Zmluva č. 2/KB/2023

uzatvorená podľa §269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov (ďalej v texte tiež ako „ObZ") a podľa zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov (ďalej v texte tiež ako „zákon o verejnom obstarávaní")
(ďalej len „Zmluva")

medzi zmluvnými stranami:

Zmluvné strany:

Odberateľ: **Nemocnica Snina, s.r.o.**
Sládkovičova 300/3, 069 01 Snina

v mene odberateľa:

Konateľ spoločnosti:	MUDr. Andrej Kulan
IČO:	365 09 108
DIČ:	2022075770
IČ DPH:	SK2022075770
Bankové spojenie:	VÚB a.s., Snina
IBAN:	SK34 0200 0000 0020 7759 9655

(ďalej len „Odberateľ")

a

Dodávateľ: **TÜV SÜD Slovakia s.r.o.**
Jašíkova 6, 821 03 Bratislava

V mene dodávateľa:

Štatutárny zástupca:	Ing. Branislav Chmel
IČO:	35852216
DIČ:	2020263674
Bankové spojenie:	UniCredit Bank Czech Republic and Slovakia, a.s.
IBAN:	SK15 1111 0000 0010 9250 9000

(ďalej ako „Dodávateľ")

(Odberateľ a Dodávateľ spolu ďalej aj ako „**Zmluvné strany**")

I. PREAMBULA

1.1. Zmluvné strany uzatvárajú túto Zmluvu na základe víťaznej ponuky Dodávateľa v rámci procesu verejného obstarávateľa (v Zmluve uvedeného ako **Odberateľ**) na obstaranie predmetu zákazky: **„Dodávka systému SIEM a NAS vrátane inštalačných a konfiguračných prác“.**

1.2. Odberateľ je Prijímateľom v projekte **Rozšírenie spôsobilosti Nemocnice Snina v oblasti informačnej a kybernetickej bezpečnosti**, kód projektu v ITMS2014+: **311071CBW6 číslo zmluvy: 3213/2022 .**

1.3. Zmluvné strany vyhlasujú, že údaje v časti Zmluvné strany sú pravdivé a aktuálne a zaväzujú sa vzájomne, bez meškania oznámiť obchodnému partnerovi každú zmenu, ktorá by mohla mať vplyv na plnenie zmluvných záväzkov.

1.4. Odberateľ je v zmysle § 17 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov prevádzkovateľom základnej služby. Uzatvorením tejto zmluvy Dodávateľ berie na vedomie, že uzatvára zmluvu so subjektom, ktorý je zaradený do zoznamu základných služieb a jej prevádzkovateľ do registra prevádzkovateľov základných služieb, z čoho pre zmluvné strany vyplývajú práva a povinnosti.

II. PREDMET ZMLUVY

2.1. Predmetom tejto Zmluvy je záväzok Dodávateľa dodať a nakonfigurovať SIEM a NAS riešenie (systém) pre vyhľadávanie hrozieb, monitoring kybernetickej bezpečnosti, správu protokolov a riadenie bezpečnostných udalostí, (súčasťou dodávky je implementácia hardvéru vrátane inštalačných, konfiguračných a testovacích prác podľa špecifikácie v prílohe č. 1 tejto Zmluvy, (ďalej v texte tiež ako „predmet zmluvy“ alebo „systém“), na miesto určené Odberateľom.

2.2. Dodávateľ sa zaväzuje, že za podmienok dohodnutých v tejto Zmluve Odberateľovi dodá predmet zmluvy uvedený v bode 1 tohto článku a na Odberateľa prevedie vlastníctvo predmetu zmluvy. Odberateľ sa Dodávateľovi zaväzuje zaplatiť zmluvnú cenu uvedenú v čl. IV ods. 4.1 tejto Zmluvy.

2.3. Zmluvné strany sa dohodli, že pri dodaní systému vrátane inštalačných a konfiguračných prác si budú poskytovať potrebnú súčinnosť tak, aby prispeli k riadnemu a včasnému plneniu povinností vyplývajúcich z tejto Zmluvy. Poskytnutím súčinnosti v zmysle tejto Zmluvy sa rozumie najmä bezodkladná relevantná reakcia na oprávnené požiadavky druhej Zmluvnej strany prostredníctvom osobných konzultácií (elektronicky alebo písomne), a to spôsobom a v rozsahu potrebnom na dodanie predmetu zmluvy. V prípade, ak z povahy danej súčinnosti nevyplýva kratšia lehota, súčinnosť je Zmluvná strana povinná poskytnúť najneskôr do 3 (troch) pracovných dní odo dňa obdržania požiadavky na poskytnutie súčinnosti.

III. DODACIE PODMIENKY, TERMÍN A MIESTO DODANIA

3.1. Dodávateľ sa zaväzuje dodať Odberateľovi predmet zmluvy podľa čl. II tejto Zmluvy do 90 kalendárnych dní odo dňa vystavenia objednávky Odberateľom, pričom objednávka bude vystavená v súlade s touto Zmluvou.

3.2. Dodávateľ je povinný predmet zmluvy definovaný v čl. II Zmluvy Odberateľovi dodať na miesto plnenia Zmluvy, ktorým je sídlo Odberateľa.

3.3. Predmet Zmluvy sa považuje za dodaný podpísaním akceptačného protokolu, ktorým bude potvrdené odovzdanie a prevzatie predmetu.

3.4. Zodpovedným zástupcom Odberateľa na prevzatie predmetu zmluvy a na podpísanie akceptačného a preberacieho protokolu je:

Ing. Igor Kirňák

Akceptačný a preberací protokol bude vyhotovený v troch originálach, pričom jeden bude tvoriť prílohu faktúry (daňového dokladu).

3.5. Dopravu predmetu zmluvy na miesto dodania zabezpečuje Dodávateľ na vlastné náklady tak, aby bola zabezpečená jeho dostatočná ochrana.

3.6. V prípade omeškania Dodávateľa s povinnosťou dodať predmet zmluvy v termíne v zmysle bodu 1 tohto článku je Odberateľ oprávnený uplatniť si voči Dodávateľovi zmluvnú pokutu vo výške 0,05 % zo zmluvnej ceny nedodaného systému za každý aj začatý deň omeškania, pričom právo Odberateľa na náhradu škody nie je dotknuté.

3.7. Ak Dodávateľ nedodá Odberateľovi systém v dohodnutej lehote podľa ods. 3.1 tohto článku, takéto konanie sa považuje za závažné porušenie zmluvných podmienok a oprávňuje Odberateľa odstúpiť od Zmluvy.

