Opis predmetu zákazky

Špecifikácia činností, tvoriacich predmet zákazky:
(Poznámka: Ak sa niekde v nasledovnom texte Opisu predmetu zákazky uvádzajú prílohy, myslia sa tým prílohy ku tomuto opisu predmetu zákazky a sú uvedené ako osobitný dokument. Prílohy ku súťažným podkladom sú uvedené v tomto dokumente).

Predmet zákazky

Predmetom verejného obstarávania je v súlade s § 3 ods. 3 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní" v príslušnom gramatickom tvare) zákazka na uskutočnenie stavebných prác.

Bližšia špecifikácia opisu predmetu zákazky je uvedená v prílohe č. 1

Podrobné vymedzenie predmetu zákazky tvorí samostatnú časť súťažných podkladov rozpočet spracovaný verejným obstarávateľom. a záväzok obstarávateľskej organizácie dielo zhotovené v súlade so stanovenými podmienkami v týchto súťažných podkladoch.

Nasledovné dokumenty tvoria neoddeliteľnú súčasť časti Opisu predmetu zákazky týchto súťažných podkladov a majú poradie záväznosti uvedené v zostupnom poradí:

a) Časť Opis predmetu zákazky
b) Prípadné vysvetlenia podľa zákona o verejnom obstarávaní
c) Rozpočet (výkaz výmer/kalkulácia ceny predmetu)

Prílohy časti Opisu predmetu zákazky:

Príloha č. 1 Funkčná špecifikácia

Podrobná technická špecifikácia

Podrobný opis je uvedený v návrhu Zmluvy, ktorá tvorí prílohu č. 3 týchto súťažných podkladov.

Všeobecné ustanovenia

Každá ponuka na uskutočnenie zákazky musí spĺňať všetky požadované funkčné charakteristiky a technické parametre podľa tejto časti Opis predmetu zákazky týchto súťažných podkladov, podľa tejto časti Opisu predmetu zákazky, a podľa rozpočtu. Technické riešenie uchádzača musí zodpovedať svojimi parametrami technickej špecifikácii, výkonnostným, dizajnovým a funkčným požiadavkám obstarávateľskej organizácie uvedenými v tejto časti Opisu predmetu zákazky a jej prílohách (rozpočet, prípadne vysvetlenia).

Zákazka je v celom rozsahu opísaná tak, aby bola presne a zrozumiteľne špecifikovaná. Ak niektorý z použitých parametrov, alebo rozpätie parametrov identifikuje konkrétny typ výrobku, alebo výrobok konkrétneho výrobcu, obstarávateľská organizácia umožní nahradiť takýto výrobok ekvivalentným výrobkom alebo ekvivalentom technického riešenia pod podmienkou, že ekvivalentný výrobok alebo ekvivalentné technické riešenie bude spĺňať rovnaké alebo lepšie úžitkové, prevádzkové a funkčné charakteristiky, ako pôvodný výrobok alebo technické riešenie. T. z. že pri výrobkoch, príslušenstvách konkrétnej značky, uchádzač môže predložiť aj ekvivalenty inej značky v rovnakej alebo vyššej kvalite podľa príslušných platných technických noriem.

Pre účely tohto verejného obstarávania sú ekvivalentnými výrobkami a technickými riešeniami také výrobky a technické riešenia, ktoré spĺňajú úžitkové, prevádzkové a funkčné charakteristiky, ktoré sú nevyhnutné na zabezpečenie účelu, na ktoré sú výrobky určené.

Uchádzač je povinný ekvivalentný výrobok a technické riešenie predložiť zdokumentovateľným spôsobom tak, aby obstarávateľská organizácia mohla vyhodnotiť ponuku z pohľadu splnenia požiadaviek na predmet zákazky.

PODMIENKY TÝKAJÚCE SA ZÁKAZKY:
Verejný obstarávateľ si vyhradzuje právo neprijať ponuku, ktorá prekročí finančný limit zákazky, t.j. **predpokladanú hodnotu zákazky, uvedenú v oznámení o vyhlásení verejného obstarávania.**

Podmienky vykonania zákazky sú uvedené v návrhu Zmluvy, ktorá tvorí prílohu č. 3 týchto súťažných podkladov.

