Kúpna zmluva č. Z20243561_Z

uzatvorená v zmysle §409 a nasl. Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Ľubovnianska nemocnica, n.o.
Sídlo:	Obrancov mieru 3, 06401 Stará Ľubovňa, Slovenská republika
IČO:	37886851
DIČ:	2022057565
IČ DPH:	SK2022057565
Bankové spojenie:	IBAN: SK45 0200 0000 0020 3667 1956
Telefón:	0524317216

1.2 Dodávateľ:

Obchodné meno:	iServices s. r. o.
Sídlo:	Zadunajská cesta 8, 85101 Bratislava, Slovenská republika
IČO:	43872930
DIČ:	2022500524
IČ DPH:	SK2022500524
Bankové spojenie:	IBAN: SK4411000000002622819087, BIC: TATRSKBX
Telefón:	+421262244226

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Dodávka a inštalácia ESET PROTECT Enterprise On-Prem alebo cloudového riešenia s licenciou na 24 mesiacov vrátane Enterprise servisnej podpory na 12 mesiacov
Kľúčové slová:	antivírus, antivírusový softvérový balík, ESET PROTECT Enterprise On-Prem alebo cloud, SLA, Eset
CPV:	48761000-0 - Antivírusový softvérový balík; 72261000-2 - Softvérové podporné služby; 72250000-2 - Služby týkajúce sa podpory systému; 72263000-6 - Implementácia softvéru; 60000000-8 - Dopravné služby (bez prepravy odpadu)
Druh/y:	Tovar; Služba

2.2 Funkčná a technická špecifikácia predmetu Zmluvy:

Zoznam položiek:

1. Licencia ESET PROTECT Enterprise On-Prem alebo cloud pre ochranu 280 endpointov na licenčné obdobie 24 mesiacov

2. Migračné, implementačné a optimalizačné práce ESET PROTECT 280 EndPointov a Inštalácia serverového riešenia ESET XDR

3. Poskytovanie služieb rozšírenej servisnej on site podpory formou SLA pre platformu výrobcu ESET pre prostredie ESET Protect a ESET Inspect na 12 mesiacov

4. Rozsah podpory - Komplexná starostlivosť o prevádzku ESET Inspect riešenia pozostávajúceho z ESET Protect

5. Antivírusové riešenie pre koncové body a servery:

6. Integrovaná cloudová analýza neznámych vzoriek

7. Sifrovanie celých diskov

8. XDR riešenie

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

Položka č. 1: Licencia ESET PROTECT Enterprise On-Prem alebo cloud pre ochranu 280 endpointov na licenčné obdobie 24 mesiacov

Funkcia

Licencia ESET PROTECT Enterprise On-Prem alebo cloud
Predmetom zákazky je nákup dodanie produktového balíka bezpečnostných riešení na ochranu koncových pracovných staníc, serverov, mobilných zariadení, ktorý obsahuje viacvrstvovú antivírusovú ochranu, technológiu automatickej analýzy podozrivých súborov v cloudovom sandboxe výrobcu, pokročilú vrstvu ochrany v podobe XDR nástroja na detekciu a reakciu, šifrovanie celých diskov a možnosť prevádzkovať jednotnú management konzolu na správu týchto riešení v cloudovom nasadení alebo lokálnom (on-prem) nasadení podľa voľby verejného obstarávateľa za účelom zvýšenia kybernetickej bezpečnosti. Prostredie
Verejný obstarávateľ pripúšťa aj predloženie ekvivalentného riešenia za podmienky, že uchádzačom predložený ekvivalent bude spĺňať všetky min. požiadavky vereného obstarávateľa na predmet zákazky. Odkaz technickej špecifikácie na obchodnú značku alebo výrobcu tovaru je uvádzaný z dôvodu garantovania technických vlastností, kvalitatívnych parametrov tovaru a účelu použitia. Verejný obstarávateľ pripúšťa tovar podľa technickej špecifikácie nahradiť ekvivalentným tovarom resp. riešením s rovnakými alebo výkonnostne lepších technickými vlastnosťami a kvalitou, za podmienky zabezpečenia plného
prechodu zo súčasne využívaného antivírusového balíka (ESET) verejným obstarávateľom na uchádzačom navrhované riešenie bez akýkoľvek strát údajov resp. služieb, ktoré využíva verejný obstarávateľ v súčasnosti. V prípade predloženia ekvivalentu musí zároveň uchádzač garantovať bezchybnú implementáciu (bez akejkoľvek straty dát verejného obstarávateľa) ním navrhovaného ekvivalentného riešenia v prostredí verejného obstarávateľa. Zároveň predložený ekvivalent nesmie vyžadovať iné vedľajšie náklady, ktoré by musel zabezpečiť verejný obstarávateľ v rámci súčinnosti viažucej sa k dodaniu predmetu
zákazky a prijatím predloženého ekvivalentu nesmie dôjsť k zvýšeným priamym alebo nepriamym nákladom vyplývajúcim z dodania predmetu zákazky. V prípade predkladania ekvivalentu uchádzač predkladá zároveň aj harmonogram, v ktorom uvedie jednotlivé činnosti, ktoré je potrebné v nadväznosti na dodanie a implementáciu ekvivalentného riešenia v prostrední verejného obstarávania vykonať a zároveň aj časovú os implementácie ekvivalentného riešenia. Časový harmonogram navrhovaný uchádzačom pri predložení ekvivalentného riešenia (odo dňa účinnosti zmluvy, ktorá bude výsledkom verejného obstarávania)
nesmie presiahnuť viac ako 5 pracovných dní (implementácia v prostredí verejného obstarávania)