3.8. Odberateľ si vyhradzuje právo odmietnuť prevziať systém, ak systém svojimi vlastnosťami, resp. kvalitou, špecifikáciou nezodpovedá systému deklarovaného Dodávateľom pri podpise tejto Zmluvy.

IV. CENA

4.1. Odberateľ a Dodávateľ sa na základe víťaznej ponuky Dodávateľa v rámci postupu verejného obstarávania, a v súlade so zákonom č. 18/1996 Z. z. o cenách, v znení neskorších predpisov dohodli na cene za predmet zmluvy vo výške:

Cena bez DPH	62 981,68 EUR
Suma DPH	12 596,34 EUR
Cena s DPH	75 578,02 EUR

Cena je konečná a zahŕňa všetky náklady Dodávateľa spojené s plnením Predmetu zmluvy podľa článku II. tejto Zmluvy.
Cena za jednotlivé časti predmetu zmluvy je bližšie špecifikovaná v Prílohe č. 3

4.2. Odberateľ uhradí Dodávateľovi zmluvnú cenu po riadnom dodaní systému zo strany Dodávateľa v zmysle článku II ods. 1 tejto Zmluvy formou bezhotovostného platobného styku, bez poskytnutia preddavku. Dodávateľ je povinný vystaviť faktúru za dodávku systému najneskôr 15 dní od podpísania akceptačného a preberacieho protokolu. Zmluvnú cena bude Odberateľom uhradená na základe predloženej faktúry vystavenej Dodávateľom, s lehotou splatnosti 60 kalendárnych dní odo dňa jej doručenia Odberateľovi. Faktúra musí obsahovať náležitosti v zmysle § 71 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, odkaz na zmluvu, na základe ktorej je vystavená, fakturované sumy zaokrúhlene na 2 (dve) desatinné miesta, ITMS2014+ kód projektu, ďalšie náležitosti, ktoré Odberateľ oznámi Dodávateľovi kedykoľvek počas účinnosti tejto Zmluvy v nadväznosti na financovanie predmetu

zmluvy z prostriedkov EÚ. V prípade, že faktúra nebude obsahovať všetky uvedené náležitosti, alebo bude obsahovať chybné údaje, je Odberateľ oprávnený vrátiť ju Dodávateľovi na doplnenie alebo opravu. V takomto prípade sa preruší plynutie lehoty splatnosti faktúry a nová lehota začne plynúť dňom nasledujúcim po dni doručenia opravenej alebo doplnenej faktúry Odberateľovi.

4.3. Odberateľ uhradí Dodávateľovi zmluvnú cenu vykonaním platby na bankový účet Dodávateľa uvedený v záhlaví tejto Zmluvy.

4.4. Zmluvné strany sa dohodli, že Dodávateľ nie je oprávnený postúpiť akékoľvek pohľadávky voči Odberateľovi vyplývajúce z tejto Zmluvy na tretiu osobu bez predchádzajúceho písomného súhlasu Odberateľa. Právny úkon, na základe ktorého Dodávateľ postúpi svoju pohľadávku voči Odberateľovi na tretiu osobu bez predchádzajúceho písomného súhlasu Odberateľa, je podľa § 39 ObZ neplatný.

V. ZÁRUČNÉ PODMIENKY A ZODPOVEDNOSŤ ZA VADY

5.1. Zmluvné strany sa dohodli, že záruka na predmet zmluvy – záručná doba je v dĺžke 24 mesiacov a začína plynúť odo dňa dodania predmetu zmluvy uvedeného v akceptačnom protokole.

5.2. Odberateľ je povinný oznámiť písomne, e-mailom na adresu: Oliver.Havrila@tuvsud.com, alebo iným spôsobom odsúhlaseným Zmluvnými stranami Dodávateľovi vady systému kedykoľvek do uplynutia záručnej doby, a to bez ohľadu na to, kedy sa Odberateľ o nich dozvedel, a bez ohľadu na to, či ide o vady skryté alebo zjavné

5.3. Zmluvné strany sa dohodli, že počas záručnej doby má Dodávateľ povinnosť bezplatne odstrániť vadu (chybu) predmetu zmluvy. V prípade, že takáto oprava nie je možná je Dodávateľ povinný nahradiť vadný systém novým systémom. Lehota na odstránenie vady je 30 kalendárnych dní od oznámenia vady, ak sa Zmluvné strany nedohodnú inak.

5.4. Dodávateľ zodpovedá za vady, ktoré má predmet zmluvy v okamihu, keď prechádza nebezpečenstvo škody na systéme na Odberateľa, aj keď sa vada stane zjavnou až po tomto čase. Dodávateľ zodpovedá taktiež za akúkoľvek vadu, ktorá vznikne po uvedenej dobe, ak je spôsobená porušením povinností Dodávateľa podľa tejto Zmluvy.

5.5. Dodávateľ je povinný pristupovať do prostredia Objednávateľa výlučne len v súlade s technickou špecifikáciou spôsobu pripojenia, ktorá zabezpečuje vysokú bezpečnosť.

5.6. Spôsob reklamácie vád systému bude prebiehať najmä telefonicky a písomne prostredníctvom elektronickej pošty.

VI. UKONČENIE ZMLUVY

6.1. Táto Zmluva zanikne uplynutím doby, na ktorú bola uzatvorená v zmysle čl. III tejto Zmluvy. Zmluvu je možné ukončiť písomnou dohodou Zmluvných strán alebo písomným odstúpením od Zmluvy niektorou Zmluvnou stranou.

6.2. V prípade zániku Zmluvy dohodou Zmluvných strán, táto zaniká dňom uvedeným v tejto dohode. V dohode sa upravia aj vzájomné nároky Zmluvných strán, vzniknuté z plnenia zmluvných povinností alebo z ich porušenia ku dňu zániku Zmluvy dohodou.

6.3. Ak Dodávateľ koná v rozpore s touto Zmluvou, výzvou na predkladanie ponúk, právnymi predpismi a na písomnú výzvu Odberateľa toto konanie a jeho následky v určenej lehote neodstráni, je Odberateľ oprávnený od Zmluvy odstúpiť, pričom nastávajú účinky odstúpenia od Zmluvy v zmysle § 349 a § 351 ObZ. Predchádzajúca písomná

výzva Odberateľa nie je potrebná v prípade odstúpenia od Zmluvy zo strany Odberateľa podľa bodu 6.4 tohto článku.