Predmet zákazky: **UPGRADE ANTIVÍRUSOVÉHO SOFTVÉRU ESET A SLUŽBY ROZŠÍRENEJ PODPORY KYBERNETICKEJ BEZPEČNOSTI S AKTÍVNYM MONITORINGOM XDR PLATFORMY**

FUNKČNÁ ŠPECIFIKÁCIA PREDMETU ZÁKAZKY

Predmetom zákazky je dodanie (predĺženie licencie) 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, správu zraniteľností a patchov aplikácií tretích strán, ochranu poštových serverov/mailboxov, ochranu cloudového prostredia Microsoft365/Google Workspace, nástroj na 2-faktorovú autentifikáciu, a možnosť prevádzkovať jednotnú management konzolu na správu týchto riešení v cloudovom nasadení alebo lokálnom (on-prem) nasadení podľa voľby obstarávateľa za účelom povýšenia kybernetickej bezpečnosti. Prostredie verejného obstarávateľa spadá do kritickej infraštruktúry. Dĺžka licencie a trvania služieb : 24 mesiacov

EKVIVALENT:

Verejný obstrávateľ prispúšťa aj predloženie ekvivalentného riešenia za podmienky, že uchádzačom predložený ekvivalent bude spĺňať všetky min. požiadavky vereného obstrávateľa 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 vlastnostami a kvalitou, za podmienky zabezpečenia plného prechodu zo súčasne využívaného antivírusového balíka (ESET) na uchádzačom navrhované riešenie bez akýkoľvek strát údajov resp. služieb, ktoré využíva verejný obstrávateľ. V prípade predloženia ekvivalentu musí zároveň uchádzač garantovať bezchybnú implementáciu (bez akejkoľvek straty dát verejného obstrávateľa) ním návrhovaného ekvivalentného riešenia v prostredí verejného obstrávateľa. 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 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 obstrávania 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 presiahnúť viac ako 3 pracovných dní (implementácia v prostredí verejného obstrávania).

CPV: 48761000-0 Antivírusový softvérový balík,72261000-2 Softvérové podporné služby;72250000-2 Služby

Požadované minimálne technické vlastnosti, parametre a hodnoty

		parametre			
		MJ	**min.**	**max.**	**presne**
1.	Licencie ESET PROTECT Elite alebo ekvivalent, na licenčné obdobie 24 mesiacov s rozšírenou servisnou podporou formou SLA na obdobie 24 mesiacov				vyžaduje sa
1.1.	Dodanie licencií ESET PROTECT Elite alebo ekvivalent pre ochranu min. 300 endpointov				vyžaduje sa
1.2.	Dodanie implementačných, konfiguračných prác pre XDR platformu ESET PROTECT Elite alebo ekvivalent				vyžaduje sa
1.3.	Implementácia prostredia ESET PROTECT alebo ekvivalent (centrálneho manažmentu) pre serverové prostredie, pracovné stanice v rozsahu	deň	3		
1.4.	Implementácia a konfigurácia mailovej bezpečnosti ECOS, alebo ekvivalent pre O365 a Google prostredie v minimálnom rozsahu 3 človekodní	deň	3		
1.5.	Implementačné a optimalizačné práce pre prostredie ESET Inspect alebo ekvivalent (uchádzač uvedie presný názov ním ponúkaného riešenia) v rozsahu	deň	21		
1.6.	Implementácia a konfigurácia sandbox funkcionality na endpointoch.				vyžaduje sa
1.7.	Technické školenie pre administrátorov verejného obstarávateľa na nástroj ESET Inspect v poslednej vydanej verzii (najaktuálnejšie dostupnej na trhu) v rozsahu	deň	1		

1.8.	Technické školenie pre administrátorov verejného obstrávateľa na nástroje ESET Protect v rozsahu	deň	1		
1.9.	Súčasťou dodania predmetu zákazky je poskytovanie aktualizácií (update), nových verzií (upgrade) alebo podpory obstarávaných licencií.				vyžaduje sa
1.10.	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.				vyžaduje sa

