vznikli počas existencie právneho vzťahu podľa tejto zmluvy, najneskôr do 30 dní od ukončenia tejto zmluvy.

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 každá zmluvná strana obdrží jeden (1) 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:
Príloha č. 1 – Špecifikácia predmetu zmluvy
Príloha č. 1a - Špecifikácia položky 5
Príloha č. 2 – Cenník
Príloha č. 3 – ZOZNAM KONTAKTNÝCH OSÔB ZODPOVEDNÝCH ZA PLNENIE ZMLUVY
A ZOZNAM CERTIFIKOVANÝCH TECHNICKÝCH PRACOVNÍKOV
Príloha č. 4 – Zoznam subdodávateľov

XI.

Odkladacia podmienka

1. Zmluva nadobúda platnosť dňom podpisu obidvoma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky po splnení odkladacej podmienky podľa odseku 2 alebo 3 tohto článku zmluvy. Táto zmluva podlieha povinnému zverejňovaniu zmlúv podľa osobitného predpisu.
2. Zmluva nadobudne účinnosť po ukončení kontroly, ak ÚVO ako SO neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok VO, pričom rozhodujúci je dátum doručenia záznamu z kontroly prijímateľovi NFP, teda objednávateľovi. Ak boli v rámci kontroly VO identifikované nedostatky, ktoré mali alebo mohli mať vplyv na výsledok VO, zmluva nadobudne účinnosť momentom doručenia písomnej akceptácie navrhovanej finančnej opravy uvedenej v správe z kontroly vypracovanej Poskytovateľom NFP a kumulatívneho splnenia podmienky na uplatnenie finančnej opravy.
3. Ak zákazka, ktorej výsledkom bolo uzavretie zmluvy nebola predmetom kontroly ÚVO ako SO z dôvodu, že nebola vyhodnotená ako riziková, zmluva nadobudne účinnosť dňom doručenia oznámenia poskytovateľa prijímateľovi, že zákazka nebola na základe poskytovateľom vykonanej rizikovej analýzy vyhodnotená ako riziková.

V Nitre, dňa xxxx

Za objednávateľa:

V Bratislave, dňa xxxx

Za dodávateľa:

Doc. Ing. Klaudia Halászová
Rektorka

Ing. Pavol Šimák
konateľ

Položka 1: Dokumentácia KIB

Lehota plnenia: do troch mesiacov od nadobudnutia účinnosti zmluvy

Zahŕňa nasledovné aktivity:

- Revízia analýzy rizík pre aktíva podporujúce ZS podľa štandardov medzinárodnej normy ISO/IEC 27005:2018 a metodiky uvedenej vo Vyhláške NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- Revízia analýzy dopadov kľúčových činností mesta a vyhodnotenie parametrov.
- Príprava / revízia základných politík riadenia kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej ZoKB), 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 KIB).
- Riadenie kontinuity činností a procesov, vypracovanie vybraných krízových plánov a otestovanie týchto plánov v podmienkach mesta.

Výstupom okrem vytvorenej dokumentácie bude:

- celkový prehľad kybernetických rizík v prostredí verejného obstarávateľa vrátane súboru návrhov opatrení na ich zníženie s cieľom dosiahnutia akceptovateľnej miery rizika;
- identifikované kľúčové procesy, ich závislosti a ich parametre potrebné pri návrhu náhradných scenárov obnovy pri havárii;
- sada politík upravených pre riadenie kybernetickej bezpečnosti v prostredí verejného obstarávateľa a v súlade s požiadavkami ZoKB a Vyhlášky o KIB;
- zálohovací štandard, ktorý definuje nastavenie vybraných technológií v súlade s analýzou biznis dopadov organizácie a popis opatrení súvisiacich so zálohovacími postupmi.