6.4. Odberateľ si vyhradzuje právo odstúpenia od Zmluvy aj bez predchádzajúcej písomnej výzvy, ak Dodávateľ dodá systém, ktorý nezodpovedá množstvu, akosti a kvalite dohodnutého v Zmluve a v súťažných podkladoch. Odberateľ je oprávnený od Zmluvy odstúpiť aj v prípade, ak Dodávateľ nedodá systém v lehote podľa článku III ods. 3.1 tejto Zmluvy.

6.5. Odstúpenie od Zmluvy musí mať písomnú formu a musí byť druhej Zmluvnej strane doručené. Účinky odstúpenia nastávajú dňom doručenia odstúpenia druhej Zmluvnej strane.

6.6. Za deň doručenia sa považuje deň prevzatia písomnosti. V prípade, že adresát odmietne písomnosť prevziať, za deň doručenia sa považuje deň odmietnutia prevzatia písomnosti. V prípade, že si adresát neprevezme písomnosť v úložnej lehote na pošte, za deň doručenia sa považuje posledný deň úložnej doby na pošte. V prípade, že sa písomnosť vráti odosielateľovi s označením pošty adresát neznámy alebo adresát sa odsťahoval alebo s inou poznámkou podobného významu, za deň doručenia sa považuje deň vrátenia zásielky odosielateľovi.

6.7. Dodávateľ berie na vedomie, že dokumentácia z verejného obstarávania podlieha kontrole riadiaceho orgánu a/alebo sprostredkovateľského orgánu pre Operačný program Integrovaná infraštruktúra. Dodávateľ v nadväznosti na predchádzajúcu vetu súhlasí s tým, že Odberateľ je oprávnený bez akýchkoľvek sankcií odstúpiť od Zmluvy s Dodávateľom v prípade, kedy ešte nedošlo k plneniu zo Zmluvy medzi Odberateľom a Dodávateľom a výsledky kontroly riadiaceho orgánu neumožňujú financovanie výdavkov vzniknutých z obstarávania, výsledkom ktorého je táto Zmluva.

VII. SUBDODÁVATELIA

7.1. Dodávateľ je oprávnený zabezpečiť plnenie tejto Zmluvy alebo jej častí prostredníctvom subdodávateľov v súlade s podmienkami Verejného obstarávania a touto Zmluvou. Dodávateľ zodpovedá za každé plnenie takéhoto subdodávateľa v rozsahu, ako keby plnenie poskytoval sám.

7.2. Zoznam subdodávateľov s ich identifikačnými údajmi v rozsahu: (i) meno a priezvisko alebo obchodné meno, resp. názov, (ii) adresa pobytu alebo sídlo, (iii) IČO alebo dátum narodenia, ak nebolo pridelené IČO, (iv) podiel plnenia zo Zmluvy v percentuálnom vyjadrení, ako aj údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia, tvorí neoddeliteľnú súčasť tejto Zmluvy ako Príloha č. 2. Ak to vyplýva zo zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov, musí byť subdodávateľ zapísaný v registri partnerov verejného sektora. Dodávateľ je povinný písomne oznámiť kontaktnej osobe Odberateľa akúkoľvek zmenu údajov o subdodávateľovi bezodkladne po tom, ako sa o takej zmene dozvedel.

7.3. Dodávateľ je oprávnený zmeniť alebo doplniť subdodávateľa počas trvania Zmluvy. Dodávateľ je povinný Odberateľovi najneskôr tri (3) pracovné dni pred dňom, v ktorom subdodávateľ začne poskytovať Predmet plnenia alebo jeho časť podľa tejto Zmluvy, predložiť písomné oznámenie o zmene alebo doplnení subdodávateľa, ktoré bude obsahovať údaje o navrhovanom subdodávateľovi v rozsahu podľa odstavca 7.2 tohto článku. Odberateľ má právo zmenu odmietnuť, ak nie sú splnené podmienky uvedené v tomto bode.

7.4. V prípade, že na plnenie tejto Zmluvy alebo jej častí nevyužije Dodávateľ subdodávateľov, predloží o tejto skutočnosti čestné vyhlásenie pri podpise Zmluvy.

VIII. MLČANLIVOSŤ

8.1. Za dôverné informácie sa v zmysle tejto Zmluvy a v zmysle § 271 ods. 1 ObZ považujú, bez obmedzenia, informácie akejkoľvek povahy týkajúce sa Odberateľa, vrátane informácií, ktoré boli alebo budú získané priamo či nepriamo Dodávateľom v súvislosti s realizáciou tejto Zmluvy, buď v písomnej, ústnej, elektronickej alebo inej forme, bez ohľadu na to, či sú označené ako tajné alebo dôverné, okrem iného vrátane napr. údajov, dát, podkladov, dokumentov alebo akýchkoľvek iných informácií o Odberateľovi, ako aj údajov a informácií o tretích osobách v súvislosti s realizáciou spolupráce podľa tejto Zmluvy, a to bez ohľadu na formu ich zachytenia (ďalej len „***Dôverné informácie***").

8.2. Dodávateľ môže poskytnúť Dôverné informácie iba v nevyhnutnom rozsahu a výlučne pre účely spojené s realizáciou spolupráce podľa tejto Zmluvy svojim zamestnancom, svojim daňovým a právnym poradcom, pokiaľ takéto osoby súhlasili s tým, že budú viazané touto Zmluvou alebo podobnou Zmluvou za rovnakých podmienok, aké sú uvedené v tejto Zmluve. V prípade poskytnutia Dôverných informácií osobám uvedeným v tomto bode, zodpovedá Dodávateľ priamo za ochranu takto poskytnutých údajov, akoby tieto informácie spracúval sám na vlastnú zodpovednosť.

8.3. Dodávateľ sa zaväzuje zabezpečiť utajenie Dôverných informácií a chrániť Dôverné informácie s náležitou odbornou starostlivosťou pred ich stratou, scudzením alebo akýmkoľvek iným možným zneužitím. Dodávateľ je povinný zabezpečiť utajenie Dôverných informácií a mlčanlivosť o Dôverných informáciách aj u svojich zamestnancov, a akýchkoľvek iných osôb.

8.4. Zmluvné strany sú povinné zachovávať mlčanlivosť a ochraňovať Dôverné informácie počas platnosti tejto Zmluvy, ako aj počas 10 rokov odo dňa ukončenia, resp. zrušenia tejto Zmluvy.

8.5. V prípade porušenia povinnosti zabezpečenia utajenia Dôverných informácií a mlčanlivosti o Dôverných informáciách zo strany Dodávateľa, je Dodávateľ povinný uhradiť zmluvnú pokutu vo výške 1 000,- EUR za každé porušenie povinnosti stanovenej v tomto článku, ktorú je Dodávateľ povinný uhradiť Odberateľovi do kalendárnych 14 dní odo dňa, kedy Odberateľ informoval Dodávateľa o porušení tejto povinnosti.