Bližšia min. technická špecifikácia na softvérové riešenie pre prostredie XDR:					
2.	**Antivírusové riešenie pre koncové body a servery:**				
2.1.	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				vyžaduje sa
2.2.	Antimalware, antiransomware, antispyware a anti-phishing na aktívnu ochranu pred všetkými typmi hrozieb				vyžaduje sa
2.3.	Personálny firewall pre zabránenie neautorizovanému prístupu k zariadeniu so schopnosťou automatického prebratia pravidiel z brány Windows Firewall.				vyžaduje sa
2.4.	Modul pre ochranu operačného systému a elimináciu aktivít ohrozujúcich bezpečnosť zariadenia s možnosťou definovať pravidlá pre systémové registre, procesy, aplikácie a súbory				vyžaduje sa
2.5.	Ochrana pred neautorizovanou zmenou nastavenia / vyradenie z prevádzky / odinštalovaním antimalware riešení a kritických nastavení a súborov operačného systému				vyžaduje sa
2.6.	Aktívna aj pasívna heuristická analýza pre detekciu doposiaľ neznámych hrozieb				vyžaduje sa
2.7.	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				vyžaduje sa
2.8.	Systém na detekciu malwaru už na sieťovej úrovni poskytujúci ochranu aj pred zneužitím zraniteľností na sieťovej vrstve				vyžaduje sa
2.9.	Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).				vyžaduje sa
2.10.	Anti-phishing so schopnosťou detekcie homoglyph útokov				vyžaduje sa
2.11.	Kontrola RAM pamäte pre lepšiu detekciu malwaru využívajúcu silnú obfuskáciu a šifrovanie				vyžaduje sa
2.12.	Cloud kontrola súborov pre urýchlenie skenovania fungujúce na základe reputácie súborov.				vyžaduje sa
2.13.	Kontrola súborov v priebehu sťahovania pre zníženie celkového času kontroly				vyžaduje sa
2.14.	Kontrola súborov pri zapisovaní na disku a extrahovaní archivačných súborov				vyžaduje sa
2.15.	Detekcia s využitím strojového učenia				vyžaduje sa
2.16.	Funkcia ochrany proti zapojeniu do botnetu pracujúcej s detekciou sieťových signatúr				vyžaduje sa
2.17.	Ochrana pred sieťovými útokmi skenujúca sieťovú komunikáciu a blokujúca pokusy o zneužitie zraniteľností na sieťovej úrovni				vyžaduje sa
2.18.	Kontrola s podporou cloudu pre odosielanie a online vyhodnocovanie neznámych a potenciálne škodlivých aplikácií.				vyžaduje sa
2.19.	Lokálny sandbox				vyžaduje sa
2.20.	Modul behaviorálnej analýzy pre detekciu správania nových typov ransomwaru				vyžaduje sa
2.21.	Systém reputácie pre získanie informácií o závadnosti súborov a URL adries				vyžaduje sa
2.22.	Cloudový systém na detekciu nového malwaru ešte nezaneseného v aktualizáciách signatúr				vyžaduje sa