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	Hodnota/Charakteristika			

Položka č. 2: Migračné, implementačné a optimalizačné práce ESET PROTECT 280 EndPointov a Inštalácia serverového riešenia ESET XDR

Funkcia
Licencie ESET PROTECT Enterprise alebo ekvivalent, na licenčné obdobie min. 24 mesiacov s rozšírenou servisnou podporou formou SLA na obdobie min. 12 mesiacov
Dodanie licencií ESET PROTECT Enterprise alebo ekvivalent pre ochranu min. 280 endpointov
Dodanie implementačných, konfiguračných prác pre XDR platformu ESET PROTECT Enterprise alebo ekvivalent
Implementácia prostredia ESET PROTECT alebo ekvivalent (centrálneho manažmentu) pre serverové prostredie, pracovné stanice v rozsahu 4 Man-day (MJ)
Implementačné a optimalizačné práce pre prostredie ESET Inspect alebo ekvivalent (uchádzač uvedie presný názov ním ponúkaného riešenia) v rozsahu 12 MJ
Implementácia a konfigurácia sandbox funkcionality na endpointoch.
Technické školenie pre administrátorov verejného obstarávateľa na nástroj ESET Inspect alebo ekvivalent v poslednej vydanej verzii (najaktuálnejšie dostupnej na trhu) v rozsahu 2 MJ
Technické školenie pre administrátorov verejného obstrávateľa na nástroje ESET Protect alebo ekvivalent v rozsahu 1 MJ
Súčasťou dodania predmetu zákazky je poskytovanie aktualizácií (update), nových verzií (upgrade) alebo podpory obstarávaných licencií.
Poskytovanie služieb rozšírenej servisnej podpory formou SLA s aktívnym monitoringom pre XDR platformu a na prenosné zariadenia prostredníctvom centrálnej konzoly na obdobie min. 12 mesiacov.

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	Hodnota/Charakteristika			

Položka č. 3: Poskytovanie služieb rozšírenej servisnej on site podpory formou SLA pre platformu výrobcu ESET pre prostredie ESET Protect a ESET Inspect na 12 mesiacov

Funkcia
Poskytovanie služieb rozšírenej servisnej podpory s aktívnym monitoringom ESET Inspect riešenia a centrálnej konzoly ESET PROTECT alebo ekvivalentné riešenie

Podpora poskytovaná 8x5, v prac. dňoch v čase 7:00-15:00 h, potvrdenie prijatia požiadavky na servisný zásah do min. 60 minút, nástup na riešenie najneskôr do 4 h od nahlásenia incidentu.
Nástup na riešenie najneskôr do 4 hodín od nahlásenia incidentu, ktorý sa vzťahuje na ESET PROTECT a ESET Inspect prostredia (alebo ekvivalent)

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	**Hodnota/Charakteristika**			