IX. POVINNOSŤ DODÁVATEĽA PRI VÝKONE AUDITU/KONTROLY/OVEROVANIA

9.1. Dodávateľ berie na vedomie, že finančné prostriedky Odberateľa určené na zaplatenie Predmetu zmluvy podľa článku IV. tejto Zmluvy zahŕňajú aj finančné prostriedky z Európskeho fondu regionálneho rozvoja (Operačný program Integrovaná infraštruktúra v rámci operačnej osi 7). Dodávateľ berie na vedomie, že podpisom tejto Zmluvy sa stáva súčasťou Systému riadenia európskych štrukturálnych a investičných fondov a Systému finančného riadenia. Dodávateľ zároveň berie na vedomie, že na použitie prostriedkov, kontrolu použitia týchto prostriedkov a vymáhanie ich neoprávneného použitia alebo zadržania sa vzťahuje režim upravený v osobitných predpisoch, napr. zákon č. 357/2015 Z. z. o finančnej kontrole a o audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „zákon č. 357/2015 Z. z."), zákon č.

523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 440/2000 Z. z. o správach finančnej kontroly v znení neskorších predpisov, zákon č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 528/2008 Z. z. o pomoci a podpore poskytovanej z fondov Európskeho spoločenstva v znení neskorších predpisov a v zmysle ďalších príslušných predpisov Slovenskej republiky a právnych aktov Európskej únie.

9.2. Zmluvné strany sa dohodli a súhlasia, že všetky zmeny v Systéme riadenia európskych štrukturálnych a investičných fondov, Systéme finančného riadenia alebo v právnych dokumentoch vydaných oprávnenými osobami, z ktorých pre Dodávateľa vyplývajú práva a povinnosti v súvislosti s plnením podľa tejto Zmluvy a Zmluvy o poskytnutí NFP, ak boli tieto dokumenty zverejnené, sú pre Dodávateľa záväzné dňom ich zverejnenia.

9.3. Okrem povinností uvedených v tejto Zmluve je Dodávateľ povinný strpieť výkon kontroly/auditu/overovania oprávnenými osobami súvisiaceho s dodaním predmetu zmluvy a poskytnúť im všetku potrebnú súčinnosť, a to kedykoľvek počas platnosti a účinnosti tejto Zmluvy, ako aj v termínoch stanovených pre Odberateľa v zmluvných vzťahoch s príslušnými orgánmi zapojenými do implementácie fondov Európskej únie, v rámci ktorých si Odberateľ nárokuje financovanie výdavkov uhradených Dodávateľovi, ktoré vznikli s plnením podľa tejto Zmluvy.

9.4. Dodávateľ sa zaväzuje umožniť výkon finančnej kontroly/auditu/overovania príslušnými oprávnenými osobami uvedenými v bode 9.5 tohto článku Zmluvy a vytvoriť podmienky pre jej výkon v zmysle príslušných právnych predpisov Slovenskej republiky a právnych aktov Európskej únie a ako kontrolovaný subjekt pri výkone kontroly riadne plniť povinnosti, ktoré mu vyplývajú z uvedených predpisov a to počas platnosti a účinnosti tejto Zmluvy a počas platnosti a účinnosti Zmluvy o poskytnutí NFP. Uvedená doba sa predĺži v prípade, ak nastanú skutočnosti uvedené v článku 90 Nariadenia Rady (ES) č. 1083/2006 (alebo o obdobné ustanovenie v nariadení Európskeho parlamentu a Rady, ktorým sa zruší nariadenie 1083/2006 pre programové obdobie 2014 – 2020) alebo článku 32 Vykonávacieho Nariadenia Komisie (EÚ) č. 908/2014 o čas trvania týchto skutočností. Dodávateľ sa zaväzuje podrobiť sa aj výkonu kontroly poverenými zamestnancami Odberateľa.

9.5. Oprávnenými osobami sú najmä:

a) Poskytovateľ, s ktorým má Odberateľ uzatvorenú Zmluvu o poskytnutí nenávratného finančného príspevku a ním poverené osoby,
b) Útvar vnútorného auditu Riadiaceho orgánu alebo Sprostredkovateľského orgánu a nimi poverené osoby,
c) Najvyšší kontrolný úrad SR, Úrad vládneho auditu, Certifikačný orgán a nimi poverené osoby,
d) Orgán auditu, jeho spolupracujúce orgány a osoby poverené na výkon kontroly/auditu,
e) Splnomocnení zástupcovia Európskej komisie a Európskeho dvora audítorov,
f) Orgán zabezpečujúci ochranu finančných záujmov ES,
g) Osoby prizvané orgánmi uvedenými v písm. a) až f) v súlade s príslušnými právnymi predpismi SR a právnymi aktmi ES.

9.6. Odberateľ berie na vedomie, že sprostredkovateľský orgán Operačného programu Integrovaná infraštruktúra prioritná os 7 je pri vykonávaní administratívnej finančnej

kontroly v nevyhnutnom rozsahu oprávnený od Odberateľa alebo od osoby, ktorá je vo vzťahu k finančnej operácii alebo jej časti Dodávateľa alebo akejkoľvek inej osoby, ktorá má informácie, doklady alebo iné podklady, ktoré sú potrebné pre výkon finančnej kontroly, ak ich poskytnutiu nebráni osobitný predpis (ďalej aj „tretia osoba"):

- vyžadovať a odoberať, v určenej lehote originály alebo úradne osvedčené kópie dokladov, písomností, záznamy dát na pamäťových médiách prostriedkov výpočtovej techniky, ich výpisov, výstupov, vyjadrenia, informácie, dokumenty a iné podklady súvisiace s administratívnou finančnou kontrolou alebo finančnou kontrolou na mieste;
- vyžadovať od tretej osoby súčinnosť v rozsahu oprávnení podľa zákona č. 357/2015 Z. z.;
- osoby poverené na výkon kontroly sú oprávnené v nevyhnutnom rozsahu za podmienok ustanovených v osobitných predpisoch okrem oprávnení uvedených článku IX, ods. 9.5 v predchádzajúcich písmenách vstupovať do objektu, zariadenia, prevádzky, dopravného prostriedku, na pozemok tretej osoby, alebo vstupovať do obydlia, ak sa používa aj na podnikanie alebo na vykonávanie inej hospodárskej činnosti;
- oboznámiť sa pri začatí finančnej kontroly na mieste s bezpečnostnými predpismi, ktoré sa vzťahujú na priestory, v ktorých sa vykonáva finančná kontrola na mieste.

