ZMLUVA O DIELO

uzavretá podľa ust. § 536 a nasl. Obchodného zákonníka č. 513/1991 Zb. v znení neskorších predpisov medzi týmito zmluvnými stranami:

I.
ZMLUVNÉ STRANY

Objednávateľ:	Mesto Revúca
Sídlo:	Námestie slobody 13/17, 050 80 Revúca
Štatutárny zástupca:	Ing. Július Buchta, MBA
IČO:	00328693
DIČ:	2020724805

a

Zhotoviteľ:	**void SOC, s.r.o.**
Sídlo:	Plynárenská 5, 829 75 Bratislava
Štatutárny orgán:	Mgr. Martin Lohnert, konateľ spoločnosti Ing. Ondrej Smolár, konateľ spoločnosti
IČO:	46957545
IČ DPH:	SK2023692418
Bankové spojenie:	SK18 1100 0000 0029 2912 3439

II.
PREDMET ZMLUVY

1. Predmetom tejto zmluvy, dielom je poskytovanie nasledovných služieb:

Modul 1.	**Nasadenie informačného systému 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**
Modul 2.	**Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)**
Modul 3.	**Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti**
Modul 4.	**Zriadenie SOC ako služby v prevádzke 24/7**
Modul 5.	**Nasadenie DLP**
Modul 6.	**Nasadenie zálohovania**

a to všetko v rozsahu a spôsobom podľa OPISU ZÁKAZKY, ktorý tvorí nedeliteľnú prílohu č. 1 tejto Zmluvy ako aj v zmysle cenovej ponuky víťazného uchádzača ktorá tvorí nedeliteľnú prílohu č. 2 k tejto zmluve.

2. Uvedené dielo, resp. službu poskytne zhotoviteľ podľa tejto zmluvy, OPISU PREDMETU zákazky, ktorý tvoril prílohu č. 1 tejto zmluvy a bol súčasťou výzvy na predkladanie ponúk, svojej ponuky predloženej v rámci prieskumu trhu, ktorý prieskum predchádzalo uzatvoreniu tejto zmluvy, ako aj prípadných iných požiaviek objednávateľa.
3. Zhotoviteľ sa zaväzuje plniť svoj záväzok osobne. V prípade, ak svoj záväzok (jeho časť) plní zhotoviteľ prostredníctvom tretej osoby, zodpovedá voči objednávateľovi ako keby záväzok (jeho časť) vykonával sám.
4. Objednávateľ sa zaväzuje, že riadne poskytnutú službu zaplatí dohodnutú cenu.
5. Všetky veci potrebné na vlastné zhotovenie diela, poskytnutie služby obstará zhotoviteľ, dielo, resp. poskytnutie služby vykoná na vlastné náklady a na svoje nebezpečenstvo a zodpovednosť.

III.
ČAS PLNENIA

Zhotoviteľ sa zaväzuje, že inštalácia softvérového vybavenia na riadenie rizík bude v prevádzke objednávateľa najneskôr do 30 pracovných dní odo dňa nadobudnutia platnosti a účinnosti zmluvy, pričom začatie poskytovania služby musí byť v celom rozsahu spustené najneskôr do troch mesiacov odo dňa začatia inštalácie softvérového vybavenia na riadenie rizík.

Implementácia BCM, riadenia kontinuity musí byť začatá najneskôr do 30 pracovných dní odo dňa nadobudnutia platnosti a účinnosti zmluvy.

Táto zmluva sa uzatvára na dobu určitú, a to do 31.10.2023.

IV.
CENA

(1) Cena za vykonanie diela podľa tejto zmluvy je po dohode zmluvných strán 102 440 EUR bez DPH, čo predstavuje 122 928 EUR s DPH. Cena je tvorená ako cena pevná nemenná. Zmena ceny je možná výlučne písomným dodatkom k tejto Zmluve a v súlade so zákonom o verejnom obstarávaní. Presná špecifikácia ceny je definovaná v Prílohe č. 3 tejto zmluvy, Návrhu na plnenie kritérií, ktorý návrh na plnenie kritérií bol predložený uchádzačom ako víťazom zákazky s nízkou hodnotou ktorá predchádzala uzatvoreniu tejto zmluvy.

(2) Akékoľvek zmeny ceny smerom nahor, a teda zmeny, ktorých následkom je zvýšenie ceny diela sú možné len na základe obojstranne (oboma zmluvnými stranami) odsúhlaseného a podpísaného Dodatku k tejto Zmluve.

(3) Cena diela, dohodnutá medzi oboma zmluvnými stranami, zahŕňa všetky vykázané a ocenené práce a dodávky, odborné posudky, vyjadrenia, skúšky a ďalšie súvisiace práce zhotoviteľa, ktoré budú potrebné či už pri realizácii alebo potrebné k prevzatiu diela a jeho prípadnému odovzdaniu do užívania.

(4) Zhotoviteľ sa nemôže dovolávať a uplatňovať nároky na zvýšenie ceny diela v prípadoch:
a) vlastných chyb,

b) nepochopenia zadania,
c) nedostatkov riadenia a koordinácie činností pri príprave a realizácii diela,
d) zvýšenia cien dodávok a prác.

Zhotoviteľ nesmie zrealizovať prípadné naviac práce bez predchádzajúceho písomného súhlasu objednávateľa a uzatvoreného dodatku k ZoD na tieto práce naviac. V prípade, ak zhotoviteľ vykoná naviac práce bez predchádzajúceho písomného súhlasu objednávateľa, nemá nárok na zaplatenie za takto vykonané práce

V.
PLATOBNÉ PODMIENKY

(1) Zhotoviteľ bude fakturovať dokončené práce vždy raz mesačne faktúrou vystavenou na 10 deň nasledujúceho mesiaca po riadnom poskytnutí služby. Neexistuje možnosť zálohových platieb.

(2) Faktúry zhotoviteľa budú obsahovať tieto údaje:
- označenie povinnej a oprávnenej osoby, adresa príslušnej prevádzky, sídlo, IČO, IČ DPH,
- dátum uzavretia zmluvy (prípadne i jej číslo),
- číslo faktúry,
- dátum uskutočnenia zdaniteľného plnenia,
- deň odoslania a deň splatnosti faktúry (podľa zmluvy),
- označenie peňažného ústavu a číslo účtu zhotoviteľa, na ktorý sa má platiť,
- fakturovanú sumu s uvedením DPH,
- označenie diela (i fakturovanej časti diela podľa zmluvy);
- pečiatku a podpis osoby oprávnenej fakturovať v mene zhotoviteľa,
- v prílohe k faktúre písomné schválenie vecnej stránky faktúry v zmysle tejto zmluvy.

(1) Ak faktúra nebude obsahovať požadované údaje, je objednávateľ oprávnený ju vrátiť na doplnenie zhotoviteľovi, čím sa preruší splatnosť faktúry a nová splatnosť začína plynúť od doručenia novej faktúry.

(2) Splatnosť faktúry je 30 dní odo dňa jej doručenia druhej zmluvnej strane .

VI.
ZODPOVEDNOSŤ ZA VADY

(1) Zhotoviteľ zodpovedá za to, že služby v zmysle predmetu zmluvy sú, resp. vykonané riadne v súlade so zmluvou, príslušnými právnymi predpismi, technickými normami a počas záručnej doby budú mať vlastnosti dohodnuté v zmluve a/alebo obvyklé vlastnosti ktoré od takéhoto diela možno očakávať. Taktiež zhotoviteľ zodpovedá za vady, ktoré predmet diela má v čase jeho odovzdania, ako aj za vady, ktoré sa prejavili po odovzdaní diela.