Položka č. 4: Rozsah podpory - Komplexná starostlivosť o prevádzku ESET Inspect riešenia pozostávajúceho z ESET Protect

Funkcia				
Rozsah podpory - Komplexná starostlivosť o prevádzku XDR platformy alebo ekvivalentu charakteristický pre balík ESET PROTECT Enterprise (alebo ekvivalent)				
Proaktívne riešenie vznikajúcich problémov v rozsahu 1 MD mesačne. V rámci tejto aktivity sú požadované nasledovné min. činnosti pre riešenie (resp. ekvivalentné riešenie, ktoré spĺňa min. požadované činnosti):				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Technické vlastnosti	**Hodnota/Charakteristika**			
-	- Proaktívny monitoring vybraných parametrov a dostupnosť všetkých služieb aplikačného riešenia EDR/XDR serverového systému			
-	- Aktívny monitoring EDR/XDR pravidiel s príslušným notifikačným mechanizmom			
-	- Nastavovanie pravidelných reportov podľa požiadaviek objednávateľa v celkom rozsahu 2 reporty za mesiac			
-	Security podpora pre ESET endpointové produkty:			
-	• Malware: chýbajúca detekcia			
-	• Malware: problém s liečením			
-	• Malware: infekcia ransomvérom			
-	• Zachytenie False positive			
-	• Vyšetrenie podozrivého správania			
-	Vyšetrenie malware incidentu a odozva na vzniknutý malware incident:			
-	• Základná analýza zaslaného súboru			
-	• Detailná analýza zaslaného súboru			
-	• Analýza a vyšetrenie odovzdaných súvisiacich dát			
-	• Asistencia pri odozve/protiopatreniach na malware incident			
-	Security podpora pre EDR/XDR:			
-	• Podpora s vytváraním EDR/XDR pravidiel			
-	• Podpora s vytváraním EDR/XDR výnimiek			
-	• ESET Inspect operatívna optimalizácia prostredia			
-	• ESET Inspect služba Threat Hunting alebo ekvivalent (poskytovaná na požiadanie zo strany objednávateľa)			
Pravidelné vyhodnocovanie EDR/XDR incidentov na mesačnej báze s príslušným návrhom opatrení a reštrikcií	- V mesačnej správe zahrnuté aj vyhotovenie úplného ročného analytického reportu, ktorý bude sumarizovať všetky zistenia a odporúčania za ročné sledované obdobie			
-	- Kontrola logov			
-	- Aktualizácia aplikačného vybavenia v zmysle odporúčaní výrobcom			
-	- Dodanie informácií o známych bezpečnostných chybách a aplikovanie náprav			
-	- Vo fáze poskytovania podpory, pravidelné stretnutia pracovnej skupiny min. 1x mesačne			

-	- Evidencia EDR/XDR incidentov a úprav na on-line portáli/HelpDesku

Položka č. 5: Antivírusové riešenie pre koncové body a servery:

Funkcia
Podporované klientske platformy OS - min. Windows, Linux, MacOS, Android, všetko v slovenskom alebo českom jazyku Natívna podpora architektúr pre platformy Windows a MacOS: x86, x64, ARM64
Antimalware, antiransomware, antispyware a anti-phishing na aktívnu ochranu pred všetkými typmi hrozieb
Personálny firewall pre zabránenie neautorizovanému prístupu k zariadeniu so schopnosťou automatického prebratia pravidiel z brány Windows Firewall.
Modul pre ochranu operačného systému a elimináciu aktivít ohrozujúcich bezpečnosť zariadenia s možnosťou definovať pravidlá pre systémové registre, procesy, aplikácie a súbory
Ochrana pred neautorizovanou zmenou nastavenia / vyradenie z prevádzky / odinštalovaním antimalware riešení a kritických nastavení a súborov operačného systému
Aktívna aj pasívna heuristická analýza pre detekciu doposiaľ neznámych hrozieb
Systém na blokáciu exploitov zneužívajúcich zero-day zraniteľností, ktorý pokrýva najpoužívanejšie vektory útoku: min. sieťové protokoly, Flash Player, Java, Microsoft Office, webové prehliadače, e-mailových klientov, PDF čítačky
Systém na detekciu malwaru už na sieťovej úrovni poskytujúci ochranu aj pred zneužitím zraniteľností na sieťovej vrstve
Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).
Anti-phishing so schopnosťou detekcie homoglyph útokov
Kontrola RAM pamäte pre lepšiu detekciu malwaru využívajúcu silnú obfuskáciu a šifrovanie
Cloud kontrola súborov pre urýchlenie skenovania fungujúce na základe reputácie súborov.
Kontrola súborov v priebehu sťahovania pre zníženie celkového času kontroly
Kontrola súborov pri zapisovaní na disku a extrahovaní archivačných súborov
Detekcia s využitím strojového učenia
Funkcia ochrany proti zapojeniu do botnetu pracujúcej s detekciou sieťových signatúr
Ochrana pred sieťovými útokmi skenujúca sieťovú komunikáciu a blokujúca pokusy o zneužitie zraniteľností na sieťovej úrovni
Kontrola s podporou cloudu pre odosielanie a online vyhodnocovanie neznámych a potenciálne škodlivých aplikácií.
Lokálny sandbox
Modul behaviorálnej analýzy pre detekciu správania nových typov ransomwaru
Systém reputácie pre získanie informácií o závadnosti súborov a URL adries
Cloudový systém na detekciu nového malwaru ešte nezaneseného v aktualizáciách signatúr
Technológia na detekciu rootktitov obvykle sa maskujúcich za súčasti operačného systému.
Skener firmvéru BIOSu a UEFI
Skenovanie súborov v cloude OneDrive
Funkcionalita pre MS Windows v min. rozsahu: Antimalware, Antispyware, Personal Firewall, Personal IPS, Application Control, Device control, Security Memory (zabraňuje útokom na bežiace aplikácie), kontrola integrity systémových komponentov
Funkcionalita pre k MacOS v min. rozsahu- Personal Firewall, Device control, autoupgrade
Možnosť aplikovania bezpečnostných politík aj v offline režime na základe definovaných podmienok
Ochrana proti pokročilým hrozbám (APT) a 0-day zraniteľnostiam
Podpora automatického vytvárania dump súborov na stanici na základe nálezov
Okamžité blokovanie/mazanie napadnutých súborov na stanici (s možnosťou stiahnutia administrátorom na ďalšiu analýzu)
Duálny aktualizačný profil pre možnosť sťahovania aktualizácií z mirroru v lokálnej sieti a zároveň vzdialených serverov pri nedostupnosti lokálneho mirroru (pre cestujúcich používateľov s notebookmi).
Možnosť definovať webové stránky, ktoré sa spustia v chránenom režime prehliadača, pre bezpečnú prácu s kritickými systémami alebo internetovým bankovníctvo
Aktívne ochrany pred útokmi hrubou silou na protokol SMB a RDP

Možnosť zablokovania konkrétnej IP adresy po sérii neúspešných pokusov o prihlásenie pre protokoly SMB a RDP s možnosťou výnimiek vo vnútorných sieťach
Automatické aktualizácie bezpečnostného softvéru s možnosťou odloženia reštartu stanice.
"Zmrazenie“ na požadovanej verzii – produkt je možné nakonfigurovať tak, aby nedochádzalo k automatickému povyšovaniu majoritných a minoritných verzií najmä na staniciach, kde sa vyžaduje vysoká stabilita