9.7. Sprostredkovateľský orgán je pri vykonávaní administratívnej finančnej kontroly podľa zákona č. 357/2015 Z. z. povinný potvrdiť tretej osobe odobratie poskytnutých originálov alebo úradne osvedčených kópií dokladov, písomností, záznamov dát na pamäťových médiách prostriedkov výpočtovej techniky, ich výpisov, výstupov, vyjadrení, informácií, dokumentov a iných podkladov súvisiacich s administratívnou finančnou kontrolou alebo finančnou kontrolou na mieste a zabezpečiť ich riadnu ochranu pred stratou, zničením, poškodením a zneužitím. Uvedené potvrdenie sa vydáva, ak sprostredkovateľský orgán žiada o poskytnutie podkladov nad rámec definovaný Zmluvou o poskytnutí NFP. Tieto doklady sprostredkovateľský orgán vráti bezodkladne tomu, od koho sa vyžiadali, ak nie sú potrebné na konanie podľa zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov alebo na iné konanie podľa osobitných predpisov. Dodávateľ je povinný zabezpečiť prítomnosť oprávnených osôb zo strany Dodávateľa počas vykonávania kontroly u Dodávateľa.

9.8. Vykonaním kontroly oprávnenej osoby podľa odstavca 9.5 písm. a) tohto článku Zmluvy nie je dotknuté právo Riadiaceho orgánu alebo iného oprávneného orgánu na vykonanie novej kontroly/vládneho auditu, a to počas celej doby účinnosti Zmluvy o poskytnutí NFP.

X. LICENCIA

10.1. Aby sa predišlo všetkým pochybnostiam, Zmluvné strany vyhlasujú, že Predmetom plnenia tejto Zmluvy nie sú také služby, ktorých výstupom by bol vznik Diela.

10.2. Aby sa predišlo všetkým pochybnostiam, Zmluvné strany vyhlasujú, že Predmetom plnenia tejto Zmluvy nie sú také služby, ktoré by spadali pod licenčnú alebo sublicenčnú zmluvu.

XI. OKOLNOSTI VYLUČUJÚCE ZODPOVEDNOSŤ /VYŠŠIA MOC/

11.1. Za prípady vyššej moci sa považujú také neobvyklé okolnosti, ktoré nastanú po nadobudnutí platnosti a účinnosti tejto Zmluvy nezávisle od vôle Zmluvných strán, a ktoré bránia Zmluvnej strane plniť povinnosť alebo povinnosti dohodnuté v tejto Zmluve, a ktoré nemohli byť danou Zmluvnou stranou predvídané alebo odvrátené. Ide napríklad o prípady vojny, inváze, občianske vojny, povstanie, občianske nepokoje, embargo, zásah štátu či vlády, živelné udalosti, generálne štrajky, pandémie. Nejde však o stratu spôsobilosti preukázanú Dodávateľom v rámci procesu verejného obstarávania. Ak takáto okolnosť vznikla v čase, keď bola Zmluvná strana už v omeškaní s plnením svojej povinnosti, nebude sa na ňu prihliadať.

11.2. O okolnostiach vylučujúcich zodpovednosť bude tá Zmluvná strana, ktorej je týmto znemožnené plnenie, informovať druhú Zmluvný stranu písomne a predloží jej dôkazy, že tieto okolnosti majú podstatný vplyv na plnenie zmluvných povinností. Príslušná Zmluvná strana nezodpovedá za škodu a druhá Zmluvná strana nemá nárok na zmluvnú pokutu alebo inú sankciu vyplývajúcu z tejto Zmluvy, ak je nesplnenie povinnosti Zmluvnej strany zapríčinené okolnosťou/okolnosťami vylučujúcou/vylučujúcimi zodpovednosť a túto/tieto preukáže.

11.3. Dodávateľ je oprávnený pozastaviť alebo obmedziť dodanie predmetu zmluvy, pokiaľ je dodanie systému podľa tejto Zmluvy znemožnené alebo obmedzené neodvrátiteľnou udalosťou, ktorú nebolo možné predvídať alebo jej zabrániť (najmä vyššia moc a iné okolnosti vylučujúce zodpovednosť v zmysle Obchodného zákonníka).

11.4. Pokiaľ okolnosti vyššej moci trvajú dlhšie ako 90 (deväťdesiat) kalendárnych dní, Zmluvné strany sa zaväzujú rokovať o dotknutých povinnostiach, najmä o predĺžení termínov podľa tejto Zmluvy. Ak nedôjde k dohode, má každá iná ako Povinná strana právo od tejto Zmluvy odstúpiť.

XII. ZÁVEREČNÉ USTANOVENIA

12.1. Zmluvné strany pre účely tejto Zmluvy určujú kontaktné osoby zodpovedné za vecnú a odbornú komunikáciu v súvislosti s touto Zmluvou takto:

a) Za Odberateľa: Erika Ferková, informatik@nemocnicasnina.sk
b) Za Dodávateľa: Oliver Havrila, MSc., Oliver.Havrila@tuvsud.com

12.2. Táto zmluva nadobúda platnosť dňom jej podpisu oboma zmluvnými stranami a účinnosť po ukončení finančnej kontroly, ak poskytovateľ príspevku z fondov EÚ neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok verejného obstarávania, pričom rozhodujúci je dátum doručenia správy z kontroly prijímateľovi. Ak boli v rámci finančnej kontroly verejného obstarávania identifikované nedostatky, ktoré mali alebo mohli mať vplyv na výsledok verejného obstarávania, zmluva nadobudne účinnosť momentom súhlasu prijímateľa s výškou finančnej opravy uvedenej v správe z kontroly a kumulatívneho splnenia podmienky na uplatnenie finančnej opravy podľa Metodického pokynu č.5, ktorý upravuje postup pri určení finančných opráv za verejné obstarávanie.

12.3. Akékoľvek zmeny tejto Zmluvy, prílohy k tejto Zmluve a dodatky k tejto Zmluve musia mať písomnú formu.

12.4. Všetky právne vzťahy vyplývajúce z tejto Zmluvy sa riadia slovenským Obchodným zákonníkom a právnym poriadkom Slovenskej republiky.

12.5. Zmluvné strany sa budú usilovať o to, aby riešili každý spor predovšetkým vzájomnou dohodou a predišli tým prípadnému súdnemu riešeniu sporu. Obe Zmluvné strany budú spolupracovať a budú sa v dobrej viere usilovať o vyriešenie problému vnútornou cestou bez vedenia súdneho sporu.