Podrobný opis služieb, ktoré je uchádzač povinný poskytnúť je v nasledujúcich podkapitolách:

Revízia analýza rizík

- Revízia analýzy rizík (AR) podľa požiadaviek uvedených vo Vyhláške o KB a v súlade s metodikou medzinárodnej normy ISO/IEC 27005:2018. Pri AR je potrebné identifikovať/revidovať:
 - i. relevantné hrozby
 - ii. aktíva podieľajúce sa na dodávke ZS
 - iii. relevantné a známe zraniteľnosti
 - iv. určiť pravdepodobnosti a odhady dopadov pri realizáciách hrozieb
 - v. stanoviť úroveň rizika
 - vi. stanoviť mieru účinkov bezpečnostných opatrení a úroveň reziduálneho rizika
 - vii. navrhnúť opatrenia na zníženie reziduálnych rizík, ktoré sú vyššie ako akceptovateľná miera rizika definovaná vedením

Výstupom bude celkový prehľad kybernetických rizík v prostredí Verejného obstarávateľa vrátane súboru návrhov opatrení na ich zníženie s cieľom dosiahnutia akceptovateľnej miery rizika.

Revízia analýzy dopadov kľúčových procesov a činností

- Určenie funkčných závislostí kľúčových procesov v prostredí klienta a potrebných zdrojov pre udržanie kontinuity ich výkonu

- Určenie relevantných scenárov havárií
- Určenie parametrov Cieľový čas obnovenia - Recovery Time Objective (RTO) a Cieľový bod obnovenia - Recovery Point Objective (RPO) pre jednotlivé kľúčové procesy

Výstupom tejto revízie budú identifikované kľúčové procesy, ich závislosti a ich parametre potrebné pri návrhu náhradných scenárov obnovy pri havárii.

Príprava / revízia základných politík riadenia kybernetickej bezpečnosti

- Verejného obstarávateľa v tejto časti zákazky požaduje vypracovanie základných politík pre riadenie kybernetickej bezpečnosti podľa Prílohy č. 1 k Vyhláške o KB v časti B.
- Základné povinné politiky, ktoré verejný obstarávateľ požaduje sú tieto:
 - i. Bezpečnostná stratégia kybernetickej bezpečnosti
 - ii. Politika organizácie bezpečnosti
 - iii. Politika pre riadenie bezpečnostných rizík
 - iv. Politika pre riadenie informačných aktív
 - v. Pravidlá správania a dobrej praxe
 - vi. Politika pre riadenie dodávateľských vzťahov
 - vii. Politika pre riadenie vývoja a údržby v oblasti informačno-komunikačných technológií
 - viii. Politika pre riadenie a prevádzku informačno-komunikačných technológií
 - ix. Politika pre riadenie súladu
 - x. Politika pre riadenie kontinuity procesov a činností

Výstupom tejto prípravy bude sada politík upravených pre riadenie kybernetickej bezpečnosti v prostredí Verejného obstarávateľa a v súlade s požiadavkami ZoKB a Vyhlášky o KB.

Riadenie kontinuity činností a procesov, vypracovanie vybraných krízových plánov a otestovanie týchto plánov v podmienkach verejného obstarávateľa

Riadenie kontinuity činností (BCM) je schopnosť organizácie alebo spoločnosti pokračovať v dodávke alebo výrobe produktov a služieb na vopred dohodnutej úrovni aj po negatívnom incidente alebo výskyte krízovej situácie (napr. výpadok primárneho internetového spojenia) plynúcej na nedostupnosť vybranej agendy spoločnosti. Projekt implementácie opatrení v oblasti BCM zahŕňa 4 fázy:

- i. Analýza biznis dopadov (BIA)
- ii. Príprava internej smernice/metodiky pre riadenie oblasti BCM
- iii. Príprava Plánov kontinuity činností (BCP) a Plánov havarijnej obnovy (DRP)
- iv. Testovanie navrhnutých plánov s vybranými zamestnancami

V prípade znalostí technického riešenia môže byť dodatočným výstupom Zálohovací štandard, ktorý definuje nastavenie vybraných technológií v súlade s analýzou biznis dopadov organizácie a popis opatrení súvisiacich so zálohovacími postupmi.