2.23.	Technológia na detekciu rootktitov obvykle sa maskujúcich za súčasti operačného systému.				vyžaduje sa
2.24.	Skener firmvéru BIOSu a UEFI				vyžaduje sa
2.25.	Skenovanie súborov v cloude OneDrive				vyžaduje sa
2.26.	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				vyžaduje sa
2.27.	Funkcionalita pre k MacOS v min. rozsahu- Personal Firewall, Device control, autoupgrade				vyžaduje sa
2.28.	Možnosť aplikovania bezpečnostných politík aj v offline režime na základe definovaných podmienok				vyžaduje sa
2.29.	Ochrana proti pokročilým hrozbám (APT) a 0-day zraniteľnostiam				vyžaduje sa
2.30.	Podpora automatického vytvárania dump súborov na stanici na základe nálezov				vyžaduje sa
2.31.	Okamžité blokovanie/mazanie napadnutých súborov na stanici (s možnosťou stiahnutia administrátorom na ďalšiu analýzu)				vyžaduje sa
2.32.	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).				vyžaduje sa
2.33.	Možnosť definovať webové stránky, ktoré sa spustia v chránenom režime prehliadača, pre bezpečnú prácu s kritickými systémami alebo internetovým bankovníctvo				vyžaduje sa
2.34.	Aktívne ochrany pred útokmi hrubou silou na protokol SMB a RDP				vyžaduje sa
2.35.	Možnosť zablokovania konkrétnej IP adresy po sérii neúspešných pokusov o prihlásenie pre protokoly SMB a RDP s možnosťou výnimiek vo vnútorných sieťach				vyžaduje sa
2.36.	Automatické aktualizácie bezpečnostného softvéru s možnosťou odloženia reštartu stanice.				vyžaduje sa
2.37.	"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				vyžaduje sa
3.	**Integrovaná cloudová analýza neznámych vzoriek**				
3.1.	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				vyžaduje sa
3.2.	Sandbox umožňujúci spustenie vzoriek malwaru pre: • Windows • Linux				vyžaduje sa
3.3.	Možnosť využitia na koncových bodoch a serveroch pre aktívnu detekciu škodlivých súborov				vyžaduje sa
3.4.	Analýza neznámych vzoriek v rade jednotiek minút				vyžaduje sa
3.5.	Optimalizácia pre znemožnenie obídenia anti-sandbox mechanizmy				vyžaduje sa
3.6.	Schopnosť analýzy rootkitov a ransomvéru				vyžaduje sa
3.7.	Schopnosť detekcie a zastavenie zneužitia alebo pokusu o zneužitie zero day zraniteľnosti				vyžaduje sa
3.8.	Riešenie pracuje s behaviorálnou analýzou				vyžaduje sa
3.9.	Kompletný výsledok o zanalyzovanom súbore vrátane informácie o nájdenom i nenájdenom škodlivom správaní daného súboru				vyžaduje sa
3.10.	Manuálne odoslanie vzorky do sandboxu				vyžaduje sa
3.11.	Možnosť proaktívnej ochrany, kedy je potenciálna hrozba blokovaná, pokiaľ nie je známy výsledok analýzy zo sandboxu				vyžaduje sa
3.12.	Neobmedzené množstvo odosielaných súborov				vyžaduje sa
3.13.	Všetka komunikácia prebieha šifrovaným kanálom				vyžaduje sa
3.14.	Okamžité odstránenie súboru po dokončení analýzy v cloudovom sandboxe				vyžaduje sa