12.6. Všetky spory vyplývajúce z tejto Zmluvy (vrátane sporov o náhradu škody, sporov o platnosť, resp. neplatnosť právnych úkonov, atď.) bude v konaní na prvom stupni rozhodovať súd so sídlom na území Slovenskej republiky, ktorý je v týchto veciach určený ako príslušný súd, a v ostatných stupňoch súdy na území Slovenskej republiky určené podľa procesných predpisov platných na území Slovenskej republiky.

12.7. Pri plnení predmetu tejto Zmluvy sú si obe Zmluvné strany vedomé svojich povinností vyplývajúcich zo zákona č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

12.8. Prípadné neplatné časti Zmluvy budú vzájomnou dohodou Zmluvných strán upravené do takej miery, aby mohli byť tieto časti Zmluvy považované za platné. Práva a záväzky oboch Zmluvných strán budú interpretované a presadzované podľa upravených podmienok alebo predpokladov s tým, že v čo možno najvyššej miere bude zachovaný úmysel Zmluvných strán.

12.9. Táto Zmluva je vyhotovená v štyroch rovnopisoch, z ktorých každý má právnu silu originálu. Každá zo Zmluvných strán obdrží dva rovnopisy tejto Zmluvy.

12.10. Neoddeliteľnou súčasťou tejto zmluvy sú nasledovné prílohy:

- Príloha č. 1: Podrobná špecifikácia predmetu zmluvy
- Príloha č. 2: Zoznam subdodávateľov
- Príloha č. 3: Stanovenie ceny pracovných dní (človekodní)

12.11. Zmluvné strany prehlasujú, že si zmluvu prečítali, porozumeli jej obsahu a na znak súhlasu Zmluvu podpisujú.

V Bratisla[redacted]23/05/2023
Dodávate[redacted]

v Snine dňa: 26.5.2023
Odberateľ: [redacted]

Ing. [redacted] Chmel
Generálny riaditeľ / CEO

MUDr. Andrej [redacted]
konateľ spoločnosti

Príloha č. 1: Podrobná špecifikácia predmetu zmluvy

Predmetom zmluvy je dodávka:

- systému SIEM na infraštruktúre verejného obstarávateľa, vrátane hardvéru, vrátane inštalačných a konfiguračných prác,
- systému pre monitoring výkonu, prevádzky a bezpečnosti počítačových sietí na infraštruktúre verejného obstarávateľa vrátane hardvéru vrátane inštalačných a konfiguračných prác,
- NAS.

Minimálne hardvérové požiadavky pre SIEM server:
CPU Intel rada E5-26XX min. 12x CPU Cores, RAM DDR4 128GB, HDD SSD 6TB v RAID1, 3x NIC, 1x NIC pre manažment serveru, redundantný zdroj, montáž do racku max. 2U.

Minimálne hardvérové požiadavky pre NAS:
Min. 8x 3,5´´ SATA HDD, Podpora "hot swap", 2x RJ-45 10Gb Port, Redundantné napájacie zdroje, Výsuvné "rack rails", CPU min. 4 jadrá 2,2 GHz, RAM min. 4GB, 2 pamäťové sloty, Podpora pre RIAD 0,1,5,6,10, Podpora pre iSCSI, 3x 8TB NAS HDD, Cache buffer 256MB.

Minimálne požiadavky na dodávku systému SIEM na infraštruktúre verejného obstarávateľa sú:

Bezpečnostné požiadavky na SIEM

SIEM (Security Information and Event Management) je nástroj používaný na monitorovanie a analýzu bezpečnostných udalostí a výstrah generovaných z rôznych systémov a zariadení v rámci IT infraštruktúry Nemocnice Snina. Požadované funkčné požiadavky na SIEM zahŕňajú:

- Zber udalostí: SIEM musí byť schopný zbierať udalosti (logy) z rôznych zdrojov, ako sú servery, sieťové zariadenia, databázy, aplikácie atď.
- Monitorovanie v reálnom čase: SIEM musí byť schopný monitorovať udalosti a výstrahy generované v reálnom čase a poskytovať okamžité upozornenia na kritické udalosti,
- Korelácia a analýza: SIEM musí byť schopný korelovať udalosti z rôznych zdrojov a analyzovať
  ich s cieľom identifikovať potenciálne bezpečnostné hrozby a anomálie,
- Výstrahy a hlásenia: SIEM musí byť schopný generovať výstrahy a správy na základe vopred definovaných pravidiel a prahových hodnôt,
- Integrácia spravodajstva o hrozbách (Threat Intelligence): SIEM musí byť schopný integrovať sa s externými zdrojmi spravodajstva o hrozbách, aby sa zlepšili jeho možnosti analýzy a detekcie,
- Analýza správania používateľov a entít (UEBA): SIEM by mal byť schopný vykonávať analýzu správania používateľov a entít s cieľom odhaliť nezvyčajnú aktivitu a potenciálne hrozby.
- Reakcia na incidenty: SIEM musí byť schopný poskytnúť funkcie reakcie na incidenty, ako sú napríklad akcie automatickej odozvy, správa prípadov a forenzná analýza.
- Súlad: SIEM by mal byť schopný pomáhať pri plnení požiadaviek na súlad generovaním správ a upozornení na porušenia pravidiel.
- Škálovateľnosť: SIEM by mal byť schopný škálovať, aby vyhovoval rastúcim potrebám Nemocnice Snina a zvládal veľké objemy údajov.

- Integrácia s inými bezpečnostnými nástrojmi: SIEM musí byť schopný integrovať sa s inými bezpečnostnými nástrojmi, ako sú firewally, IDS/IPS a riešenia ochrany koncových bodov, aby poskytoval komplexné bezpečnostné riešenie.