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	Hodnota/Charakteristika			

Položka č. 6: Integrovaná cloudová analýza neznámych vzoriek

Funkcia
Funkcia cloudového sandboxu je integrovaná do produktu pre koncové a serverové zariadenia, tzn. Cloudový sandbox nemá vlastného agenta, nevyžaduje inštaláciu ďalšie komponenty či už v rámci produktu alebo implementácie HW prvku do siete
Sandbox umožňujúci spustenie vzoriek malwaru pre: • Windows • Linux
Možnosť využitia na koncových bodoch a serveroch pre aktívnu detekciu škodlivých súborov
Analýza neznámych vzoriek v rade jednotiek minút
Optimalizácia pre znemožnenie obídenia anti-sandbox mechanizmy
Schopnosť analýzy rootkitov a ransomvéru
Schopnosť detekcie a zastavenie zneužitia alebo pokusu o zneužitie zero day zraniteľnosti
Riešenie pracuje s behaviorálnou analýzou
Kompletný výsledok o zanalyzovanom súbore vrátane informácie o nájdenom i nenájdenom škodlivom správaní daného súboru
Manuálne odoslanie vzorky do sandboxu
Možnosť proaktívnej ochrany, kedy je potenciálna hrozba blokovaná, pokiaľ nie je známy výsledok analýzy zo sandboxu
Neobmedzené množstvo odosielaných súborov
Všetka komunikácia prebieha šifrovaným kanálom
Okamžité odstránenie súboru po dokončení analýzy v cloudovom sandboxe
Možnosť voľby, aké kategórie súborov do cloudového sandboxu budú odchádzať (spustiteľné súbory, archívy, skripty, pravdepodobný spam, dokumenty atp.)
Veľkosť odoslaných súborov do cloudového sandboxu môže dosahovať až 64MB
Výsledky analyzovaných súborov sú dostupné a automatizovane distribuované všetkým serverom a staniciam naprieč organizáciou, tak aby nedochádzalo k duplicitnému testovaniu

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	Hodnota/Charakteristika			

Položka č. 7: Šifrovanie celých diskov

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

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	**Hodnota/Charakteristika**			

Položka č. 8: XDR riešenie

Funkcia
Možnosť prevádzky centrálneho servera v cloude alebo on-premise na platforme Windows Server
Webová konzola pre správu a vyhodnotenie
Možnosť prevádzky s databázami: Microsoft SQL, MySQL
Možnosť prevádzky v offline prostredí
Autonómne správanie so schopnosťou vyhodnotiť podozrivú/ škodlivú aktivitu a zareagovať na ňu aj bez aktuálne dostupného riadiaceho servera alebo internetového pripojenia
Logovanie činností administrátora (tzv.Audit Log)
Podpora EDR pre systémy Windows, Windows server, MacOS a Linux
Možnosť autentizácie do manažmentu EDR pomocou 2FA
Možnosť riadenia manažmentu EDR prostredníctvom API, a to ako pre: Prijímanie informácií z EDR serverov aj Zasielanie príkazov na EDR servery
Integrovaný nástroj v EDR riešení pre vzdialené zasielanie príkazov priamo z konzoly
Možnosť izolácie zariadenia od siete
Možnosť tvorby vlastných IoC
Možnosť škálovania množstva historických dát vyhodnotených v EDR min. 3 mesiace pre raw-data a min. 3 roky pre detekované incidenty.
„učiaci režim“ pre automatizované vytváranie výnimiek k detekčným pravidlám
Indikátory útoku pracujúce s behaviorálnou detekciou
Indikátory útoku pracujúce s reputáciou
Riešenie umožnuje analýzu vektorov útoku
Schopnosť detekcie: min. škodlivých spustiteľných súborov: skriptov, exploitov, rootkitov, sieťových útokov, zneužitie WMI nástrojov, bezsúborového malwaru, škodlivých systémových ovládačov / kernel modulov, pokusov o dump prihlasovacích údajov užívateľa
Schopnosť detekovať laterálny pohyb útočníka
Analýza procesov, všetkých spustiteľných súborov a DLL knižníc.
Náhľad na spustené skripty použité pri detegovanej udalosti
Možnosť zabezpečeného vzdialeného spojenia cez servery výrobcu do konzoly EDR
Schopnosť automatizovaného response úkonu pre jednotlivé detekčné pravidlá v podobe: izolácia stanice, blokácia hash súboru, blokácia a vyčistenie siete od konkrétneho súboru, ukončení procesu, reštart počítača, vypnutie počítača
Možnosť automatického vyriešenia incidentu administrátorom
Prioritizácia vzniknutých incidentov
Možnosť stiahnutia spustiteľných súborov zo staníc pre bližšiu analýzu vo formáte archívu opatreným heslom
Integrácia a zobrazenie detekcií vykonaných antimalware produktom
Riešenie je schopné generovať tzv. forest/full execution tree model
Vyhľadávanie pomocou novo vytvorených IoC nad historickými dátami
Previazanie s technikami popísanými v knowledge base MITRE ATT&CK
Integrovaný vyhľadávač VirusTotal s možnosť rozšírenia o vlastné vyhľadávače