3.15.	Možnosť voľby, aké kategórie súborov do cloudového sandboxu budú odchádzať (spustiteľné súbory, archívy, skripty, pravdepodobný spam, dokumenty atp.)				vyžaduje sa
3.16.	Veľkosť odoslaných súborov do cloudového sandboxu môže dosahovať až 64MB				vyžaduje sa
3.17.	Výsledky analyzovaných súborov sú dostupné a automatizovane distribuované všetkým serverom a staniciam naprieč organizáciou, tak aby nedochádzalo k duplicitnému testovaniu				vyžaduje sa
4.	**Šifrovanie celých diskov**				
4.1.	Podpora platforiem Windows a MacOS				vyžaduje sa
4.2.	Správa cez jednotný centrálny manažment				vyžaduje sa
4.3.	Unikátna technológia pre platformu Windows (nevyužíva sa BitLocker)				vyžaduje sa
4.4.	Podpora Pre-Boot autentizácia				vyžaduje sa
4.5.	Podpora TMP modulu				vyžaduje sa
4.6.	Podpora Opal samošifrovacích diskov				vyžaduje sa
4.7.	Možnosť definovať: počet chybne zadaných pokusov, zložitosť a dĺžku autentizačného hesla				vyžaduje sa
4.8.	Možnosť obmedziť platnosť autentizačného hesla				vyžaduje sa
4.9.	Podpora okamžitého zmazania šifrovacieho kľúča a následné uzamknutie počítača				vyžaduje sa
4.10.	Recovery z centrálnej konzoly				vyžaduje sa
5.	**XDR riešenie**				
5.1.	Možnosť prevádzky centrálneho servera v cloude				vyžaduje sa
5.2.	Webová konzola pre správu a vyhodnotenie				vyžaduje sa
5.3.	Možnosť prevádzky s databázami: Microsoft SQL, MySQL				vyžaduje sa
5.4.	Možnosť prevádzky v offline prostredí				vyžaduje sa
5.5.	Autonómne správanie so schopnosťou vyhodnotiť podozrivú/ škodlivú aktivitu a zareagovať na ňu aj bez aktuálne dostupného riadiaceho servera alebo internetového pripojenia				vyžaduje sa
5.6.	Logovanie činností administrátora (tzv.Audit Log)				vyžaduje sa
5.7.	Podpora EDR pre systémy Windows, Windows server, MacOS a Linux				vyžaduje sa
5.8.	Možnosť autentizácie do manažmentu EDR pomocou 2FA				vyžaduje sa
5.9.	Možnosť riadenia manažmentu EDR prostredníctvom API, a to ako pre: Prijímanie informácií z EDR serverov aj Zasielanie príkazov na EDR servery				vyžaduje sa
5.10.	Integrovaný nástroj v EDR riešení pre vzdialené zasielanie príkazov priamo z konzoly				vyžaduje sa
5.11.	Možnosť izolácie zariadenia od siete				vyžaduje sa
5.12.	Možnosť tvorby vlastných IoC				vyžaduje sa
5.13.	Možnosť škálovania množstva historických dát vyhodnotených v EDR min. 3 mesiace pre raw-data a min. 3 roky pre detekované incidenty.				vyžaduje sa
5.14.	„učiaci režim“ pre automatizované vytváranie výnimiek k detekčným pravidlám				vyžaduje sa
5.15.	Indikátory útoku pracujúce s behaviorálnou detekciou				vyžaduje sa
5.16.	Indikátory útoku pracujúce s reputáciou				vyžaduje sa
5.17.	Riešenie umožnuje analýzu vektorov útoku				vyžaduje sa
5.18.	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				vyžaduje sa
5.19.	Schopnosť detekovať laterálny pohyb útočníka				vyžaduje sa
5.20.	Analýza procesov, všetkých spustiteľných súborov a DLL knižníc.				vyžaduje sa
5.21.	Náhľad na spustené skripty použité pri detegovanej udalosti				vyžaduje sa

5.22.	Možnosť zabezpečeného vzdialeného spojenia cez servery výrobcu do konzoly EDR				vyžaduje sa
5.23.	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				vyžaduje sa
5.24.	Možnosť automatického vyriešenia incidentu administrátorom				vyžaduje sa
5.25.	Prioritizácia vzniknutých incidentov				vyžaduje sa
5.26.	Možnosť stiahnutia spustiteľných súborov zo staníc pre bližšiu analýzu vo formáte archívu opatreným heslom				vyžaduje sa
5.27.	Integrácia a zobrazenie detekcií vykonaných antimalware produktom				vyžaduje sa
5.28.	Riešenie je schopné generovať tzv. forest/full execution tree model				vyžaduje sa
5.29.	Vyhľadávanie pomocou novo vytvorených IoC nad historickými dátami				vyžaduje sa
5.30.	Previazanie s technikami popísanými v knowledge base MITRE ATT&CK				vyžaduje sa
5.31.	Integrovaný vyhľadávač VirusTotal s možnosť rozšírenia o vlastné vyhľadávače				vyžaduje sa
6.	**Management konzola pre správu všetkých riešení v rámci ponúkaného balíka v rozsahu:**				
6.1.	Možnosť prevádzkovať jednotnú management konzolu na správu týchto riešení v cloudovom nasadení.				vyžaduje sa
6.2.	Webová konzola				vyžaduje sa
6.3.	Možnosť inštalácie na Windows aj Linux				vyžaduje sa
6.4.	Predpripravená virtual appliance pre virtuálne prostredie VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box				vyžaduje sa
6.5.	Server/proxy architektúra pre sieťovú pružnosť – zníženie záťaže pri sťahovaní aktualizácií detekčných modulov výrobcu				vyžaduje sa
6.7.	Možnosť prebudenia klientov pomocou Wake On Lan				vyžaduje sa
6.8.	Vzdialené vypnutie, reštart počítača alebo odhlásenie všetkých užívateľov				vyžaduje sa
6.9.	Možnosť konfigurácie virtual appliance cez užívateľsky prívetivé webové rozhranie Webmin				vyžaduje sa
6.10.	Nezávislí manažment agent pre platformy Windows, Linux a MacOS				vyžaduje sa
6.11.	Management agent pre architektúry na platformy Windows a MacOS: x86, x64, ARM64				vyžaduje sa
612.	Nezávislý agent (pracuje aj offline) vzdialenej správy pre zabezpečenie komunikácie a ovládania operačného systému verejného obstarávateľa				vyžaduje sa
6.13.	Offline uplatňovanie politík a spúšťanie úloh pri výskyte definovanej udalosti (napríklad: odpojenie od siete pri nájdení škodlivého kódu).				vyžaduje sa
6.14.	Administrácia v najpoužívanejších jazykoch vrátane slovenčiny				vyžaduje sa
6.15.	Široké možnosti konfigurácie oprávnení administrátorov (napríklad možnosť správy iba časti infraštruktúry, ktoré konkrétnemu administrátorovi podlieha)				vyžaduje sa
6.16.	Zabezpečenie prístupu administrátorov do vzdialenej správy pomocou 2FA				vyžaduje sa
6.17.	Podpora štítkov/tagovania pre jednoduchšiu správu a vyhľadávanie				vyžaduje sa
6.18.	Správa karantény s možnosťou vzdialeného vymazania / obnovenia / obnovenia a vylúčenia objektu z detekcie				vyžaduje sa
6.19.	Vzdialené získanie zachyteného škodlivého súboru				vyžaduje sa
6.20.	Detekcia nespravovaných (rizikových) počítačov komunikujúcich na sieti.				vyžaduje sa
6.21.	Podpora pre inštalácie a odinštalácie aplikácií 3.strán				vyžaduje sa
6.22.	Vyčítanie informácií o verziách softvéru 3. strán				vyžaduje sa

6.23.	Možnosť vyčítať informácie o hardvéri na spravovaných zariadeniach (CPU, RAM, diskové jednotky, grafické karty…).				vyžaduje sa
6.24.	Možnosť vyčítať sériové číslo zariadenia				vyžaduje sa
6.25.	Možnosť vyčítať voľné miesto na disku				vyžaduje sa
6.26.	Detekcia aktívneho šifrovania BitLocker na spravovanej stanici				vyžaduje sa
6.27.	Zobrazenie časovej informácie o poslednom boote stanice				vyžaduje sa
6.28.	Odoslanie správy na počítač / mobilné zariadenie, ktoré sa následne zobrazí užívateľovi na obrazovke				vyžaduje sa
6.29.	Vzdialené odinštalovanie antivírusového riešenia 3. strany				vyžaduje sa
6.30.	Vzdialené spustenie akéhokoľvek príkazu na cieľovej stanici pomocou Príkazového riadka				vyžaduje sa
6.31.	Dynamické skupiny pre možnosť definovania podmienok, za ktorých dôjde k automatickému zaradeniu klienta do požadovanej skupiny a automatickému uplatneniu klientskej úlohy				vyžaduje sa
6.32.	Automatické zasielanie upozornení pri dosiahnutí definovaného počtu alebo percent ovplyvnených klientov (napríklad: 5 % všetkých počítačov/50 klientov hlási problémy)				vyžaduje sa
6.33.	Podpora SNMP Trap, Syslogu a qRadar SIEM				vyžaduje sa
6.34.	Podpora formátov pre Syslog správy: CEF, JSON, LEEF				vyžaduje sa
6.35.	Podpora inštalácie skriptom - *.bat, *.sh, *.ini (GPO, SSCM…).				vyžaduje sa
6.36.	Rýchle pripojenie na klienta pomocou RDP z konzoly pre vzdialenú správu.				vyžaduje sa
6.37.	Reportovanie stavu klientov chránených inými bezpečnostnými programami.				vyžaduje sa
6.38.	Schopnosť zaslať reporty a upozornenia na e-mail				vyžaduje sa
6.39.	Konzola podporuje multidoménové prostredie (schopnosť pracovať s viacerými AD štruktúrami)				vyžaduje sa
6.40.	Konzola podporuje multitenantné prostredie (schopnosť v jednej konzole spravovať viac počítačových štruktúr)				vyžaduje sa
6.41.	Podpora VDI prostredia (Citrix, VMware, SCCM, apod)				vyžaduje sa
6.42.	Podpora klonovania počítačov pomocou golden image				vyžaduje sa
6.43.	Podpora inštanciách klonov				vyžaduje sa
6.44.	Podpora obnovy identity počítača pre VDI prostredie na základe FQDN				vyžaduje sa
6.45.	Možnosť definovať viacero menných vzorov klonovaných počítačov pre VDI prostredie				vyžaduje sa
6.46.	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				vyžaduje sa
7.	**Správa zraniteľností a patchov aplikácií tretích strán:**				
7.1.	Automatizované kontroly podľa vlastného harmonogramu na základe prispôsobiteľných pravidiel				vyžaduje sa
7.2.	Filtrovanie, zoskupovanie a triedenie zraniteľností podľa ich závažnosti				vyžaduje sa
7.3.	Možnosť manuálnych alebo automatických opráv				vyžaduje sa
7.4.	Prispôsobiteľné politiky záplat				vyžaduje sa
7.5.	Podpora multitenant v komplexných sieťových prostrediach - prehľad zraniteľností v konkrétnych častiach organizácie				vyžaduje sa
7.6.	Databáza zraniteľností, CVSS 2.0 a CVSS 3.1				vyžaduje sa
8.	**Ochrana poštových serverov/mailboxov:**				
8.1.	Komplexná vrstva ochrany na úrovni servera s cieľom zabrániť prieniku spamu a malvéru do e-mailových schránok používateľov				vyžaduje sa
8.2.	Antimalvér, antispam, anti-Phishing, ochrana hostiteľských serverov, ochrana založená na strojovom učení				vyžaduje sa
8.3.	Správa karantény				vyžaduje sa
8.4.	Podpora klastrov				vyžaduje sa

9.	**Ochrana cloudového prostredia Microsoft365/Google Workspace:**				
9.1.	Pokročilá ochrana pre aplikácie služby Microsoft 365 prostredníctvom ľahko použiteľnej cloudovej konzoly				vyžaduje sa
9.2.	Filtrovanie spamu, antimalvérová kontrola, anti-phishing a cloudový sandboxing				vyžaduje sa
7.1.	Ochrana cloudových úložísk				vyžaduje sa
9.	**Nástroj na 2-faktorovú autentifikáciu:**				
9.1.	Jednoduché overovanie pre používateľov jedným ťuknutím				vyžaduje sa
9.2.	Overovanie cez Push notifikácie				vyžaduje sa
9.3.	Podpora existujúcich tokenov a hardvérových kľúčov a smartfónov				vyžaduje sa
9.4.	Overovanie pri prístupe k VPN, RDP a Outlooku, webové aplikácie				vyžaduje sa
9.5.	Riešenie bez programátorského zásahu musí mať integráciu: HOTP, alebo na HMAC- založené jednorázové heslá one-time password (OTP), Audit používateľov v denníku. (úspešné, neúspešne pokusy o overenie).				vyžaduje sa
10.	**Bližšia špecifikácia služieb rozšírenej servisnej on-site pre prostredie XDR:**				
10.	Poskytovanie služieb rozšírenej servisnej podpory s aktívnym monitoringom ESET Inspect riešenia a centrálnej konzoly ESET PROTECT alebo ekvivalentné riešenie				vyžaduje sa
10.1.	Definícia podpory:				
10.1.1	Podpora poskytovaná 8x5, v prac. dňoch v čase 8:00-16:00 h, potvrdenie prijatia požiadavky na servisný zásah do min. 60 minút, nástup na riešenie najneskôr do 4 h od nahlásenia incidentu.				vyžaduje sa
10.1.2	Nástup na riešenie najneskôr do 4 hodín od nahlásenia incidentu, ktorý sa vzťahuje na ESET PROTECT a ESET Inspect prostredia (alebo ekvivalent)				vyžaduje sa
10.2.	Rozsah podpory				
10.2.1.	Komplexná starostlivosť o prevádzku XDR platformy alebo ekvivalentu charakteristický pre balík ESET PROTECT Enterprise (alebo ekvivalent)				vyžaduje sa
10.3.	Požadované proaktívne činnosti pre oblasť podpory				

10.3.1.	Proaktívne riešenie vznikajúcich problémov v rozsahu 1,5 MD mesačne. V rámci tejto aktivity sú požadované nasledovné min. činnosti pre riešenie (resp. ekvivalentné riešenie, ktoré spĺňa min. požadované činnosti): - proaktívny monitoring vybraných parametrov a dostupnosť všetkých služieb aplikačného riešenia EDR/XDR serverového systému. - aktívny monitoring EDR/XDR pravidiel s príslušným notifikačným mechanizmom - nastavovanie pravidelných reportov podľa požiadaviek objednávateľa v celkom rozsahu 2 reporty za mesiac. Security podpora pre ESET Inspect endpointové produkty: -Malware: chýbajúca detekcia, -Malware: problém s liečením, -Malware: infekcia ransomvérom, -Zachytenie False positive, -Vyšetrenie podozrivého správania -Vyšetrenie malware incidentu a odozva na vzniknutý malware incident: Základná analýza zaslaného súboru, -Detailná analýza zaslaného súboru, -Analýza a vyšetrenie odovzdaných súvisiacich dát, -Asistencia pri odozve/protiopatreniach na malware incident, Podpora pre riešenie bezpečnostných incidentov v prostredí XDR: -Podpora s vytváraním XDR pravidiel, -Podpora s vytváraním XDR výnimiek, -ESET Inspect, alebo ekvivalent operatívna optimalizácia prostredia, -ESET Inspect služba Threat Hunting, alebo ekvivalent (poskytovaná na požiadanie zo strany objednávateľa). -pravidelné vyhodnocovanie XDR incidentov na mesačnej báze s príslušným návrhom opatrení a reštrikcií -v mesačnej správe je zahrnuté aj vyhotovenie úplného ročného analytického reportu, ktorý bude sumarizovať všetky zistenia a odporúčania za ročné sledované obdobie -kontrola logov -napojenie na SIEM a zadefinovanie parametrov (poskytovaná na požiadanie zo strany objednávateľa). -aktualizácia aplikačného vybavenia v zmysle odporúčaní výrobcom, -dodanie informácií o známych bezpečnostných chybách a aplikovanie náprav -vo fáze poskytovania podpory, pravidelné stretnutia pracovnej skupiny min. 1x mesačne, -evidencia XDR incidentov a úprav na on-line portáli/HelpDesku.				vyžaduje sa	

11.	**Pezsonálne zabezpečenie:**					
11.1.	Nutnosť 3 pracovníkov so špecializáciou ESET Optimization Specialist (doklady sú vydané výrobcom tovaru resp. riešenia, alebo ekvivalentu), 3 pracovníci s certifikáciou: - Základné technické znalosti ESET riešení, alebo ekvivalent, - Základná technická certifikácia, - Pokročilá technická certifikácia, - Produktová technická certifikácia na ESET Mail Security pre Microsoft Exchange Server, alebo ekvivalent V zmysle legislatívy požadujeme, aby akýkoľvek partner vedel deklarovať aspoň 3 certifikovanýchi pracovníkov s certifikáciou CySA+. Táto certifikácia deklaruje všestrannú skúsenosť spoločnosti a pracovníov pri analýzach bezpečnostných incidentov. 1 certifikovana osoba v roli projektový manažér s platným certifikátom projektového riadenia PRINCE2 Practitioner.				vyžaduje sa	