Položka 2: Informačný systém pre identifikáciu a riadenie rizík v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§6) v rovine riadenia, revízie a aktualizácie potrebnej dokumentácie

Lehota plnenia: do troch mesiacov od nadobudnutia účinnosti zmluvy

Dodanie Informačného systému pre identifikáciu a riadenie rizík, ktorý musí spĺňať tieto funkčné vlastnosti:

- správa aktív – vedenie zoznamu aktív subjektu, vrátane ich vlastníkov
- správa zraniteľností – vedenie zoznamu rozpoznaných zraniteľností, vrátane ich vlastníkov
- správa hrozieb – vedenie zoznamu rozpoznaných hrozieb

- správa opatrení – vedenie zoznamu opatrení potrebných na potlačenie zraniteľností
- správa vzťahov – evidencia rozpoznaných vzťahov medzi aktívami a zraniteľnosťami
- správa rizík – identifikácia a ohodnotenie rizík na základe pravdepodobností hrozieb, uplatňovaných opatrení a dopadov na subjekt,
- semikvantitatívna prípadne kvantitatívna metóda hodnotenia významnosti rizík,
- číselné ohodnotenie pravdepodobnosti hrozieb a účinnosti opatrení,
- významnosť rizík vyjadrená číselne a následne kategorizovaná.

Užívateľské rozhranie a výstupy musia spĺňať tieto požiadavky:

- pre interakciu s používateľom musí byť k dispozícii webové rozhranie bez špeciálnych nárokov na webový prehliadač v plnej podpore slovenského jazyka,
- výstupy musia byť realizované vo forme prehľadov a zostáv vo formáte PDF vyhotovené v slovenskom jazyku vrátane šablón a komentárov,
- softvér musí umožňovať riadiť prístup užívateľov k obsahu rizikovej analýzy.

Správa používateľov musí umožňovať:

- evidenciu používateľov, oprávnených pristupovať k subjektom a identifikovať resp. manažovať ich riziká,
- širokú integráciu na existujúce systémy správy používateľov,
- pridelovanie rolí oprávneným používateľom s rôznym stupňom oprávnení.

IS pre identifikáciu a riadenie rizík musí byť umožňovať vykonávať revízie a aktualizáciu rizikovej analýzy, riadiť riziká, aktíva, zraniteľnosti a hrozby systémom, ktorý dokumentuje históriu a je auditovateľný. Verejný objednávateľ požaduje informačný systém typu klient – server nasadený u verejného obstarávateľa na jeho serveri bez závislosti na cloudových službách, aktualizáciách cez internet a inom komerčnom programovom vybavení okrem operačného systému.

Dodávka musí obsahovať časovo neobmedzenú licenciu informačného systému.

Položka 3: Sieťová a komunikačná bezpečnosť

Lehota plnenia: do troch mesiacov od nadobudnutia účinnosti zmluvy

Dodanie a implementácia New Generation Firewall (NGFW) na správu sieťovej prevádzky a blokovanie nebezpečnej sieťovej komunikácie. Firewall bude disponovať rozšírenými bezpečnostnými funkciami typu:

- VPN,
- Intrusion Prevention (IPS),
- Web Filtering,
- Antivirus/Animalware,
- Application Control,
- Advanced Threat Protection (ATP),
- Cloud-Delivered Security,
- Sandboxing,
- SSL Inspection,
- Identity Management,
- Mobile Security,
- SD-WAN,
- Wireless Controller,
- DDoS Protection,
- Bandwidth Management,
- Logging & Reporting,
- Automation & API Integration,
- Multi-Tenancy,

- Geo-IP Filtering.

Základné požiadavky na FW:

- Firewall bude umožňovať aj sandboxing (možnosť využiť cloudovú funkciu, nakoľko bude zapnutá na komunikácii prichádzajúcej zo siete Internet).
- Napojenie na RADIUS/SSO a bude podporovať SD-WAN.
- VPN prístup (cca 50 konkurenčných VPN používateľov).
- Možnosť rozdeliť firewall na min. 2 virtuálne firewally.
- Firewall by mal byť zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií a pod. Zároveň by mala byť týmto jedným výrobcom zaistená podpora minimálne po dobu plánovanej životnosti FW.
- FW by mal obsahovať jeden dedikovaný port pre správu pomocou konzoly.
- FW by mal obsahovať aspoň jeden dedikovaný OOB (Out-of-band) management port pre plnohodnotnú správu FW.
- FW by mal zároveň umožňovať funkcionalitu DHCP servera.
- FW by mal byť schopný ukladať údaje na interný disk.
- FW by mal podporovať agregáciu portov pomocou protokolu 802.3ad (LACP).
- FW by mal byť rozmerovo kompatibilný s 19 „rozdávčačom“.
- FW by mal podporovať dva nezávislé redundantné zdroje napájania AC 230V, vymeniteľné za behu zariadenia.
- FW by mal plne podporovať IPv4 aj IPv6.
- FW by mal podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64.
- FW by mal podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing).
- PBR (Policy-Based Routing) by malo byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, užívateľ.
- FW by mal podporovať režim clusteringu, využiteľný pre prípadné dodatočné zvýšenie priepustnosti.
- FW by mal podporovať site-to-site VPN pomocou protokolu IPSec.
- FW by mal podporovať Remote Access VPN pomocou protokolov IPSec a SSL (min. TLS v 1.2 / 1.3).
- Počet súčasne pripojených užívateľov nesmie byť licenčne obmedzený.
- Jednotlivé HW appliance musia obsahovať plnohodnotné grafické rozhranie (GUI) pre správu sieťových a bezpečnostných funkcií bez nutnosti používania centrálného management servera.
- FW by mal podporovať aplikačnú detekciu a kontrolu ako svoju natívnu funkcionalitu.
- FW by mal podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít.
- FW by mal obsahovať integrovaný systém ochrany proti sieťovým útokom (IPS). Databáza IPS signatúr by mala byť uložená priamo vo FW.
- Min. 1 Gbps priepustnosť rozhrania so zapnutými funkciami:
 - IPS, malware protection, url filtering,
 - SSL inšpekcia v režime pre prichádzajúci/odchádzajúci traffic na WAN rozhranie.

Požaduje sa dodanie FW s rozšírenou 5 ročnou zárukou a min. 5 ročnou technickou podporou zariadenia a podpory zo strany výrobcu (vydávanie bezpečnostných záplat).

Počet zariadení:	2 ks

HW appliance NGFW/UTM firewall; Platforma postavená na HW akcelerovanej architektúre (tj. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií ; HW appliance do racku s veľkosťou 1RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu; Zariadenie vybavené dvoma zdrojmi;	
HW akcelerované rozhrania na každom firewalle využiteľné pre management	min. 2x GE RJ45
HW akcelerované rozhrania na každom firewalle využiteľné pre spracovanie komunikácie	min. 16x GE RJ45 Ports, 8x GE SFP Slots, 4x 10 GE SFP+ Slots
Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky.	
Podpora VLAN	min. 4000
Podpora LACP	Vyžaduje sa
Počet FW pravidiel	min. 8000
Možnosť definície FW pravidiel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je:	min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.
Celková priepustnosť firewallu	min. 39/39/28 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B)
Latencia firewallu	nepresahuje 3.5 μ s (merané na malých UDP paketoch (64B))
Počet nových spojení za sekundu (setup-rate)	min. 140 000
Celkový počet súčasných TCP spojení firewallu	min. 3 000 000
PPS (počet spracovaných paketov za 1 sekundu)	min. 42 000 000
Funkcia detekcie aplikácií na L7 (Application Control)	Vyžaduje sa
Detekcia známych aplikácií na základe signatúr	min 3500 preddefinovaných aplikácií/signatúr
pre populárne cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii)	Vyžaduje sa
aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu	

priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response)	min. 6.7 Gbps
podpora použitia Application control aj formou profilov priradených k pravidlám	Vyžaduje sa
Funkcie detekcie a zamedzenia narušení (IPS/IDS)	Vyžaduje sa
počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom	min. 11000
funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám	
možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS	Vyžaduje sa
priepustnosť funkcie IPS vrátane logovania	min. 5.3 Gbps
Funkcie antivírovej kontroly	Vyžaduje sa
Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom	Vyžaduje sa
AV kontrola rozšírená o inšpekciu tzv. sandbox technikou	Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky
Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním	min. 3.1 Gbps
Podpora služby výrobcu umožňujúca detekovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hash-ov	Vyžaduje sa
Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky	Vyžaduje sa
Podpora SSL dešifrovania/SSL inšpekcie	min. 3 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou)
Funkcia DNS filtra	Vyžaduje sa
Možnosť blokovat DNS dotazy na základe príslušnosti k URL kategórii	Vyžaduje sa
Možnosť definovať vlastný tzv. blacklist domén	Vyžaduje sa
Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL	Vyžaduje sa
Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos	Vyžaduje sa

Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri	Vyžaduje sa
Podpora SSL VPN	Vyžaduje sa
Priepustnosť SSL VPN	Vyžaduje sa
Podpora IPSEC VPN v režime site-2-site aj client-2-site	
Priepustnosť IPSEC VPN (AES256-SHA256, UDP packet size 512B)	min. 35 Gbps
Podpora izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politik, smerovania a pod.	Vyžaduje sa
FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu;	Vyžaduje sa
Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky	Vyžaduje sa
Možnosť konfigurácie a následnej správy dodaných zariadení prostredníctvom existujúceho manažmentového nástroja.	Vyžaduje sa
Podpora SNMP vrátane SMPB MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete	Vyžaduje sa
Požaduje sa certifikácia ICSA Labs minimálne pre Firewall	Vyžaduje sa
Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať.	Vyžaduje sa
Možnosť kombinovať akcie pre automatizačné pravidlá	min. webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy.
Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel	min. schopnosť parsovať vstupy z logov a z predchádzajúcich vykonaných akcií
Podpora otvoreného API pre ďalšie možnosti integrácie	Vyžaduje sa
Natívna podpora SD-WAN funkcionality ktorá je súčasťou dodávaného zariadenia aj s potrebnými licenciami a ktorú je možné konfigurovať a následne spravovať prostredníctvom existujúceho manažmentového nástroja.	Vyžaduje sa

Položka 4 SIEM, LMS

Lehota plnenia: do dvoch mesiacov od nadobudnutia účinnosti zmluvy.

Dodanie a implementácia systému pre centralizované ukladanie a správu logov s integrovaným nástrojom na analýzu a riešenie bezpečnostných udalostí a incidentov zo špecifikovaných zariadení, monitorovanie bezpečnosti sietí a informačných systémov s cieľom naplnenia požiadaviek legislatívy na riešenie kybernetických bezpečnostných incidentov a opatrení pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov, a to najmä zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Základná funkčnosť systému:

- ukladanie udalostí z preddefinovaných zdrojov logov aplikácií, operačných systémov a sieťového hardware,
- monitorovanie bezpečnostne relevantných udalostí prevádzkovej infraštruktúry a informačných systémov,
- korelovanie bezpečnostne relevantných udalostí,
- vyhodnocovanie bezpečnostne relevantných udalostí,
- detekcia a riešenie bezpečnostných incidentov,

Tento aplikačný komponent zabezpečí zber logov zo sieťových zariadení a koncových staníc, spoločne s funkcionalitami:

- LMS (Log Management System) – retencia logov 13 mesiacov,
- Detekcia potencionálnych hrozieb,
- Možnosť tvorby vlastných korelačných pravidiel,
- NTA (Network Traffic Analyzer),
- FIM (File Integrity Monitoring).

Minimálne požadované komponenty pre zber logov:

- AD (Active Directory),
- DHCP,
- DNS,
- VPN,
- Firewall.

Zber logov v prostredí Microsoft / Linux / MacOS:

- udalosti z Microsoft Serverových prostredí DHCP, DNS, Active Directory sú získavané bez agenta inštalovaného priamo na koncovom Windows Server systéme,
- Windows / Linux / MacOS agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálné spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému,
- Windows / Linux / MacOS agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov,
- možnosť inštalácie agenta cez GPO.

Funkčné požiadavky systému:

- zbierať, detegovať a vyhodnocovať udalosti ako sú pokusy o neautorizované prístupy, zmeny integrity vybraných častí operačného systému,

- umožňovať monitoring, vyhodnocovanie a následné generovanie alertov a to všetko v reálnom čase, pričom nesmie technicky limitovať počet spracovávaných a ukladaných udalostí (napríklad pri prekročení licencie alebo výkonu riešenia),
- umožňovať uchovávanie pôvodnej informácie zo zdroja logu o časovej značke udalosti,
- každý log musí mať unikátny identifikátor, pre jednoznačnú identifikáciu,
- musí podporovať detekciu sieťových incidentov,
- bez nutnosti požiadaviek na externý databázový server,
- možnosť tvorby vlastných Dashboardov a Vizuálnych Analýz,
- podporuje zber dát so šifrovaným prenosom (TLS, prípadne šifrovaný obsah správ) na celej trase zdroj /kolektor/ centrálna konzola,
- podporuje vlastnú alebo externú integráciu na multifaktorovú autentifikáciu, multifaktorová autentifikácia minimálne s podporou Google Authenticator a SMS správy
- musí podporovať funkcionality auditovania integrity súborov pre minimálne nasledujúce typy súborov Linux:
 - /bin,
 - /boot,
 - /etc,
 - /sbin,
 - /usr/bin,
 - /usr/local/bin,
 - /usr/local/sbin,
 - /usr/sbin,
 - /usr/share/keyrings,
 - /var/spool/cron,
- musí podporovať funkcionality auditovania integrity súborov pre minimálne nasledujúce typy súborov Windows:
 - bat,
 - .cfg,
 - .conf,
 - .config,
 - .dll,
 - .exe,
 - .ini,
 - .sys,
 - .ps1,
 - .cmd,
- NTA môže byť nasadené do internej či externej časti siete bez licenčného obmedzenia množstva nasadených zariadení,
- NTA poskytuje špecifické korelačné pravidlá pre SIEM súvisiace s analýzou sieťovej prevádzky,
- NTA poskytuje špecifické vyhľadávacie vzory (queries) pre SIEM súvisiace s analýzou sieťovej prevádzky,
- NTA poskytuje špecifické šablóny pre tvorbu dashboard v SIEM súvisiace s analýzou sieťovej prevádzky,
- NTA musí byť možné inštalovať do fyzického, virtualizačného alebo cloud prostredia.

Ďalšie požiadavky:

- Aktualizácie systému sú distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu.
- Systém musí podporovať integráciu externých zdrojov informácií.
- Zber udalostí v prostredí Microsoft:
 - Udalosti z Microsoft prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Windows systéme. Windows agent musí súčasne

- podporovať ako monitoring interných Windows logov, tak i monitoring textových súborových logov. (nie je možné riadiť hromadne)
- Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií.
- Agent zabezpečuje v prípade potreby funkcionality kontroly integrity súborov.
- Agent zabezpečuje v prípade potreby funkcionality auditovania prístupov k súborom na zariadení. (pri Essentials nie)
- Nerelevantné logy sú filtrované na strane Windows agenta a nie sú odosielané po sieti.
- Windows agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálnie spravovaný a automaticky aktualizovaný priamo z centrálnej správovskej konzoly systému.
- Windows agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov.
- Zber udalostí v prostredí Linux / MacOS:
 - Udalosti z Linux / MacOS prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Linux / MacOS systéme. Linux / MacOS agent musí súčasne podporovať ako monitoring interných logov, tak i monitoring textových súborových logov.
 - Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií.
 - Nerelevantné logy sú filtrované na strane Linux / MacOS agenta a nie sú odosielané po sieti.
 - Linux / MacOS nevyžaduje administrátorské zásahy na koncovom systéme – je centrálnie spravovaný a automaticky aktualizovaný priamo z centrálnej správovskej konzoly systému.
 - Linux agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov.
- Zber udalostí zo sieťového prostredia:
 - Zber udalostí zo sieťovej komunikácie minimálne: DNS, DHCP a IDS.

Kapacitné požiadavky:

Zdroje logov:

- Dodávaný systém musí podporovať zber logov z nasledujúcich zariadení a systémov: Windows server Active Directory; Windows server File system; Linux server; network switch (Cisco, Mikrotik, Fortigate); Firewally Fortigate, Cisco alebo Mikrotik,
- Windows desktop - **rádovo do 1200 ks zariadení**
- Požadovaná retencia logov udalostí pre okamžité spracovanie systémom pre uvedené počty zariadení je min. 390 dní. Systém musí zároveň umožňovať archivovať staršie záznamy.
- Systém musí obsahovať centrálnie spravované riešenie, ktoré zbiera udalosti na pobočkách alebo v záložnom datacentre a umožňuje ich odoslanie po saturovanej linke bez straty dát.
- Systém musí podporovať centralizovanú správu pre zber udalostí z viacerých lokalít priamo z centrálného úložiska dát vrátane požiadaviek na virtualizáciu a komunikačnú maticu pre šifrovaný prenos dát.
- Riešenie pre zber udalostí z iných lokalít musí byť schopné automaticky nadviazať spojenie s centrálnym úložiskom dát a prenášané dáta šifrovať. V prípade výpadku spojenia medzi inou lokalitou a centrálou musí spojenie automaticky obnoviť.
- Zber udalostí bude realizovaný z 1 lokality verejného obstarávateľa.

Súčasťou dodávky sú:

- potrebné SW licencie prípadne predplatné služby pre naplnenie požiadaviek **na obdobie 12 mesiacov**,
- dodanie a inštalácia,
- jednorazové implementačné služby minimálne v nasledujúcom rozsahu:
 - nastavenie a konfigurácia systému v IT prostredí verejného obstarávateľa,
 - konfigurácia Windows systémov pre zasielanie logov do systému,
 - overenie funkčných a výkonových parametrov Windows agentov,
 - konfigurácia Linux systémov pre zasielanie logov do systému,
 - overenie funkčných a výkonových parametrov Linux agentov, o predvedenie vytvorenia a uloženia vlastného dashboardu a reportu, o predvedenie vytvorenia a uloženia užívateľsky definovaného parseru,
 - predvedenie nastavenia značkovania udalostí a vytvárania upozornení s limitom alebo koreláciou,
 - nastavenie a predvedenie odoslania udalosti, ktorá vyvolala alert na externý Syslog server cez TCP protokol;
 - nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom verejného obstarávateľa,
 - zaškolenie obsluhy a správy systému pre min. 2 zamestnancov verejného obstarávateľa, o vytvorenie a odovzdanie prevádzkovej dokumentácie systému, administrátorskej dokumentácie,
- post-implementačná podpora v rozsahu **minimálne 18 človekodní na obdobie 12 kalendárnych mesiacov**, ktorá zahŕňa:
 - pravidelnú kontrolu bezpečnostných udalostí (alertov), o participáciu na odstraňovaní bezpečnostného incidentu, o konfiguračné práce v systéme, o konzultácie k používaniu produktu.

Osobitné požiadavky na plnenie a podpora riešenia

Zmluvná cena bude rovnomerne rozdelená na 12 mesačných platieb počas doby trvania Zmluvy na základe faktúr zasielaných Dodávateľom prostredníctvom elektronického alebo poštového styku. Dodávateľ nie je oprávnený navýšiť cenu o žiadne položky mimo zmluvnej ceny (doprava, náhradné diely a pod.).	
Dodávateľ je povinný preukázať Objednávateľovi, že v čase uzavretia zmluvy je oficiálnym partnerom spoločnosti/výrobcu v Slovenskej republike pre ponúkané riešenie (pokiaľ nie je dodávateľom priamo výrobca riešenia), ktorý je zároveň oprávnený predávať licencie pre sektor verejnej správy.	
Úroveň partnerstva Dodávateľa podľa predchádzajúceho bodu musí byť pre Objednávateľa verifikovateľné z verejných zdrojov (napr. webová stránka výrobcu), alebo takéto partnerstvo doloží Dodávateľ písomným potvrdením výrobcu v elektronickej podobe do 3 dní od uzavretia zmluvy.	
Podpora	
Dodávateľ zabezpečí pre Objednávateľa prioritizáciu pri riešení kritických incidentov na technickej podpore výrobcu ponúkaného riešenia a poskytnutie príslušných eskalačných kontaktov v slovenčine pre celú komunikáciu (webovú, elektronickú, písomnú aj telefonickú). Technologická infraštruktúra podpory a poskytovateľ technickej podpory sa musí nachádzať výlučne na území štátov Európskej Únie.	
Definícia podpory	Podpora poskytovaná 8x5 v prac. dňoch v čase 8:00-16:00 h, potvrdenie prijatia požiadavky na servisný zásah do 60 min, nástup na riešenie najneskôr do 4 h od nahlásenia incidentu.

Požadované proaktívne činnosti pre oblasť podpory	<p>Proaktívne riešenie vznikajúcich problémov v rozsahu 2 MD mesačne. V rámci tejto aktivity sú požadované nasledovné činnosti:</p> <ul style="list-style-type: none"> - proaktívny monitoring vybraných parametrov a dostupnosť všetkých služieb SIEM riešenia - nastavovanie pravidelných reportov podľa požiadaviek objednávateľa v celkom rozsahu 2 reporty za mesiac, - pravidelné vyhodnocovanie bezpečnostných incidentov na mesačnej báze s príslušným návrhom opatrení a reštrikcií, - analyzovať bezpečnostné logy, - uskutočňovať aktívnu analýzu zistení, - analyzovať techniky používané v nadväznosti na útoky na počítačové a sieťové systémy - aktualizácia aplikačného vybavenia v zmysle odporúčaní výrobcom, - dodanie informácií o známych bezpečnostných chybách a aplikovanie náprav, - evidencia bezpečnostných incidentov a úprav na on-line portáli/HelpDesku.
Požaduje sa prístup aktualizáciám softvérových balíkov na celé obdobie trvania zmluvy.	
Požaduje sa možnosť vytvárať tikety k incidentom minimálne telefonicky a emailom na základe dodatočného upresnenia.	
Požadujú sa výrobcom poskytované a garantované informácie a podpora k produktu ešte pred vznikom incidentu (proaktívna podpora), od odborne vyškolených špecialistov technickej podpory výrobcu plnohodnotne v slovenčine v písomnej aj ústnej forme.	
Tovary a služby sa budú považovať za poskytované až po zaregistrovaní na zákazníckom účte Objednávateľa vedeného výrobcom produktu, alebo dodaní licenčných kľúčov pričom túto skutočnosť bude možné overiť cez zákaznícky portál výrobcu, alebo pravidiel dodaných samotným výrobcom.	
V cene riešenia musia byť zahrnuté všetky náklady (ďalej len „TCO“) súvisiace s predmetom zákazky (najmä, ale nie výlučne poskytnutie licencie, dodanie, záplaty, aktualizácie, podpora a pod.).	
Porušenie povinností dodávateľa, uvedených v Osobitných požiadavkách na plnenie sa považuje za podstatné porušenie zmluvy zo strany dodávateľa, zakladajúce právo objednávateľa odstúpiť od zmluvy a o dodávateľovi bude podaná negatívna referencia.	
Dodávateľ na svoje náklady preškolí 2 administrátorov Objednávateľa na centralizovanú správu a implementáciu produktu v trvaní najmenej 1 školiaci deň pre každú osobu v sídle	
Pri implementácii Objednávateľ poskytne Dodávateľovi nevyhnutnú súčinnosť a to najmä dodaním potrebných kontaktov, informácií, technickej dokumentácie, špecifikácií, konfigurácií, hesiel, fyzických a vzdialených prístupov pre Dodávateľa. Tieto budú poskytnuté Dodávateľovi výlučne v súlade s platnými internými IKT predpismi a procesmi objednávateľa. Prípadné náklady na inú požadovanú súčinnosť zo strany Objednávateľa budú ním vyčíslené, budú sa započítavať do TCO a znáša ich v plnej výške Dodávateľ.	

Položka 5 Upgrade antivírusového softvéru ESET a služby rozšírenej podpory kybernetickej bezpečnosti s aktívnym monitoringom XDR platformy

Špecifikácia sa nachádza v Prílohe č. 1a zmluvy