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	**Hodnota/Charakteristika**			

Položka č. 9: Management konzola pre správu všetkých riešení v rámci ponúkaného balíka v rozsahu:

Funkcia

Možnosť prevádzkovať jednotnú management konzolu na správu týchto riešení v cloudovom nasadení alebo lokálnom (on-prem) nasadení
Webová konzola
Možnosť inštalácie na Windows aj Linux
Predpripravená virtual appliance pre virtuálne prostredie VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box
Server/proxy architektúra pre sieťovú pružnosť – zníženie záťaže pri sťahovaní aktualizácií detekčných modulov výrobcu
Možnosť prebudenia klientov pomocou Wake On Lan
Vzdialené vypnutie, reštart počítača alebo odhlásenie všetkých užívateľov
Možnosť konfigurácie virtual appliance cez užívateľsky prívetivé webové rozhranie Webmin
Nezávislí manažment agent pre platformy Windows, Linux a MacOS
Management agent pre architektúry na platformy Windows a MacOS: x86, x64, ARM64
Nezávislý agent (pracuje aj offline) vzdialenej správy pre zabezpečenie komunikácie a ovládania operačného systému verejného obstarávateľa
Offline uplatňovanie politík a spúšťanie úloh pri výskyte definovanej udalosti (napríklad: odpojenie od siete pri nájdení škodlivého kódu).
Administrácia v najpoužívanejších jazykoch vrátane slovenčiny
Široké možnosti konfigurácie oprávnení administrátorov (napríklad možnosť správy iba časti infraštruktúry, ktoré konkrétnemu administrátorovi podlieha)
Zabezpečenie prístupu administrátorov do vzdialenej správy pomocou 2FA
Podpora štítkov/tagovania pre jednoduchšiu správu a vyhľadávanie
Správa karantény s možnosťou vzdialeného vymazania / obnovenia / obnovenia a vylúčenia objektu z detekcie
Vzdialené získanie zachyteného škodlivého súboru
Detekcia nespravovaných (rizikových) počítačov komunikujúcich na sieti.
Podpora pre inštalácie a odinštalácie aplikácií 3.strán
Vyčítanie informácií o verziách softvéru 3. strán
Možnosť vyčítať informácie o hardvéri na spravovaných zariadeniach (CPU, RAM, diskové jednotky, grafické karty…).
Možnosť vyčítať sériové číslo zariadenia
Možnosť vyčítať voľné miesto na disku
Detekcia aktívneho šifrovania BitLocker na spravovanej stanici
Zobrazenie časovej informácie o poslednom boote stanice
Odoslanie správy na počítač / mobilné zariadenie, ktoré sa následne zobrazí užívateľovi na obrazovke
Vzdialené odinštalovanie antivírusového riešenia 3. strany
Vzdialené spustenie akéhokoľvek príkazu na cieľovej stanici pomocou Príkazového riadka
Dynamické skupiny pre možnosť definovania podmienok, za ktorých dôjde k automatickému zaradeniu klienta do požadovanej skupiny a automatickému uplatneniu klientskej úlohy
Automatické zasielanie upozornení pri dosiahnutí definovaného počtu alebo percent ovplyvnených klientov (napríklad: 5 % všetkých počítačov / 50 klientov hlási problémy)
Podpora SNMP Trap, Syslogu a qRadar SIEM
Podpora formátov pre Syslog správy: CEF, JSON, LEEF
Podpora inštalácie skriptom - *.bat, *.sh, *.ini (GPO, SSCM…).
Rýchle pripojenie na klienta pomocou RDP z konzoly pre vzdialenú správu.
Reportovanie stavu klientov chránených inými bezpečnostnými programami.
Schopnosť zaslať reporty a upozornenia na e-mail
Konzola podporuje multidoménové prostredie (schopnosť pracovať s viacerými AD štruktúrami)
Konzola podporuje multitenantné prostredie (schopnosť v jednej konzole spravovať viac počítačových štruktúr)
Podpora VDI prostredia (Citrix, VMware, SCCM, apod)
Podpora klonovania počítačov pomocou golden image