Funkčné požiadavky na SIEM riešenie

- Riešenie musí byť centralizovaným bodom analýzy logov a musí byť schopné spracovať a vizualizovať prichádzajúce údaje v takmer reálnom čase.
- Riešenie musí poskytnúť funkčnú analýzu logov (chyby, anomálie); bezpečnostnú analýzu (udalostí, incidentov, výstrah); a mať auditné logy v rámci súladu.
- Riešenie musí poskytnúť zber logov z akýchkoľvek zariadení a systémov bez obmedzenia na konkrétneho výrobcu.
- Riešenie musí podporovať diagnostiku zlyhaní alebo prevádzkových problémov až po aplikačnú úroveň.
- Riešenie musí mať integrované lokálne šifrovanie log (minimálne AES 196 a vyššie) a algoritmus kompresie protokolov
- Riešenie musí byť schopné vyrovnať sa s rôznymi druhmi logov z rôznych zdrojov, s rôznymi dobami uchovávania a formátmi.
- Samotné riešenie musí byť rýchle, agilné a poskytovať výkonné možnosti vyhľadávania bez znalosti rôznych syntaxí vyhľadávania.
- Grafické rozhranie musí byť užívateľsky prívetivé, intuitívne, ľahko použiteľné a ľahko zaškoliteľné personálom
- Správa denníka (reporting) musí byť ľahko čitateľná a exportovateľná do PDF, DOCX, alebo XLXS.
- Riešenie musí integrovať ochranu logov pred neoprávneným zásahom, sledovanie zmien, úmyselné vymazanie alebo úpravu záznamov denníka.
- Vnútorná architektúra systému musí byť schopná zaznamenať zmenu, chybové prihlásenia do systémov, prípadne systémové zmeny administrátora.
- Riešenie monitoruje logy z aplikácií a databáz s cieľom analyzovať, kto, kedy a čo bolo vykonané
- Riešenie musí podporovať identifikáciu tokov údajov a odhaľovať napr. "top downloaderov" ale DoS útok.
- Riešenie musí podporovať sledovanie logov konfigurácií z operačných systémov, sieťových zariadení atď. analyzovať, kto, kedy a čo zmenilo konfiguráciu.
- Logy sa musia dať ľahko filtrovať.
- Riešenie musí mať "proaktívny" prístup, ktorý automaticky informuje o zistených bezpečnostných incidentoch na základe predkonfigurovaných politík alebo pravidiel, ktorá zahŕňa korelačné a prahové funkcie upozornení.
- Riešenie by malo podporiť súlad s predpismi GDPR, EU NIS2, Zákon 69/2018 Z.z,
- Riešenie identifikuje porušenie ochrany osobných údajov vrátane toho, kto, kedy a ako sa
- pristupuje k údajom a systémom, na ktoré sa vzťahuje GDPR.
- Riešenie podporuje oblasti súvisiace s GDPR, ako sú článok 32 – Bezpečnosť spracúvania, Článok 33 – Oznamovanie porušení ochrany osobných údajov dozornému orgánu, článok 34 – Oznamovanie porušenia OII, Článok 58 – Právomoci
- Hardvérové zariadenie musí byť montovateľné do stojana s redundantným napájaním pre 230V.
- Riešenie musí podporovať distribuovanú architektúru vrátane centrálnej správy s možnosťou rozšíriteľnosti bez licenčných obmedzení EPS.

- Riešenie musí podporovať vyhľadávanie hrozieb (threat hunting) aj s pomocou „thread feedov“ ktoré získava s otvorených ako i komerčných databáz.
- Riešenie musí podporovať pasívnu analýza sieťovej prevádzky pomocou „mirror port“, „netflow“ technológie s možnosťou archivácie a časového spúšťania.
- Riešenie musí podporovať bezpečnostnú notifikáciu (email, SMS, automatické zakladanie ticketov) s flexibilnou zmenou pravidiel.
- Riešenie disponuje funkciou EDR pre end pointy a servre (podpora Windows, Linux, MacOS), počet endpointov bez licenčných obmedzení, so štandardným súborom bezpečnostných pravidiel pre endpointy, servre a sieťové zariadenia.
- Počet sieťových zariadení (log sources): cca 150-200

Minimálne systémové požiadavky SIEM v Nemocnici Snina

ID	Požiadavka	Popis
1	Hardware	Riešenie SIEM vyžaduje vyhradený server alebo klaster serverov. Hardvér servera by mal mať dostatočný výpočtový výkon, RAM a úložnú kapacitu na spracovanie očakávaného objemu protokolov a analýzy. CPU: 12CPU Cores RAM: 128GB ECC DDR4 alebo DDR5 RAID: 10 OS storage: 240 GB NIC: 2 x 10Gbps Power supply: redundant
2	Operačný systém	Riešenie SIEM musí bežať na serverovom operačnom systéme Linux.
3	Kapacita dátového úložiska	SIEM vyžaduje veľké množstvo úložného priestoru na ukladanie protokolov generovaných rôznymi zdrojmi. Predpokladaná retencia logov: 30 dní Storage capacity: 5-8 Terabyte Storage class: SSD, alebo SATA
4	Databáza	Riešenie SIEM vyžaduje databázu na ukladanie logov a poskytovanie efektívneho vyhľadávania a analýzy. Databáza môže byť komerčná databáza, ako je Oracle, alebo databáza s otvoreným zdrojom, ako je MySQL.
5	Softvér SIEM Agent, alebo EDR agent	Agenti SIEM sú nainštalovaní v systémoch, ktoré generujú logy na zhromažďovanie a odosielanie protokolov na server SIEM. Softvér agenta by mal byť kompatibilný so systémami generujúcimi protokoly a riešením SIEM. Požadovaná podpora koncových OS pre agentov: 1. Microsoft Windows 10 2.
6	Zdroje logov	○ Desktopy ○ Laptopy ○ Servre ○ Firewally ○ Sieťové prvky (route, switche) ○ Medicínske zariadenia, ktoré vedia generovať logy
7		Požadovaný formá logov: ▪ CEF (Common Event Format) ▪ LEEF (Log Event Extended Format) ▪ RFC 5424 (Syslog Format), ▪ RFC 3164 (BSD Syslog Format)
8	Analýza packetov v sieti	○ Softvérový alebo hardvérový SIEM komponent ○ Podpora mirror port (SPAN, RSPAN) na strane switcha
9	Zálohovanie SIEM a obnova po havárii	Riešenie musí podporovať robustný plán zálohovania a obnovy po havárii, aby sa zabezpečilo, že sa logy a udalosti nestratia a že riešenie SIEM bude možné rýchlo obnoviť v prípade zlyhania alebo katastrofy.
10	Údržba a aktualizácie	Riešenie vyžaduje pravidelnú údržbu a aktualizácie, aby sa zabezpečilo, že bude aktuálne s najnovšími bezpečnostnými záplatami a funkciami.

Popis implementácie SIEM

Implementácia:

- fyzická inštalácia hardvéru do serverovej miestnosti,
- inštalácia a základná konfigurácia SIEM nástroja, vrátane všetkých jeho modulov, databázového backendu a mikroservisov,
- vykonanie základných testov, ktoré by mali zahŕňať minimálne dva základné scenáre 1) výpadok napájania,
  2) výpadok jedného z diskov s následnou obnovou dát. Cieľom základných testov je overiť si zachovanie integrity dát a odolnosti systému,
- definícia a implementácia zálohovacích scenárov pre SIEM systém a pre databázový backend,
- vykonanie testov zálohovania a obnovy,
- integrácia modulu LMS so zdrojmi dát, zabezpečiť zmeny konfigurácie zdrojov dát tak aby sa všetky potrebné informácie prenášali do SIEM nástroja,
- integrácia modulu pre sieťovú analýzu do sieťovej infraštruktúry.
  Počet MD: 27,5

Testovacia prevádzka:

- testovanie integrácie so zdrojmi dát, overiť či SIEM systém správne zbiera a spracováva dáta z rôznych zdrojov. Testovanie by sa malo zamerať na správnosť konfigurácie zdrojov dát, ako aj na správne fungovanie SIEM nástroja pri zmenách v zdrojoch dát,
- testovanie detekcie hrozieb, overiť schopnosti SIEM systému identifikovať rôzne typy bezpečnostných hrozieb. Toto by malo zahŕňať simulácie rôznych typov útokov, ako sú DDoS útoky, phishingové útoky a útoky na prihlasovacie údaje. Cieľom tohto testovania je zistiť, ako rýchlo a spoľahlivo systém identifikuje a reaguje na tieto hrozby,
- testovanie výkonnosti či SIEM systém dokáže spracovávať veľké objemy dát a zvládať zvýšenú záťaž v prípade útoku alebo incidentu. Cieľom tohto testovania je zistiť, ako rýchlo a efektívne systém spracováva dáta a či dokáže udržať dostatočnú rýchlosť a výkon v záťažových situáciách,
- testovanie ukladania logov by malo overiť, či modul LMS dokáže správne ukladať logy do databázy a chrániť ich pred stratením alebo zneužitím. Testovanie by malo zahrňovať rôzne scenáre, ako je zálohovanie, obnova logov a vymazávanie starých logov,
- testovanie vyhľadávania a filtrovania logov by malo zistiť, či modul LMS dokáže umožniť používateľom vyhľadávať a filtrovať logy podľa rôznych kritérií. Cieľom tohto testovania je zistiť, či používateľom umožňuje rýchlo a efektívne nájsť potrebné logy a vykonať analýzu logov,
- testovanie zabezpečenia by malo overiť, či má modul LMS dostatočné zabezpečenie a chráni logy pred neoprávneným prístupom a manipuláciou. Testovanie by malo zahrňovať overenie, či modul LMS umožňuje nastavenie rôznych úrovní prístupu a správu oprávnení pre používateľov,
- testovanie archivácie logov by malo zahrňovať overenie, či modul LMS umožňuje nastavenie doby uchovávania a archivovania logov, ako aj ich následnú obnovu.
- testovanie úrovne compliance by malo overiť, či SIEM dokáže splniť požiadavky na zabezpečenie a súlad s rôznymi štandardmi a reguláciami.
  Počet MD: 20

Prechodová fáza:

- ladenie korelačných pravidiel pre detekciu a identifikáciu hrozieb v SIEM systéme. Zamerať ladenie korelačných pravidiel na identifikáciu a odstránenie falošne pozitívnych a falošne negatívnych alarmov. Zabezpečiť, aby korelačné pravidlá zodpovedali konkrétnym potrebám a požiadavkám,
- príprava playbookov pre riadenie incidentov v SIEM systéme. Zamerať sa na tvorbu a overenie playbookov pre konkrétne typy incidentov. Playbooky by mali obsahovať postupy, ktoré pomôžu používateľom zvládnuť incidenty a minimalizovať dopad na organizáciu. Zabezpečiť, aby playbooky zodpovedali konkrétnym požiadavkám organizácie, boli správne dokumentované a aktualizované,
- testovanie identifikácie udalostí a incidentov s cieľom overiť, či SIEM systém dokáže správne identifikovať a kategorizovať udalosti a incidenty podľa ich závažnosti a rizika pre organizáciu.

  Počet MD: 30

Školenie incident response tímu:

- základy práce so SIEM. Malo by zahrňovať základné pojmy a princípy SIEM systému. Členovia tímu by mal byť oboznámení s funkčnosťou SIEM a aké typy udalostí a hrozieb dokáže detegovať. Taktiež by mali byť informovaní o tom, ako SIEM zabezpečuje centralizované zaznamenávanie a monitorovanie bezpečnostných udalostí a ako pomáha pri riadení bezpečnostných incidentov,
- členovia tímu by mali byť informovaní o tom, ako sa korelačné pravidlá používajú na identifikáciu hrozieb a ako sa používajú na generovanie alarmov a upozornení. Taktiež by mali byť oboznámení s tým, ako pracovať s korelačnými pravidlami a ako ich aktualizovať a modifikovať v prípade potreby,
- členovia tímu by mali byť oboznámení s tým, ako SIEM systém deteguje a kategorizuje incidenty na základe správne odladených korelačných pravidiel. Mali by byť informovaní o tom, ako správne identifikovať a kategorizovať incidenty na základe ich závažnosti a rizika pre organizáciu,
- členovia tímu by mali byť informovaní o tom, ako pracovať s playbookmi a ako sa používajú na riadenie incidentov. Dôležité je tiež zabezpečiť, aby mali prehľad o postupoch pri identifikácii, analýze a riešení incidentov. Taktiež by mali byť informovaní o tom, ako dokumentovať incidenty a aktualizovať playbooky v prípade potreby.

  Počet MD: 15

Príloha č. 2: Zoznam subdodávateľov

p. č.	Meno a priezvisko alebo obchodné meno, resp. názov	Adresa pobytu alebo sídlo	IČO alebo dátum narodenia	Údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia	Podiel na realizácii zákazky v %	Predmet subdodávky
1.						
2.						
3.						

Príloha č. 3

Príloha č. 3						
Predmet dodávky	Presný názov dodávky	MJ	Jednotková cena bez DPH (v EUR)	Počet MJ jednotiek	Cena spolu bez DPH (v EUR)	Cena spolu s DPH (v EUR)
Nákup HW	SIEM server	1	7020,8	1	7 020,80	8 424,96
Nákup HW	NAS	1	2 460,88	1	2 460,88	2 953,06
IT programátor vo fáze Implementácia a testovanie		ČD	600	27,5	16 500	19 800
IT tester vo fáze Implementácia a testovanie		ČD	500	20	10 000	12 000
Špecialista pre infraštruktúru/HW špecialista vo fáze Nasadenie		ČD	600	45	27 000	32 400
Celková cena					62 981,68 €	**75 578,02 €**