(2) Zhotoviteľ nezodpovedá za vady diela, ktoré boli spôsobené objednávateľom a zhotoviteľ ani pri vynaložení odbornej starostlivosti nemohol zistiť ich nevhodnosť.

(3) Záručná doba diela je nasledovná a začína plynúť od odovzdania diela objednávateľovi. Počas záručnej doby má objednávateľ právo požadovať a zhotoviteľ povinnosť bezodplatne odstrániť vady diela. Záručná doba na práce je v trvaní 3 rokov .

(4) Objednávateľ sa zaväzuje, že prípadnú reklamáciu vady diela uplatní bezodkladne po jej zistení (najneskôr do 10 pracovných dní) písomne alebo emailom do rúk zástupcu zhotoviteľa.

(3) V prípade, ak objednávateľ nereklamoval zjavné vady a nedorobky, zaniká jeho právo zo zodpovednosti za vady a nedorobky a ostatné vady do skončenia záručnej lehoty.

(4) Zhotoviteľ je povinný odstrániť vady v čo najkratšom technicky možnom čase. O čase odstránenia vady je povinný upovedomiť Objednávateľa bezodkladne po obdržaní reklamácie. Je povinný tak urobiť písomne alebo emailom.

VII.
SPOLOČNÉ A ZÁVEREČNÉ USTANOVENIA

(1) Objednávateľ je oprávnený vykonať kontrolu diela u zhotoviteľa podľa jeho vlastného uváženia, a tiež na kontrolných dňoch určených zhotoviteľom po ich predchádzajúcej vzájomnej dohode.

(2) Účastníci zmluvného vzťahu sa zaväzujú, že obchodné a technické informácie, ktoré im boli zverené, nesprístupnia tretím osobám, bez písomného súhlasu druhej zmluvnej strany, alebo tieto informácie nepoužijú pre iné účely než sú dohodnuté v zmluve.

(3) Zmluva je uzavretá okamihom, kedy je posledný súhlas s obsahom návrhu zmluvy doručený druhej zmluvnej strane. Meniť alebo doplňovať obsah tejto zmluvy je možné len vo forme písomných dodatkov, ktoré budú platné, ak budú potvrdené a podpísané obidvoma zmluvnými stranami.

(4) Ak sa vyskytnú otázky neriešené touto zmluvou, použijú sa primerane ustanovenia Obchodného zákonníka.

(5) Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy ako sa uvádza priebežne v texte.

(6) Táto zmluva je vypracovaná v troch exemplároch, z ktorých jeden je pre zhotoviteľa a dva pre objednávateľa.

(7) Táto zmluva sa stane platnou dňom jej podpis zmluvnými stranami. Zmluvné strany si dohodli odkladaciu podmienku účinnosti tejto zmluvy, a to ukončenie finančnej kontroly, v rámci ktorej poskytovateľ neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok verejného obstarávania – prieskumu trhu (po doručení správy z kontroly prijímateľovi).

(8) Povinnosťou zhotoviteľa je strpieť výkon kontroly/auditu/overovania súvisiacich s predmetom zmluvy kedykoľvek počas platnosti a účinnosti Zmluvy o NFP pre projekt *„Názov projektu : Zvýšenie kybernetickej bezpečnosti mesta Revúca, číslo projektu: 311071CDY6, miesto realizácie projektu: Stredné Slovensko, Banskobystrický kraj,*

okres Revúca, mesto: Revúca, Výzva - kód Výzvy: OPII-2021/7/16-DOP v zmysle príslušných právnych predpisov SR, najmä zákona č. 357/2015 Z. z. o finančnej kontrole a audite na to oprávnenými osobami a poskytnúť im na požiadanie všetku potrebnú súčinnosť. Oprávnené osoby na výkon kontroly/auditu/overovania sú najmä:

a) Poskytovateľ NFP a ním poverené osoby,
b) NKÚ, Úrad vládneho auditu,
c) Orgán auditu, jeho spolupracujúce orgány a nimi poverené osoby,
d) Osoby prizvané orgánmi uvedenými vyššie v súlade s príslušnými predpismi SR.

V Revúcej, dňa ..

V Bratislave, dňa ....

.....
objednávateľ
Ing. Július Buchta, MBA
Mesto Revúca

.....
zhotoviteľ
Mgr. Martin Lohnert
void SOC, s.r.o.

Príloha č.1 -

Opis predmetu zákazky :

Modul 1. Nasadenie informačného systému 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

Informačný systém pre identifikáciu a riadenie rizík musí spĺňať tieto funkčných 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,
- prideľovanie 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.

Požiadavky na výkon činností manažéra pre riadenie rizík prostredníctvom IS pre identifikáciu a riadenie rizík:

- tvorba analýz rizík podľa potreby a požiadaviek verejného obstarávateľa,
- pravidelné hodnotenie a ošetrovanie rizík,
- tvorba plánu eliminácie rizík,
- správa aktív a ich vlastníkov,
- dohľad nad riadením rizík.

Verejný obstarávateľ požaduje oceniť a implementovať časovo neobmedzenú licenciu informačného systému pre identifikáciu a riadenie rizík pre jedného používateľa, ako aj zrealizovať inštaláciu a na serveroch verejného obstarávateľa, vyškoliť zamestnancov verejného obstarávateľa a zabezpečiť výkon špecialistu na riadenie rizík (manažéra pre riadenie rizík) až do termínu 31.10.2023.

Modul 2. Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)

Kontinuita činností musí zadefinovať scenáre rôznych udalostí, ktoré potencionálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:

- náhla nedostupnosť personálu či nepoužiteľnosť pracoviska/budovy,
- nedostupnosť technologickej infraštruktúry či potrebných médií,
- incident či živelná katastrofa.

V rámci kontinuity činností musia byť stanovené požiadavky na zdroje (adekvátne finančné, materiálno-technické a personálne zdroje), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. V zmysle požiadaviek zákona o kybernetickej bezpečnosti sa musí určiť čo má byť:

- hlavným cieľom plánu kontinuity s ohľadom na riadenie incidentov v prípade katastrofy alebo iného rušivého incidentu a ako sa obnovia činnosti v stanovených termínoch,
- strategickým imperatívom procesu riadenia kontinuitu s ohľadom na predchádzanie ďalším stratám.

Súčasťou kontinuity činností musí byť vypracovanie analýzy funkčných dopadov a kvalifikácia potencionálnych dopadov a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Požiadavkou analýzy funkčného dopadu musí byť určenie:

- cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
- cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby.

Kontinuitou musia byť zavedené postupy zálohovania na obnovy siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujúce najmenej:

a) frekvenciu a rozsah zdokumentovania a schvaľovania obnovy záloh,
b) určenie osoby zodpovednej za zálohovanie,
c) časový interval, identifikáciu rozsahu údajov, zadefinovanie dátového média zálohovania a zabezpečenie vedenia dokumentácie o zálohovaní,
d) umiestnenie záloh v zabezpečenom prostredí s riadeným prístupom,
e) zabezpečenie šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
f) vykonávanie pravidelného preverenia záloh na základe vypracovaného plánu, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.

Kontinuita činností musí obsahovať minimálne:

- plán kontinuity na stanovenie požiadaviek a zdrojov,
- plán reakcie na incidenty a plány havarijnej obnovy prevádzky,
- politiku a ciele kontinuity,
- analýzu funkčných dopadov,
- stratégiu riadenia kontinuity vrátane evakuačných postupov,
- plán údržby a kontroly BCMS.

Požiadavky na výkon činností manažéra pre riadenie kontinuity činností:

a) riadenie incidentov v prípade katastrofy alebo rušivého incidentu,
b) realizácia a výkon interných auditov a analýz dopadov,
c) precvičovanie zavedených krízových plánov,

d) aktualizácia plánov reakcie na incidenty a plánov obnovy po katastrofe,
e) návrh opatrení riadenia kontinuity,
f) monitorovanie zariadení podstatných pre prípadný vznik incidentu.

Verejný obstarávateľ požaduje oceniť, vytvoriť a zaviesť kontinuitu činností v plnom rozsahu stanovenom zákonom č.: 69/2019 Z. z. o kybernetickej bezpečnosti a vyhláškou č.: 362/2018 Z. z., ako aj implementovať procesy kontinuity v podmienkach verejného obstarávateľa, vyškoliť zamestnancov verejného obstarávateľa a zabezpečiť výkon špecialistu (manažéra pre riadenie kontinuity) až do termínu 31.10.2023.

Modul 3. Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti

Musí byť pokryté monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb podľa nakonfigurovaných pravidiel. Monitorovací nástroj musí informovať o vzniknutých technických problémoch a nedostatku kapacít správcu príslušnej služby alebo servera. Musí byť schopný monitorovať rôzne druhy zariadení ako sú fyzické a virtuálne servery, sieťové prvky, dátové úložiská a iné zariadenia, ktoré dokážu poskytnúť údaje o svojej prevádzke. Monitoring musí byť v reálnom čase s možnosťou údaje okamžite vizualizovať prostredníctvom grafov, máp a rôznych náhľadov. Musí byť schopný porovnávať dáta v rôznych časových obdobiach, analyzovať históriu.

Funkčné požiadavky:

- Monitorovanie kľúčových informačných systémov a ich jednotlivých komponentov
- Nastavenie prahových hodnôt alertov a notifikácií
- Eskalácia notifikácií
- Tvorba reportov
- Tvorba vlastných sledovacích schém.

Do monitoringu bude zahrnutých 10 zariadení a služieb, komponentov infraštruktúry z množiny:

- Sieťových a výkonových zariadení
- VMware služieb
- Databázových a zálohovacích zariadení
- Webových služieb
- Kritického hardvéru.

Zber údajov musí podporovať:

- Agentov SNMP a IPM
- Bezagentový a špeciálny monitoring
- Monitoring virtuálnych zariadení
- Webové aplikácie a Java scenáre
- Monitoring databáz
- Kalkulované a agregované položky
- Interné sledovanie výkonu.

Musí byť podporovaná vizualizácia vo webovom rozhraní a informovanosť v rozsahu:

- Grafov a máp so zloženými pohľadmi
- Globálnych Dashboardov
- Prístupu k získaným hodnotám a zoznamu udalostí
- Zasielania oznámení
- Potvrdenia a eskalácie prijatých informácií
- Schopnosti prijať opatrenia.

Systém musí byť schopný automatizácie, napr. cez Network alebo Low-level discovery. Musí byť schopný správy aj cez smartfón, schopný nasadenia vlastných skriptov s prístupom k funkciám cez API. Musia sa dať definovať pravidlá hodnotenia údajov poskytujúce logické definície stavu zariadení.

Modul 4. Zriadenie SOC ako služby v prevádzke 24/7

Dodávka služieb súvisiacich s dohľadovým centrom bezpečnostných incidentov – SOC (Security Operations Center). Služba musí zahŕňať:

- Zber a monitorovanie udalostí v sieťach a kritických prvkoch informačných systémov v režime 24 x 7,
- nepretržitá detekcia kyberneticko-bezpečnostných incidentov,
- zber relevantných informácií pri zistených kybernetických incidentoch,
- návrh riešenia kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov,
- vyhodnocovanie riešenia kybernetických bezpečnostných incidentov a návrh systémových opatrení s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov,
- podrobná evidencia bezpečnostných incidentov, ich riešení a príslušnej komunikácie prostredníctvom na to určeného nástroja (ticketing/service desk),
- pravidelný reporting (1 x mesačne).

Sondu pre zber dát požadujeme – viruálne zariadenie. Súčasťou dodávky zariadenia je jej inštalácia a implementácia v rozsahu:

- inštalácia funkcionality zbierania záznamov z prevádzky Informačných systémov,
- zabezpečenie a sprevádzkovanie sieťovej konektivity,
- konfigurácia systémov SOC s ohľadom na špecifickosť prostredia.

Vyžadované SLA parametre sú:

	Garantovaný čas odozvy SOC
Incident kategórie HIGH - vysoko nebezpečné incidenty, ktoré môžu spôsobiť vážne škody resp. môžu mať negatívny dopad na kritické aktíva.	maximálne 2 hodiny
Incident kategórie MEDIUM - incidenty strednej závažnosti, t.j. ktoré akútne neohrozujú kritické časti prostredia.	maximálne 4 hodiny

Incident kategórie LOW - incidenty nízkej závažnosti bez priameho negatívneho vplyvu na kontinuitu služby.	maximálne 8 hodín

Zoznam kategórií bezpečnostných incidentov

Kategória	Subkategória	SLA priority
	Nevyžiadaná pošta	LOW
	Obťažovanie	LOW
	Vyhrážanie	LOW
	Potláčanie práv a slobôd	LOW
Škodlivý kód	Vírus, červ, Trójsky kôň	MEDIUM
Získavanie	Skenovanie siete	MEDIUM
	Odpočúvanie	MEDIUM
	Sociálne inžinierstvo	MEDIUM
Pokus o prienik	Využitie známej zraniteľnosti	MEDIUM
	Opakované pokusy o prihlásenie	MEDIUM
	Útok s neznámymi znakmi	MEDIUM
Podozrenie na úspešný prienik do systému	Skompromitovanie privilegovaného účtu	HIGH
	Skompromitovanie obmedzeného účtu	HIGH
	Skompromitovanie aplikácie	HIGH
	Botnet	HIGH
Nedostupnosť	DoS, DDoS	MEDIUM
	Sabotáž	MEDIUM
Ohrozenie bezpečnosti Informácii	Neoprávnený prístup k informáciám	MEDIUM
	Neoprávnená zmena Informácii	MEDIUM
Podvod	Neoprávnené využívanie	MEDIUM
	Porušenie autorských práv	MEDIUM
	Prevzatie identity	MEDIUM
	Phishing	MEDIUM
Iné		LOW

Monitorované zariadenia

Popis	Typ zariadenia/názov produktu	Počet	Proaktívny monitoring
Firewall		1	8 x 5
virtuálny server pre informačný systém samosprávy		1	8 x 5
virtuálny server pre zálohovanie		1	8 x 5
Domain Controler(Active Directory)		2	8 x 5

Popis	Typ zariadenia/názov produktu	Počet	Proaktívny monitoring
virtuálny server pre zverejňovanie na egov.revuca.sk		1	8 x 5

Súčasťou služby a jej ceny sú všetky implementačné, softvérové, hardvérové a licenčné prostriedky potrebné pre jej chod.

Modul 5. Nasadenie DLP

Nasadenie DLP ako služby je rozdelené do nasledovných krokov:

- Obstaranie SW riešenia a licencií
- Zavedenie DLP do testovaco adaptačnej prevádzky
- Analýza pracovných procesov a dátových tokov a definovanie detekčných pravidiel
- Optimalizácia detekčných pravidiel
- Nasadenie DLP na 60 ks pracovných staníc ako produkčný zdroj informácií pre SOC
- Zaškolenie personálu Prevádzkovateľa

Súčasťou riešenia musí byť aj celkový report zistení s návrhom opatrení.

Všeobecné požiadavky:

- Integrácia s MS Active Directory, Podpora pre MS SQL 2012 alebo novšia,
- Podpora operačných systémov Windows 7, 8.1, 10 a 11.
- Podpora serverových operačných systémov Windows Server 2016, 2019 a 2022. P
- Podpora terminálových prostredí ,
- Centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni OU domény,
- Riadené užívateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia,
- Skrytý režim na koncovej stanici vrátane procesov a zložiek, a to vrátane lokálnych i doménových administrátorov.

Ochrana proti zastaveniu systému (musí byť aktívna u bežného užívateľa, lokálneho i doménového administrátora, Ochrana proti zastaveniu procesov; V prípade vyšších užívateľských práv dôjde k reštartu zastavených procesov či k použitiu iných spôsobov pre obnovu služby, Ochrana proti odinštalovaniu riešenia bez potrebnej autorizácie, Ochrana proti editácii registrov, systémových komponentov či DLL knižníc, Ochrana proti zmene nastavenia na koncovej stanici, Nutná možnosť ochrany i u operačného systému v režime "safe mode".

Funkcionality zachované i v offline móde, (ak koncová stanica nie je pripojená k firemnej sieti/ internetu). Možnosť pracovať s historickými dátami. Riešenie musí podporovať možnosť poskytnúť

zálohovanie vlastných komponentov, prevažne všetkých záznamov a nastavení. 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). Zasielanie logov do SIEM riešenia objednávateľa.

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 užívateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové). 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 tlačených úloh a možnosť exportu reportov do XLS, PDF.

Zaznamenávanie komunikácie:

- Podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania,Podpora desktopových emailových klientov (Microsoft Outlook, Mozilla Thunderbird,...) – 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.

Zaznamenávanie Office 365 cloudu:

- Zaznamenávanie bežných užívateľských akcií prevedených na Office 365 cloudu (OneDrive for Business, SharePoint Online) - základné súborové operácie ako sťahovanie a zdieľanie,
- Zaznamenávanie Office 365 emailové komunikácie (Exchange Online) pre všetkých užívateľov vrátane užívateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.

Všeobecná ochrana: Definícia kategórií citlivých dát dovoľuje obmedzenie pohybu a práce s týmito dátami; určuje, ktoré média môžu byť použité pre prenos, ktoré siete môžu byť použité pre upload, na ktoré emailové adresy môžu byť dáta odoslané, ktoré aplikácie môžu s dátami pracovať. Možnosť aplikácie politík pre konkrétne aplikácie – definícia zdroja a cieľa (prístup na externé zariadenie, sieť, tlač, virtuálnu tlač) a správa užívateľských operácií (použitie schránky, snímanie obrazovky).

- Možnosť správy nepovolených cloudových úložísk.
- Možnosť úplne blokovať užívateľské akcie, informatívna notifikácia užívateľa či samotné logovanie užívateľských akcií, ochrana citlivých dát, možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov.
- Možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov. Možnosť importu vlastných slovníkov.

- Možnosť nastavenia počtu výskytov citlivých údajov. Dynamické reštrikcie nad súbormi a aplikáciami, pokiaľ je detekovaný 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.
- 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.
- Zaznamenávanie všetkých pripojených vzdialení vrátane monitorov, myší a klávesníc. Správa mobilných zariadení – MDM (Android, iOS): Správa, GPS lokalizácia, Vzdialený zámok zariadení. Vzdialené zmazanie zariadení.
- Správa aplikácií.

Osobitné požiadavky na plnenie Modul 5

- 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.
- Dodávateľ do 3 dní od nadobudnutia účinnosti 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
- Dodávateľ sa zaväzuje garantovať dostupnosť špecialistu na SAFETICA DLP riešenie v pracovnom čase 08:00 – 16:00 hod. s reakčnosťou do 4 hodín.
- Objednávateľ považuje za nevyhnutné na riadne poskytnutie plnenia predmetu zmluvy:
- a) disponovanie minimálne dvomi certifikovanými technikmi na produkt SAFETICA DLP,
- ISO/IEC 27001 (systém manažérstva informačnej bezpečnosti).

Modul 6. Nasadenie zálohovania

Nasadenie zálohovania na osobitnom zálohovacom serveri:

- Obstaranie SW a HW riešenia a licencií
- Implementácia zálohovacieho systému
- Analýza zálohovacích boxov a pravidiel
- Nasadenie obnovy záloh

• Zaškolenie personálu Prevádzkovateľa

Minimálne parametre zálohovacieho systému:

- RackStation 2,2GHz, 4GBRAM, 8xSATA, 2xUSB3.0
- záruka 5 rokov
- kapacita 12TB SATA, 6Gb/s, 256MB cache, 7200 ot.
- čítanie / zápis dát min.: 2300 / 1100 MB/s
- podpora sieťových kariet 10GbE SFP+/RJ-45 a 25GbE SFP28
- redundantný zdroj napájania
- technická a systémová podpora 8/5.

Riešenie musí obsahovať:

pokročilú technológiu vytvárania snímkou zaisťujúcu plánovateľnú a temer okamžitú ochranu dát zdieľaných zložiek a jednotiek LUN

- obnovu dát na úrovni súborov a zložiek s obnovením konkrétnych súborov alebo zložiek
- flexibilný systém kvóty pre zálohy
- automatické opravy súborov napr. pomocou zrkadlených metadát a konfiguráciou RAID
- vloženú komprimáciu dát pred zápisom na disk
- možnosť integrácie s ľubovoľnou virtualizačnou platformou
- zálohovanie bez licencií určených k ochrane počítačov a serverov so systémom Windows,
- virtuálnych počítačov, ďalších súborových serverov a cloudových aplikácií
- konsolidáciu úloh zálohovania pre fyzické i virtuálne prostredie s možnosťou rýchleho obnovenia súborov, celých fyzických počítačov a virtuálnych počítačov.
- zálohovanie v prostredí Google Workspace, Gmail, kontaktov, kalendárov a služby Drive zálohovanie dát sady Microsoft 365, OneDrive for Business, SharePoint Online, e-mailov, kontaktov a kalendárov.

Príloha č.2 - Cenová ponuka

PRIESKUM TRHU	
Názov žiadateľa:	Mesto Revúca
Sídlo:	Námestie slobody 13/17, 050 80 Revúca
IČO:	00328693
Kontaktná osoba:	Martin Huraj, projektový manažér
Telefón:	0905 347 191
E-mail:	huraj@cns-e.eu
Názov projektu:	Zvýšenie kybernetickej bezpečnosti mesta Revúca

Opis predmetu zákazky

Predmetom zákazky je dodanie riešenia, ktorého cieľom je zvýšiť kybernetickú bezpečnosť mesta a vytvoriť efektívny a trvalo udržateľný systém informačnej a kybernetickej bezpečnosti. Predmet zákazky je rozdelený na 6 modulov:

1. Nasadenie informačného systému 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
2. Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)
3. Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti
4. Zriadenie SOC ako služby v prevádzke 24/7
5. Nasadenie DLP
6. Nasadenie zálohovania

Spôsob stanovenia ceny

Nacenenie každého modulu sa skladá zo stanovenia cien pracovných pozícií pre aktivity Analýza a Dizajn, Implementácia a Testovanie, Nasadenie, stanovenia cien na nákup technických prostriedkov, programových prostriedkov a služieb a stanovenia cien za služby súvisiace s prevádzkou modulu. **Prosím o vyplnenie všetkých žlto podfarbených častí v hárku Cenova-ponuka.** Stanovenie cien pracovných pozícií obsahuje informatívne stĺpce *Sadzba - revizia výdavkov bez DPH* a *Max sadzba bez DPH prirucka OP II*, ktoré stanovujú odporúčanú a maximálnu sumu na danú pozíciu v súlade s odporúčaniami MIRRI.

Spôsob predloženia cenovej ponuky

Za účelom jednoduchšieho vyhodnotenia Vás prosím o zaslanie cenovej ponuky vo formáte excel (.xls a pod) na e-mailovú adresu huraj@cns-e.eu najneskôr do 6.5.2022 10:00.

Podrobné informácie k predmetu zákazky

Modul 1.	**Nasadenie informačného systému 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**
Zoznam funkčných vlastností:	• 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.
Užívateľské rozhranie a výstupy:	• Pre interakciu s používateľom musí byť k dispozícii webové rozhranie bez špeciálnych nárokov na webový prehliadač • Výstupy musia byť realizované vo forme prehľadov a zostáv vo formáte PDF.
Používatelia a ich správa:	• Evidencia používateľov, oprávnených pristupovať k subjektom a identifikovať resp. manažovať ich riziká musí umožňovať širokú integráciu na existujúce systémy správy používateľov • Oprávneným používateľom musí byť možné prideliť role s rôznym stupňom oprávnení.
Spôsob nasadenia a použitia:	• Objednávateľ požaduje neobmedzenú licenciu pre jedného používateľa • Objednávateľ požaduje inštaláciu, implementáciu a zaškolenie obsluhy.
Vykonávané činnosti manažérom pre riadenie rizík prostredníctvom IS:	• Tvorba analýz rizík podľa potreby a požiadaviek manažéra informačnej bezpečnosti • Pravidelné hodnotenie a ošetrovanie rizík • Tvorba plánu eliminácie rizík • Správa aktív a ich vlastníkov • Dohľad nad riadením rizík

Prostredníctvom IS musí byť možnosť vykonávať revízie a aktualizáciu rizikovej analýzy, riadiť riziká, aktíva, zraniteľnosti a hrozby systémom, ktorý dokumentuje históriu a je auditovateľný. Objednávateľ požadujem systém klient – server nasadený u objednávateľa na jeho serveri bez závislosti na cloudových službách a aktualizáciách cez internet.

Objednávateľ požaduje oceniť časovo neobmedzenú licenciu pre jedného používateľa, zaškolenie používateľa a výkon špecialistu na riadenie rizík (manažéra pre riadenie rizík):	• Analýzu a implementáciu softvéru • Nasadenie softvéru • Vyškolenie obsluhy • Ocenenie a definovanie počtu licencií pre min. 1 používateľa s neobmedzenou platnosťou • Ocenenie mesačnej práce špecialistu na riadenie rizík.
Modul 2.	**Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)**
Dodávateľ zadefinuje scenáre rôznych udalostí, ktoré potencionálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:	• náhla nedostupnosť personálu • náhla nepoužiteľnosť pracoviska/budovy • nedostupnosť technologickej infraštruktúry • náhla nedostupnosť médií • živelná katastrofa
Dodávateľ stanoví požiadavky na zdroje (adekvátnych finančných, materiálno-technických a personálnych zdrojov), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. V zmysle požiadaviek zákona o kybernetickej bezpečnosti musí určiť čo má byť:	• hlavným cieľom plánu kontinuity s ohľadom na riadenie incidentov v prípade katastrofy alebo iného rušivého incidentu a ako sa obnovia činnosti v stanovených termínoch. Cieľom tohto plánu je udržať škodu spôsobenú rušivým incidentom na prijateľnej úrovni, • strategickým imperatívom procesu riadenia kontinuitu s ohľadom na predchádzanie ďalších strát a vplyv prostredia.
Dodávateľ vypracuje analýzu funkčných dopadov a kvalifikuje potencionálne dopady a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Požiadavkou analýzy funkčného dopadu je určenie:	• cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb, • cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby. Jedná sa o identifikáciu tolerovanej doby pre obnovenie činnosti na prijateľnej úrovni a identifikáciu maximálne prijateľného množstva straty údajov merané v čase – cieľového bodu obnovenia.
Dodávateľ zavedie postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujúce najmenej:	a) frekvenciu a rozsah jej dokumentovania a schvaľovania, b) určenie osoby zodpovednej za zálohovanie, c) časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní, d) požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom, e) požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené, f) požiadavku navykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.
Dodávateľ vypracuje plán pravidelného preverenia záloh, testovania obnovy záloh a precvičovania zavedených krízových plánov najmenej raz ročne.	
Dodávateľ vypracuje alebo zabezpečí vypracovanie nim.:	• plán kontinuity na stanovenie požiadaviek a zdrojov, • plán reakcie na incidenty, • politiku a ciele kontinuity, • analýzu funkčných dopadov, • stratégiu riadenia kontinuity vrátane evakuačný postupov, • plány havarijnej obnovy prevádzky, • plán údržby a kontroly BCMS.
Dodávateľ bude pre objednávateľa zabezpečovať rolu manažéra riadenia kontinuity s úlohami:	a) riadenie incidentov v prípade katastrofy, b) riadenie incidentov v prípade rušivého incidentu, c) analýza dopadu, d) realizácia a výkon interných auditov, e) precvičovanie zavedených krízových plánov, f) aktualizácia plánov reakcie na incidenty, g) aktualizácia plánov obnovy po katastrofe, h) návrh opatrení riadenia kontinuity, i) monitorovanie zariadení podstatných pre prípadný vznik incidentu.
Modul 3.	**Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti**

Musí byť pokryté monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb podľa nakonfigurovaných pravidiel. Monitorovací nástroj musí informovať o vzniknutých technických problémoch a nedostatku kapacít správcu príslušnej služby alebo servera. Musí byť schopný monitorovať rôzne druhy zariadení ako sú fyzické a virtuálne servery, sieťové prvky, dátové úložiská a iné zariadenia, ktoré dokážu poskytnúť údaje o svojej prevádzke. Monitoring musí byť v reálnom čase s možnosťou údaje okamžite vizualizovať prostredníctvom grafov, máp a rôznych náhľadov. Musí byť schopný porovnávať dáta v rôznych časových obdobiach, analyzovať históriu.

Funkčné požiadavky:	• Monitorovanie kľúčových informačných systémov a ich jednotlivých komponentov • Nastavenie prahových hodnôt alertov a notifikácií • Eskalácia notifikácií • Tvorba reportov • Tvorba vlastných sledovacích schém.
Do monitoringu bude zahrnutých 10 zariadení a služieb, komponentov infraštruktúry z množiny:	• Sieťových a výkonových zariadení • VMware služieb • Databázových a zálohovacích zariadení • Webových služieb • Kritického hardvéru.
Zber údajov musí podporovať:	• Agentov SNMP a IPM • Bezagentový a špeciálny monitoring • Monitoring virtuálnych zariadení • Webové aplikácie a Java scenáre • Monitoring databáz • Kalkulované a agregované položky • Interné sledovanie výkonu.
Musí byť podporovaná vizualizácia vo webovom rozhraní a informovanosť v rozsahu:	• Grafov a máp so zloženými pohľadmi • Globálnych Dashboardov • Prístupu k získaným hodnotám a zoznamu udalostí • Zasielania oznámení • Potvrdenia a eskalácie prijatých informácií • Schopnosti prijať opatrenia.

Systém musí byť schopný automatizácie, napr. cez Network alebo Low-level discovery. Musí byť schopný správy aj cez smartfón, schopný nasadenia vlastných skriptov s prístupom k funkciám cez API. Musia sa dať definovať pravidlá hodnotenia údajov poskytujúce logické definície stavu zariadení.

Modul 4.	**Zriadenie SOC ako služby v prevádzke 24/7**
Služby súvisiace s dohľadovým centrom bezpečnostných incidentov – SOC (Security Operations Center) musia zahŕňať:	• zber udalostí v sieťach a kritických prvkoch informačných systémov v režime 24 x 7, • monitorovanie a analyzovanie udalostí v sieťach a kritických prvkoch informačných systémov v režime 8 x 5 – proaktívny monitoring, • nepretržitú detekciu kybernetico-bezpečnostných incidentov, • zber relevantných informácií pri zistených kybernetických incidentoch, • návrh riešenia kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov, • vyhodnocovanie riešenia kybernetických incidentov a návrh systémových opatrení s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov, • podrobnú evidenciu bezpečnostných incidentov, ich riešení a príslušnej komunikácie prostredníctvom na to určeného nástroja (ticketing/service desk), • dohľad nad celým životným cyklom bezpečnostných udalostí a incidentov, • pravidelný reporting (1 x mesačne)
Sondu pre zber dát požadujeme – virtuálne zariadenie. Súčasťou dodávky zariadenia je jeho inštalácia a implementácia v rozsahu:	• inštalácia funkcionality zbierania záznamov z prevádzky Informačných systémov, • zabezpečenie a sprevádzkovanie sieťovej konektivity, • konfigurácia systémov SOC s ohľadom na špecifickosť prostredia.

Vyžadované SLA parametre sú:

	Garantovaný čas odozvy
Incident kategórie HIGH - vysoko nebezpečné incidenty, ktoré môžu spôsobiť vážne škody, môžu mať negatívny dopad na kritické aktíva.	maximálne 2 hodiny
Incident kategórie MEDIUM - incidenty strednej závažnosti, t.j. ktoré akútne neohrozujú kritické časti prostredia.	maximálne 4 hodiny
Incident kategórie LOW - incidenty nízkej závažnosti bez priameho negatívneho vplyvu na kontinuitu služby.	maximálne 8 hodín

Zoznam kategórií bezpečnostných incidentov:

Kategória	*Subkategória*	*SLA priority*
	Nevyžiadaná pošta	LOW
	Obťažovanie	LOW
	Vyhrážanie	LOW
	Potláčanie práv a slobôd	LOW
Škodlivý kód	Vírus, červ, Trójsky kôň	MEDIUM
Získavanie	Skenovanie siete	MEDIUM
	Odpočúvanie	MEDIUM
	Sociálne inžinierstvo	MEDIUM
Pokus o prienik	Využitie známej zraniteľnosti	MEDIUM
	Opakované pokusy o prihlásenie	MEDIUM
	Útok s neznámymi znakmi	MEDIUM
Podozrenie na úspešný prienik do systému	Skompromitovanie privilegovaného účtu	HIGH
	Skompromitovanie obmedzeného účtu	HIGH
	Skompromitovanie aplikácie	HIGH
	Botnet	HIGH

	Nedostupnosť	DoS, DDoS	MEDIUM
		Sabotáž	MEDIUM
	Ohrozenie	Neoprávnený prístup k informáciám	MEDIUM
	bezpečnosti Informácii	Neoprávnená zmena Informácii	MEDIUM
	Podvod	Neoprávnené využívanie	MEDIUM
		Porušenie autorských práv	MEDIUM
		Prevzatie identity	MEDIUM
		Phishing	MEDIUM
	Iné		LOW

Monitorované zariadenia	Popis	Typ zariadenia/názov produktu	Počet	Proaktívny monitoring
	Firewall	Fortigate 60E	1	8 x 5
	virtuálny server pre informačný systém samosprávy	MS Windows 2012 R2	1	8 x 5
	virtuálny server pre zálohovanie	MS Windows 2012 R2	1	8 x 5
	Domain Controler(Active Directory)	MS Windows 2012 R2	2	8 x 5
	virtuálny server pre zverejňovanie na egov.revuca.sk	MS Windows 2012 R2	1	8 x 5

Modul 5. **Nasadenie DLP**

Nasadenie DLP ako služby je rozdelené do nasledovných krokov:

- Obstaranie SW riešenia a licencií
- Zavedenie DLP do testovaco adaptačnej prevádzky
- Analýza pracovných procesov a dátových tokov a definovanie detekčných pravidiel
- Optimalizácia detekčných pravidiel
- Nasadenie DLP na 60 ks pracovných staníc ako produkčný zdroj informácií pre SOC
- Zaškolenie personálu Prevádzkovateľa

Súčasťou riešenia musí byť aj celkový report zistení s návrhom opatrení.

Požiadavky na systém DLP:

Integrácia s MS Active Directory, podpora pre MS SQL 2012 alebo novšia, podpora operačných systémov Windows 8.1, 10,11. podpora serverových operačných systémov Windows Server 2012, 2016 a vyšších, podpora terminálových prostredí, centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni OU domény, riadené užívateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia, skrytý režim na koncovej stanici vrátane procesov, zložiek a lokálnych i doménových administrátorov.

Ochrana proti: zastaveniu systému a procesov, odinštalovaniu riešenia bez potrebnej autorizácie, editácii registrov, systémových komponentov či DLL knižníc, zmene nastavenia na koncovej stanici. Nutná je možnosť ochrany i u operačného systému v režime "safe mode".
Funkcionality zachované i v off-line móde, (ak koncová stanica nie je pripojená k firemnej sieti/ internetu). Možnosť pracovať s historickými dátami. Riešenie musí podporovať možnosť poskytnúť zálohovanie vlastných komponentv, prevažne všetkých záznamov a nastavení. Automatické generovanie emailových varovaní v prípade incidentov, možnosť zmeniť citlivosť a špecifikáciu incidentu. Automatické generovanie emailových reportov s možnosťou úprav obsahu (množstvo informácii, množina uzlov, frekvencie odosielanie, príjemcovia). Zasielanie logov do SIEM riešenia objednávateľa.

Systém musí poskytovať detailné informácie o aplikáciách, ako čas spustenia a ich aktívneho využitia, rozdelenie do kategórií, detailné informácie o weboch s rozdelením do kategórií - ako ich aktívne využitie, informácie o URL, použitom protokole, hlavičky webu, a to bez ohľadu na použitý prehliadač.
Detailné informácie o práci so súbormi, ako prehľad užívateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové). 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 tlačených úloh a možnosť exportu reportov do XLS, PDF.

Systém musí zaznamenávať komunikácie: Podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania,Podpora desktopových emailových klientov (Microsoft Outlook, Mozilla Thunderbird,...), zaznamenávať emaily nezávisle od použitej aplikácie, zaznamenávať súbory odoslané cez web mailových klientov a cez IM komunikačné nástroje. Zaznamenávať Office 365 cloud: zaznamenávať bežné užívateľské akcie prevedené na Office 365 cloude (OneDrive for Business, SharePoint Online) - základné súborové operácie ako sťahovanie a zdieľanie, zaznamenávanie Office 365 emailovej komunikácie (Exchange Online) pre všetkých užívateľov vrátane užívateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.

Systém musí mať možnosť definície kategórií citlivých dát, obmedzenia pohybu a práce s týmito dátami, na ktoré emailové adresy môžu byť dáta odoslané, ktoré aplikácie môžu s dátami pracovať. Možnosť aplikácie politík pre konkrétne aplikácie – definícia zdroja a cieľa (prístup na externé zariadenie, sieť, tlač, virtuálnu tlač) a správa užívateľských operácií (použitie schránky, snímanie obrazovky). Možnosť správy nepovolených cloudových úložísk.

Možnosť úplne blokovať užívateľské akcie, informatívna notifikácia užívateľa či samotné logovanie užívateľských akcií, ochrana citlivých dát, možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov. Možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov. Možnosť importu vlastných slovníkov. Možnosť nastavenia počtu výskytov citlivých údajov. Dynamické reštrikcie nad súbormi a aplikáciami, pokiaľ je detekovaný citlivý obsah.

Musí byť možnosť blokácie 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. Detekcia dát obsahujúcich citlivý obsah, uložených na koncovej stanici alebo na zdieľanom sieťovom disku. Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.

	Musí mať možnosť reštrikcie pre USB zariadenia, pamäťové karty, Bluetooth zariadenia, optické disky či FireWire. Možnosť vynútenia režimu iba na čítanie u pripojených zariadení. Zaznamenávanie všetkých pripojených vzdialení vrátane monitorov, myší a klávesníc. Správa mobilných zariadení – MDM (Android, iOS): správa, GPS lokalizácia, vzdialený zámok zariadení. Vzdialené zmazanie zariadení. Správa aplikácií.
Modul 6.	**Nasadenie zálohovania**
Nasadenie zálohovania na osobitnom zálohovacom serveri:	• Obstaranie SW a HW riešenia a licencií • Implementácia zálohovacieho systému • Analýza zálohovacích boxov a pravidiel • Nasadenie obnovy záloh • Zaškolenie personálu Prevádzkovateľa
Minimálne parametre zálohovacieho systému:	• RackStation 2,2GHz, 4GBRAM, 8xSATA, 2xUSB3.0 • záruka 5 rokov • kapacita 12TB SATA, 6Gb/s, 256MB cache, 7200 ot. • čítanie / zápis dát min.: 2300 / 1100 MB/s • podpora sieťových kariet 10GbE SFP+/RJ-45 a 25GbE SFP28 • redundantný zdroj napájania • technická a systémová podpora 8/5.
Riešenie musí obsahovať:	pokročilú technológiu vytvárania snímkou zaisťujúcu plánovateľnú a temer okamžitú ochranu dát zdieľaných zložiek a jednotiek LUN • obnovu dát na úrovni súborov a zložiek s obnovením konkrétnych súborov alebo zložiek • flexibilný systém kvóty pre zálohy • automatické opravy súborov napr. pomocou zrkadlených metadát a konfiguráciou RAID • vloženú komprimáciu dát pred zápisom na disk • možnosť integrácie s ľubovoľnou virtualizačnou platformou • zálohovanie bez licencií určených k ochrane počítačov a serverov so systémom Windows, virtuálnych počítačov, ďalších súborových serverov a cloudových aplikácií • konsolidáciu úloh zálohovania pre fyzické i virtuálne prostredie s možnosťou rýchleho obnovenia súborov, celých fyzických počítačov a virtuálnych počítačov. • zálohovanie v prostredí Google Workspace, Gmail, kontaktov, kalendárov a služby Drive • zálohovanie dát sady Microsoft 365, OneDrive for Business, SharePoint Online, e-mailov, kontaktov a kalendárov.

*Koniec dokumentu

PRIESKUM TRHU

Názov žiadateľa:	Mesto Revúca
Sídlo:	Námestie slobody 13/17, 050 80 Revúca
IČO:	00328693
Kontaktná osoba:	Július Emek, osoba poverená VO manažér
Telefón:	0902374738
E-mail:	julius.ernekii@gmail.com
Názov projektu:	Zvýšenie kybernetickej bezpečnosti mesta Revúca

Obchodné meno:	void SOC, s.r.o.
Sídlo:	Plynárenská 5, 829 75 Bratislava
IČO:	35 955 678
Kontaktná osoba:	Michal Šimkovič
Telefón:	+421 901 904 643
E-mail:	Michal.Simkovic@voidsoc.com
Platca DPH (áno/nie):	áno
Dátum vypracovania ponuky:	19.1.2023

Čestne prehlasujem, že návrh cenovej ponuky napĺňa jednotlivé parametre, charakteristiky a požiadavky špecifikácie stanovené žiadateľom v plnom rozsahu.
Návrh cenovej ponuky zodpovedá cenám obvyklým v danom mieste a čase.

Meno osoby, ktorá vypracovala ponuku Martin Lohnert

Stanovenie cien pracovných pozícií

Pozícia	Navrhovaná sadzba bez DPH v EUR	Sadzba - revízia výdavkov bez DPH	Max sadzba bez DPH prirucka OP II	Max % v projekte na HA	V projekte	% v projekte
IT architekt	450 €	500 €	910 €	10,00%	3	1,76%
IT tester	380 €	380 €	570 €	15,00%	25	14,71%
IT programátor/vývojár	380 €	400 €	650 €	60,00%	41	24,12%
Projektový manažér IT projektu	500 €	500 €	890 €	4,00%	1	0,59%
IT analytik	400 €	450 €	740 €	50,00%	55	32,35%
Odborník pre IT dohľad/Quality Assurance		644 €	890 €	5,00%	0	0,00%
Špecialista pre bezpečnosť IT	550 €	619 €	1 200 €	10,00%	2	1,18%
Špecialista pre infraštruktúry/HW špecialista	450 €	450 €	790 €	30,00%	10	5,88%
Špecialista pre databázy		464 €	600 €	15,00%	0	0,00%
Školiteľ pre IT systémy		400 €	710 €	5,00%	0	0,00%
IT/IS konzultant (napr. SAP)		448 €	900 €	50,00%	0	0,00%
Iné	550 €	560 €	570 €	20,00%	33	19,41%

Modul 1.	Nasadenie informačného systému 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	
	Spolu	27 500 €

Analýza a Dizajn	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €	2	760 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	4	1 600 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Špecialista na riadenie rizík	550 €	2	1 100 €
	Spolu		**8**	**3 460 €**

Nákup technických prostriedkov, programových prostriedkov a služieb	Položka	JC bez DPH v EUR	Počet ks	Cena spolu bez DPH v EUR
	Licencia s neobmedzenou platnosťou	5 000 €	1	5 000 €
			0	0 €
	Spolu		**1**	**5 000 €**

Implementácia a Testovanie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	4	1 520 €
	IT programátor/vývojár	380 €	8	3 040 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	10	4 000 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Špecialista na riadenie rizík	550 €	8	4 400 €
	Spolu		**30**	**12 960 €**

Nasadenie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	4	1 520 €
	IT programátor/vývojár	380 €	2	760 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	4	1 600 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Špecialista na riadenie rizík	550 €	4	2 200 €
	Spolu		**14**	**6 080 €**

Služby súvisiace s prevádzkou modulu	Položka	JC za mesiac bez DPH v EUR	Počet mesiacov	Cena spolu bez DPH v EUR
	Neaplikuje sa			0 €
			0	0 €
	Spolu		**0**	**0 €**

Modul 2.	Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)	
	Spolu	28 810 €

Analýza a Dizajn	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €	3	1 350 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €	4	1 520 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	4	1 600 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €	2	900 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Manažér riadenia kontinuity	550 €	4	2 200 €
	Spolu		**17**	**7 570 €**

Nákup technických prostriedkov, programových prostriedkov a služieb	Položka	JC bez DPH v EUR	Počet ks	Cena spolu bez DPH v EUR
	Neaplikuje sa			0 €
				0 €
	Spolu		**0**	**0 €**

Implementácia a Testovanie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	4	1 520 €
	IT programátor/vývojár	380 €	10	3 800 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	13	5 200 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €	2	1 100 €
	Špecialista pre infraštruktúry/HW špecialista	450 €	2	900 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Manažér riadenia kontinuity	550 €	7	3 850 €
	Spolu		**38**	**16 370 €**

Nasadenie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	2	760 €
	IT programátor/vývojár	380 €	2	760 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	2	800 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €	2	900 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Manažér riadenia kontinuity	550 €	3	1 650 €
	Spolu		**11**	**4 870 €**

Služby súvisiace s prevádzkou modulu	Položka	JC za mesiac bez DPH v EUR	Počet mesiacov	Cena spolu bez DPH v EUR
	Neaplikuje sa			0 €
				0 €
	Spolu		**0**	**0 €**

Modul 3.	**Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti**	
	Spolu	7 420 €

Analýza a Dizajn	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €	1	380 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	1	400 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		**2**	**780 €**

Nákup technických prostriedkov, programových prostriedkov a služieb	Položka	JC bez DPH v EUR	Počet ks	Cena spolu bez DPH v EUR
	Licencia s neobmedzenou platnosťou	2 000 €	1	2 000 €
				0 €
	Spolu		**1**	**2 000 €**

Implementácia a Testovanie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	2	760 €
	IT programátor/vývojár	380 €	3	1 140 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	3	1 200 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		**8**	**3 100 €**

Nasadenie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	2	760 €
	IT programátor/vývojár	380 €	1	380 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	1	400 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		**4**	**1 540 €**

Služby súvisiace s prevádzkou modulu	Položka	JC za mesiac bez DPH v EUR	Počet mesiacov	Cena spolu bez DPH v EUR
	Neaplikuje sa			0 €
				0 €
	Spolu		**0**	**0 €**

Modul 4.	Zriadenie SOC ako služby v prevádzke 24/7	
	Spolu	22 630 €

Analýza a Dizajn	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €		0 €
	Projektový manažér IT projektu	500 €	1	500 €
	IT analytik	400 €	1	400 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Manažér pre správu IT zariadení	550 €	1	550 €
	Spolu		**3**	**1 450 €**

Nákup technických prostriedkov, programových prostriedkov a služieb	Položka	JC bez DPH v EUR	Počet ks	Cena spolu bez DPH v EUR
	Licencia Virtuálna sonda	3 000 €	1	3 000 €
			0	0 €
	Spolu		**1**	**3 000 €**

Implementáda a Testovanie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	3	1 140 €
	IT programátor/vývojár	380 €	3	1 140 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	2	800 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Manažér pre správu IT zariadení	550 €	2	1 100 €
	Spolu		**10**	**4 180 €**

Nasadenie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	2	760 €
	IT programátor/vývojár	380 €	1	380 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €		0 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné - Manažér pre správu IT zariadení	550 €	2	1 100 €
	Spolu		**5**	**2 240 €**

Služby súvislace s prevádzkou modulu	Položka	JC za mesiac bez DPH v EUR	Počet mesiacov	Cena spolu bez DPH v EUR
	Služba poskytovania SOC	980 €	12	11 760 €
			0	0 €
	Spolu		**12**	**11 760 €**

Modul 5.	**Nasadenie DLP**	
	Spolu	10 880 €

Analýza a Dizajn	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €		0 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	2	800 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		2	**800 €**

Nákup technických prostriedkov, programových prostriedkov a služieb	Položka	JC bez DPH v EUR	Počet ks	Cena spolu bez DPH v EUR
	Licencia	75 €	60	4 500 €
				0 €
	Spolu		60	**4 500 €**

Implementácia a Testovanie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €	2	760 €
	IT programátor/vývojár	380 €	4	1 520 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	4	1 600 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €	2	900 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		12	**4 780 €**

Nasadenie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €		0 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	2	800 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		2	**800 €**

Služby súvisiace s prevádzkou modulu	Položka	JC za mesiac bez DPH v EUR	Počet mesiacov	Cena spolu bez DPH v EUR
	Neaplikuje sa			0 €
				0 €
	Spolu		0	**0 €**

Modul 6.	Nasadenie zálohovania	
	Spolu	5 200 €

Analýza a Dizajn	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €		0 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	1	400 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €	1	450 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €	0	0 €
	Spolu		**2**	**850 €**

Nákup technických prostriedkov, programových prostriedkov a služieb	Položka	JC bez DPH v EUR	Počet ks	Cena spolu bez DPH v EUR
	Server na zálohovanie	3 500 €	1	3 500 €
			0	0 €
	Spolu		**1**	**3 500 €**

Implementácia a Testovanie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €		0 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €	1	400 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €	1	450 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		**2**	**850 €**

Nasadenie	Pozícia	Suma za 1 ČD bez DPH v EUR	Počet ČD	Cena spolu bez DPH v EUR
	IT architekt	450 €		0 €
	IT tester	380 €		0 €
	IT programátor/vývojár	380 €		0 €
	Projektový manažér IT projektu	500 €		0 €
	IT analytik	400 €		0 €
	Odborník pre IT dohľad/Quality Assurance	0 €		0 €
	Špecialista pre bezpečnosť IT	550 €		0 €
	Špecialista pre infraštruktúry/HW špecialista	450 €		0 €
	Špecialista pre databázy	0 €		0 €
	Školiteľ pre IT systémy	0 €		0 €
	IT/IS konzultant (napr. SAP)	0 €		0 €
	Iné	550 €		0 €
	Spolu		**0**	**0 €**

Služby súvisiace s prevádzkou modulu	Položka	JC za mesiac bez DPH v EUR	Počet mesiacov	Cena spolu bez DPH v EUR
	Neaplikuje sa			0 €
				0 €
	Spolu		**0**	**0 €**

	Celková cena bez DPH v EUR za riešenie	
	Spolu	**102 440 €**

Príloha 3 - Presná špecifikácia ceny:

Č.	Názov modulu	Cena bez DPH
Modul 1.	**Nasadenie informačného systému 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**	27 500 €
Modul 2.	**Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)**	28 810 €
Modul 3.	**Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti**	7 420 €
Modul 4.	**Zriadenie SOC ako služby v prevádzke 24/7**	22 630 €
Modul 5.	**Nasadenie DLP**	10 880 €
Modul 6.	**Nasadenie zálohovania**	5 200 €
	Celková cena bez DPH v EUR za riešenie	**102 440 €**