Podpora inštanciách klonov
Podpora obnovy identity počítača pre VDI prostredie na základe FQDN
Možnosť definovať viacero menných vzorov klonovaných počítačov pre VDI prostredie
Pridanie zariadenia do vzdialenej správy pomocou: synchronizácia s Active Directory, ručné pridanie pomocou podľa IP adresy alebo názvu zariadenia, pomocou sieťového skenu nechránených zariadení v sieti, Import cez csv súbor

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Technické vlastnosti	**Hodnota/Charakteristika**			

2.3 Osobitné požiadavky na plnenie:

Názov
Podpora musí byť vykonávaná v miestach inštalácie. Pokiaľ to charakter konkrétneho incidentu umožňuje, je možné podporu vykonať aj z akéhokoľvek miesta, z ktorého je možné bezpečné pripojenie k podporovanému EDR/XDR riešeniu.
Dodávateľ sa zaväzuje do 3 pracovných dní od účinnosti zmluvy predložiť objednávateľovi kontaktné údaje osoby/osôb zodpovednej za riadne plnenie predmetu zmluvy v rozsahu: meno, priezvisko, telefónne číslo a e-mail a zároveň predloží aj telefónne číslo a e-mailovú adresu na hlásenie servisných požiadaviek objednávateľom.
Zmluvná cena bude rovnomerne rozdelená medzi 24 mesiacov, 12 mesiacov (servis) a fakturovaná v pravidelných mesačných platbách počas doby trvania Zmluvy na základe faktúr zasielaných Dodávateľom prostredníctvom elektronického alebo poštového styku. Dodávateľ nie je oprávnený navýšiť cenu o žiadne položky mimo zmluvnej ceny (doprava, náhradné diely a pod.).
Dodávateľ do 3 dní od nadobudnutia účinnosti Zmluvy preukáže, že disponuje vlastným systémom na nahlasovanie porúch v režime 8x5 a to minimálne telefonicky, e-mailom s centrálnou adresou monitorovanou počas poskytovania podpory, prípadne možnosťou integrácie na centrálny dispečing objednávateľa.
Dodávateľ musí uviesť minimálne jednu referenciu reálneho nasadenia a podpory formou SLA pre ESET Inspect riešenie, spolu v minimálnom rozsahu 300 koncových staníc za obdobie 3 rokov.
Požaduje sa predložiť rozpis sadzby DPH a ceny s DPH alebo bez DPH, ktorá ako údaj v zmluve chýba v prípade plnenia zahŕňajúce rôzne sadzby DPH do 7 dní od uzavretia zmluvy.
Ak je Dodávateľ identifikovaný pre DPH v inom členskom štáte EÚ a tovar bude do SR prepravený z iného členského štátu EÚ, tento Dodávateľ nebude pri plnení Zmluvy fakturovať DPH. Vo svojej Kontraktačnej ponuke však musí uviesť príslušnú sadzbu a výšku DPH podľa zákona č. 222/2004 Z.z. a cenu vrátane DPH. Objednávateľ nie je zdaniteľnou osobou a v tomto prípade je/bude registrovaný pre DPH podľa § 7 zákona č. 222/2004 Z.z. a bude povinný odviesť DPH v SR podľa zákona č. 222/2004 Z.z..
Nový, doposiaľ nepoužitý tovar.
Nový, doposiaľ nepoužitý krabicový softvér.
Zmena termínu dodania je možná po dohode s poverenou osobou za objednávateľa písomne prostredníctvom e-mailu.
Zmluvné strany sa dohodli, že dodávateľ v postavení veriteľa nepostúpi akúkoľvek svoju pohľadávku z tejto zmluvy tretej osobe bez predchádzajúceho písomného súhlasu dlžníka - objednávateľa. Písomný súhlas objednávateľa s týmto úkonom je zároveň platný len za podmienky, že bol na tento úkon udelený predchádzajúci písomný súhlas Ministerstva zdravotníctva SR. V prípade, že dôjde zo strany zhotoviteľa k porušeniu tejto povinnosti a svoje práva a povinnosti z tejto zmluvy postúpi tretej osobe bez súhlasu protistrany, bude sa takýto úkon pre účely tohto zmluvného vzťahu považovať za neplatný.
V prípade, ak sa po uzatvorení tejto zmluvy preukáže, že na relevantnom trhu existuje cena (ďalej tiež ako „nižšia cena“) za rovnaké alebo porovnateľné plnenie, ako je obsiahnuté v tejto zmluve a dodávateľ už preukázateľne za takúto nižšiu cenu plnenie poskytol, resp. ešte stále poskytuje,
pričom rozdiel medzi nižšou cenou a cenou podľa tejto zmluvy je viac ako 5 % v neprospech ceny podľa tejto zmluvy, zaväzuje sa dodávateľ poskytnúť objednávateľovi pre takéto plnenie objednané po preukázaní tejto skutočnosti dodatočnú zľavu vo výške rozdielu medzi ním poskytovanou cenou podľa tejto zmluvy a nižšou cenou.
Faktúry sú splatné v lehote 30 dní odo dňa ich doručenia na adresu sídla objednávateľa.
Dodávateľ do 7 dní od uzatvorenia zmluvy predloží objednávateľovi rozpočet.
Vrátane dopravy na miesto plnenia
Vrátane inštalácie na mieste plnenia

Názov	Upresnenie

Doklad preukazujúci, že uchádzač je oficiálnym partnerom spoločnosti ESET v Slovenskej republike pre ponúkané riešenie (pokiaľ uchádzač nie je priamo spoločnosť ESET) alebo doklad preukazujúci, že uchádzač je oficiálnym partnerom výrobcu ním ponúkaného ekvivalentného riešenia (resp. tovaru)	
Úroveň partnerstva uchádzača musí byť verifikovateľná z verejných zdrojov (napr. webstránka výrobcu), alebo takéto partnerstvo uchádzač preukáže dokladom - originálnym vyhotovením dokladu resp. úradne overenou kópiou - písomným potvrdením výrobcu uchádzačom ponúkaného riešenia resp. tovaru).	
Ddoklad preukazujúci, že uchádzač disponuje vlastným systémom na nahlasovanie vád v režime 24x7 a to minimálne telefonicky, e-mailom s centrálnou adresou monitorovanou počas poskytovania podpory, prípadne možnosťou integrácie na centrálny dispečing verejného obstrávateľa (doklad uchádzač predloží napr. formou čestného vyhlásenia uchádzača)	
"Uchádzač preukáže, že disponuje min. 1 špecialistom (v úhrne) pre všetky moduly ESET riešení, alebo ním ponúkaného ekvivalentného riešenia (resp. tovaru) a to: - Základné technické znalosti ESET riešení, alebo ekvivalent,-	
1Uchádzač preukáže, že disponuje min. 1 špecialistom - predkladá doklady (napr. certifikáty osôb), ktoré budú v rámci plnenia predmetu zákazky na riešenie bezpečnostných, prevádzkových incidentov a diagnostiky pre EDR/XDR platformu. Dokladmi uchádzač preukáže, že disponuje osobami- špecialistami ESET Optimization Specialist alebo uchádzač predkladá doklady 1 špecialistu ním ponúkaného ekvivalentného riešenia (doklady musia byť potvrdené resp. vydané výrobcom tovaru resp. riešenia)	
Uchádzač preukáže, že disponuje certifikáciou ISO/IEC 27001 (systém manažérstva informačnej bezpečnosti)	
Uchádzač preukáže dokladom, že disponuje min. 1 špecialistom s certifikáciou Manažér kybernetickej bezpečnosti.	

2.4 Prílohy opisného formulára Zmluvy:

Popis	Názov súboru

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát: Slovenská republika

Kraj:	Prešovský
Okres:	Stará Ľubovňa
Obec:	Stará Ľubovňa
Ulica:	Obrancov Mieru 3

3.2 Čas / lehota plnenia zmluvy:

20.05.2024 08:00:00 - 23.05.2024 14:00:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka:	súbor
Požadované množstvo:	1,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronickej platformy verzia 1.2, účinná odo dňa 3. 11. 2022 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 18 750,00 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 22 500,00 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronickej platformy uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv Trhoviska.

5.5 Túto Zmluvu bude možné meniť a dopĺňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:
Príloha č.1 Obchodné podmienky elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

V Bratislave, dňa 16.05.2024 15:10:01

Objednávateľ:
Ľubovnianska nemocnica, n.o.
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
iServices s. r. o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska