# Kúpna zmluva č. Z20244689_Z

uzatvorená v zmysle §409 a nasl. Obchodného zákonníka

## I. Zmluvné strany

1.1 Objednávateľ:

| | |
|---|---|
| Obchodné meno: | Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky |
| Sídlo: | Dobrovičova 12, 81266 Bratislava, Slovenská republika |
| IČO: | 00156621 |
| DIČ: | 2021291382 |
| IČ DPH: | |
| Bankové spojenie: | IBAN: SK6681800000007000081105 |
| Telefón: | +421259266234 |

1.2 Dodávateľ:

| | |
|---|---|
| Obchodné meno: | S4B s.r.o. |
| Sídlo: | Učiteľská 15, 82106 Bratislava, Slovenská republika |
| IČO: | 46507345 |
| DIČ: | 2023403107 |
| IČ DPH: | 46507345 |
| Bankové spojenie: | IBAN: SK0911000000002925869639, BIC: TATRSKBX |
| Telefón: | 00421903971974 |

## II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

| | |
|---|---|
| Názov: | Antivírusová ochrana |
| Kľúčové slová: | antivírusová ochrana, softvér, ochrana počítačov, ochrana serverov, ochrana pred vírusmi |
| CPV: | 48761000-0 - Antivírusový softvérový balík; 48760000-3 - Softvérový balík na ochranu pred vírusmi; 72260000-5 - Služby súvisiace so softvérom; 72263000-6 - Implementácia softvéru; 60000000-8 - Dopravné služby (bez prepravy odpadu) |
| Druh/y: | Tovar; Služba |

2.2 Funkčná a technická špecifikácia predmetu Zmluvy:

**Položka č. 1: Antivírusová ochrana**

| **Funkcia** | | | | |
|---|---|---|---|---|
| Softvérové licencie pre zabezpečenie antivírusovej ochrany pre pracovné stanice, prenosné počítače, tablety, mobilné zariadenia, servery objednávateľa, vrátane podpory virtualizácie, ako v prípade antivírusovej ochrany virtuálnych operačných systémov, tak aj možnosti inštalácie centrálneho manažmentu antivírusovej ochrany do virtualizovaného prostredia/zariadenia objednávateľa na obdobie dvadsaťštyri (24) po sebe nasledujúcich mesiacov | | | | |
| **Technické vlastnosti** | **Jednotka** | **Minimum** | **Maximum** | **Presne** |
| Softvér pre zabezpečenie antivírusovej ochrany – licencia pre užívanie konzoly pre centrálnu správu vrátane aktualizácie počas 24 mesiacov | ks | | | 1 |
| Softvér pre zabezpečenie antivírusovej ochrany - licencia – produktový balík bezpečnostných riešení na ochranu koncových pracovných staníc, serverov vrátane aktualizácie počas 24 mesiacov | ks | | | 650 |
| Softvér pre zabezpečenie antivírusovej ochrany - licencia – produktový balík bezpečnostných riešení na ochranu mobilných zariadení vrátane aktualizácie počas 24 mesiacov | ks | | | 220 |

| | | | | |
|---|---|---|---|---|
| Služba – balík inštalačných služieb (dodanie, implementácia, konfigurácia, otestovanie funkčnosti, zaškolenie zamestnancov) | bal | | | 1 |

| **Technické vlastnosti** | **Hodnota/Charakteristika** |
|---|---|
| 1. Konzola pre centrálnu správu riešenia | |
| 1.1 Všeobecná definícia | Všetky komponenty riešenia musia byť v slovenskom alebo českom jazyku – vrátane konzoly pre centrálnu správu, klientskych aplikácií a manuálov. |
| - | Komplexná údržba a vysoká dostupnosť centrálnej konzoly nasadenej v cloude a všetkých jej poskytovaných služieb a funkcií sú zabezpečené vendorom riešenia. |
| - | Možnosť migrácie konzoly pre centrálnu správu do on-premise prostredia kedykoľvek a bezplatne, bez vplyvu na platnosť licencie a za vynaloženia minimálneho úsilia zo strany administrátora riešenia. |
| - | Podpora produktov výrobcom nástroja bude poskytovaná v slovenskom alebo českom jazyku. |
| - | Konzola pre centrálnu správu je kompletne multi-tenantná. |
| 1.2 Základné vlastnosti | Možnosť realizovať aktualizácie klientov z iných klientov a tým šetriť šírku prenosového pásma pripojenia k internetu. |
| - | Možnosť zobrazovania notifikácií v konzole pre centrálnu správu a ich posielania e-mailom. |
| - | Možnosť preposielania notifikácií na vzdialený syslog server. |
| - | Možnosť využitia napojenia akejkoľvek tretej aplikácie za pomoci zdokumentovanej verejnej API, ku ktorej je možné vytvoriť kľúče priamo z konzoly centrálnej správy bez nutnosti interakcie technickej |
| - | podpory dodávateľa alebo výrobcu. |
| 1.3 Úlohy správy bezpečnosti | Riešenie musí umožniť integráciu so štruktúrami Microsoft Active Directory za účelom správy ochrany zariadení v týchto inventároch. |
| - | Riešenie musí byť schopné odhaliť zariadenia, ktoré nie sú vedené v Microsoft Active Directory pomocou Network Discovery. |
| - | Filtrovanie a riadenie v inventári aspoň podľa mena hostiteľa, operačného systému, IP adries, pridelených pravidiel a podľa času poslednej aktivity. |
| - | Možnosť vzdialenej inštalácie a odinštalácie EPP klienta priamo z konzoly centrálnej správy. |
| - | Možnosť upraviť úroveň skenovacích úloh a ich spúšťania a plánovania priamo z konzoly centrálnej správy. |
| - | Možnosť reštartovania chránených koncových bodov (serverov alebo pracovných staníc) priamo z konzoly centrálnej správy. |
| - | Centralizované miesto pre zaznamenávanie všetkých úloh. |
| - | Možnosť granulárneho prístupu priradenia bezpečnostných pravidiel pre koncové stanice na každej úrovni štruktúry inventáru, vrátane koreňov a listov stromov (tzn. akékoľvek OU, prípadne až priamo |
| - | konkrétna stanica). |
| - | Podpora API a integrácie do SIEM nástroja. |
| 1.4 Nastavenia úrovne bezpečnosti | Umožňuje rôzne možnosti priradenia pravidiel a to podľa užívateľa či skupiny v Microsoft Active Directory (AD), podľa sieťovej lokality, v ktorej sa zariadenie nachádza (vrátane identifikácie podľa |
| - | možnej kombinácie – inklúzia či exklúzia - nasledujúcich znakov: IP adresa, rozsah IP adries, DNS server, WINS server, default gateway, typ siete, názov hostiteľa, DHCP prípona, či je možné sa |
| - | pripojiť ku konkrétnemu hostiteľovi alebo či je dostupná konzola centrálnej správy) alebo podľa OU, v ktorej sa nachádza v AD. |
| - | Možnosť nastavenia dedičnosti medzi bezpečnostnými pravidlami granulárne podľa sekcií a podsekcií nastavení bezpečnostných pravidiel. |

| | |
|---|---|
| 1.5 Reportovanie | Možnosť nastavenia intervalu, v ktorom sú reporty generované, možnosť vytvoriť report okamžite. |
| - | Možnosť zasielania vygenerovaných reportov e-mailom. |
| - | Možnosť stiahnuť vygenerované reporty minimálne vo formátoch .pdf či .csv. |
| - | Možnosť úpravy reportov, vyberanie cieľa (skupina staníc, typ staníc atď.) a časového intervalu, z ktorého je report vytvorený. |
| 1.6 Karanténa | Vzdialená obnova či zmazanie súboru v karanténe. |
| - | Možnosť automaticky pridať súbor do výnimky pri obnove z karantény. |
| 1.7 Používatelia | Viacero preddefinovaných rolí: a) pre správu komponentov riešenia (root), b) pre správu bezpečnost. pravidiel a inventáru koncových zariadení (administrátor), c) pre správu a tvorbu reportov(reportér) |
| - | Podpora 2FA overenia s možnosťou vynútenia. |
| - | Možnosť vynútiť zmenu hesla používateľa po uplynutí určitej doby od jeho poslednej zmeny. |
| - | Možnosť automatického zablokovania užívateľského účtu pri opakovaných neúspešných pokusoch o prihlásenie. |
| - | Možnosť detailného výberu služieb a typov staníc, ktoré môže užívateľ spravovať. |
| 1.8 Logovanie | Zaznamenávanie používateľských aktivít. |
| - | Detailný log pre každú aktivitu. |
| - | Komplexné vyhľadávanie v logovacích záznamoch. |
| 1.9 Správa a inštalácia ochrany | Možnosť selekcie výberu modulov ochrany pred samotnou inštaláciou a určenie, ktoré moduly majú byť nainštalované. |
| - | Možnosť výberu spôsobu realizácie inštalácie a to minimálne stiahnutím inštalačného balíčku priamo do pracovnej stanice, vzdialená Inštalácia priamo z konzoly centrálnej správy, alebo distribúciou |
| - | inštalačného balíčka cez GPO či SCCM. |
| - | Možnosť Inštalácie na koncové stanice vo vzdialenej lokalite priamo z už existujúceho nainštalovaného klienta v danej vzdialenej lokalite (optimalizácia prenosu pre WAN/VPN). |
| - | Konzola centrálnej správy bude reportovať počet chránených koncových staníc a počet koncových staníc, ktoré chránené nie sú. |
| - | Konzola správy obsahuje prispôsobiteľné „widgety“ pre okamžitý prehľad o stave ochrany v organizácií. |
| - | Konzola centrálnej správy obsahuje detailné informácie o chránených zariadeniach: názov, IP adresa, operačný systém, nainštalované moduly, aplikované pravidlá, informácie o aktualizáciách. |
| - | Konzola centrálnej správy umožňuje získanie všetkých informácií potrebných pre riešenie problémov s ochranou koncových staníc vrátane podrobných logov. |
| - | Konzola správy umožňuje hromadne zmeniť nastavenia na všetkých staniciach naraz alebo len selektívne pre konkrétnu skupinu staníc. |
| - | Pre rozdielne skupiny používateľov bude možné granulárne nastaviť aké skupiny zariadení majú právo spravovať. |
| - | Možnosť vytvárať inštalačné balíčky pre 32-bit a 64-bit operačné systémy, vrátane samo inštalačného balíčku, ktorý obsahuje kompletnú aplikáciu bez nutnosti prístupu k sieti pre jeho inštaláciu. |
| - | Inštalačný balíček umožňuje tzv. „tichú“ inštaláciu (nezobrazia sa žiadne upozornenia, nevyžaduje sa žiadna používateľská interakcia). |
| - | Administrátor bude môcť v inventári správcovskej konzoly vytvárať skupiny a podskupiny, kam bude môcť presúvať chránené koncové body. |

| | |
|---|---|
| - | Možnosť spustenia Network discovery z akéhokoľvek už nainštalovaného klienta. |
| 2. Vlastnosti a funkcie ochrany fyzických koncových bodov | |
| 2.1 Všeobecná definícia | Podpora operačných systémov: Windows 10 1507 a vyšší, Windows 8.1, Windows 8, Windows 7, Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, |
| - | Windows Embedded Standard 7, Windows Embedded Compact 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, |
| - | Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server 2011, Windows Server 2008 R2, Ubuntu 14.04 LTS a vyšší |
| - | Red Hat Enterprise Linux, CentOS 6.0 a vyšší, SUSE Linux Enterprise Server 11 SP4 a vyšší, OpenSUSELeap 42.x, Fedora 25 a vyšší, Debian 8.0 a vyšší, Oracle Linux 6.3 a vyšší, |
| - | Amazon Linux AMI 2016.09 a vyšší, Mac OS X El Capitan (10.11) a vyšší. |
| - | Automatické skenovanie dát, pri ich manipulácií – tzn. otváranie súborov, kopírovanie súborov, prenášanie súborov (LAN, WAN, zdieľané úložisko, prenosné média, pevný disk...). |
| - | Automatické skenovanie súborov v reálnom čase s možnosťou nastavenia skenovania len špecifických typov súborov. |
| - | Automatické skenovanie súborov v reálnom čase s možnosťou obmedzenia na maximálnu veľkosť súboru. |
| - | Aktualizácia bezpečnostného obsahu minimálne raz za hodinu. |
| - | Detekcia na základe vírusových definícií (tzv. signatúr). |
| - | Threat Emulation Technológia (v cloudovom prostredí dodávateľa alebo lokálne). |
| - | Proaktívna detekcia hrozieb bez nutnosti aktualizácie vírusových databáz. Technológia ochrany používajúca aktívnu prevenciu používaním heuristickej analýzy a generických popisov zraniteľností |
| - | k zablokovaniu nových pokusov o zneužitie zraniteľnosti ešte pred vydaním bezpečnostnej záplaty. |
| - | Umožňuje ochranu proti cieleným útokom pomocou strojového učenia s viac ako 80 tisíc vzorcami chovania. |
| - | Pokročilá analýza spúšťaných procesov ešte pred ich spustením a ich zablokovanie v prípade vykázania škodlivého chovania (vrátane ochrany proti 0-day útokom). |
| - | Pokročilá analýza bežiacich procesov v reálnom čase a ich zablokovanie v prípade detekcie škodlivého chovania (vrátane ochrany proti 0-day útokom). |
| - | Detekcia 0-day útokov na základe cloudového i lokálneho (100% funkčnosť i v prípade výpadku pripojenia k internetu) strojového učenia. |
| - | Detekcia 0-day útokov na základe odhaľovania anomálií. |
| - | Dynamická detekcia 0-day útokov, botnetových sietí, DDoS a exploit útokov v cloudových službách dodávateľa pomocou umelej inteligencie a pokročilých algoritmov strojového učenia. |
| - | Detekcia 0-day bez súborových útokov. |
| - | Detekcia 0-day útokov na úrovni sieťových prenosov (útoky na RDP, pokusy o zistenie dostupnosti, detekcia laterálneho pohybu útočníka). |
| - | Možnosť automatickej kontroly koncových bodov na nesprávnu konfiguráciu a neaktuálnosť bezpečnostných záplat aplikácií na známe zraniteľnosti. |

| | |
|---|---|
| - | Umožňuje zhodnotenie celkového skóre rizika spoločnosti na základe nesprávne nakonfigurovaných nastavení systému, známych zraniteľností aktuálne nainštalovaných aplikácií a potencionálnych rizík |
| - | spôsobených aktivitou a správaním používateľov. |
| - | Možnosť notifikácií na rizikové chovanie používateľa (prihlasovanie na nezabezpečených weboch, používanie podobného hesla na rôznych weboch, používanie podobného hesla v interných a externých |
| - | aplikáciách, apod.). |
| - | Ohodnotenie stavu koncových bodov a používateľov podľa tzv. „Risk score“. Umožňuje administrátorom priorizovať pri riešení detegovaných incidentov. |
| - | Riziká sú ohodnotené podľa závažnosti a pokiaľ sú spájané s konkrétnym CVE, tak je to uvedené. |
| - | Možnosť automatickej opravy vybraných rizík, prípadne uvedenie návodu/odporúčaní k odstráneniu rizík, ktoré nemožno odstrániť automaticky. |
| - | Možnosť automatického spustenia podozrivých súborov v Sandboxe. |
| - | Možnosť špecifických nastavenia Sandboxu ako sú napríklad dĺžka analýzy po spustení vzorky, počet opakovaných spustení, prístup k internetu počas analýzy. |
| - | Možnosť manuálneho vloženia podozrivej vzorky do Sandboxu. |
| - | Výstupom Sandboxu musí byť podrobný report o vykonanej analýze vrátane sumárnej manažérskej časti, detailného zhrnutia udalostí v systéme pre expertov, časovej osi spustených procesov a zrealizovaných |
| - | systémových zmien, zoznamu a geolokačnej analýzy sieťových pripojení, prehľadu všetkých vytvorených, upravovaných a mazaných súborov ako aj snímky obrazovky prípadných chybových hlásení. |
| - | Riešenie musí obsahovať funkcie EDR a EPP integrované do jednej klientskej aplikácie. |
| - | Riešenie musí podporovať možnosť izolácie infikovaných koncových bodov. (Odpojenie od siete s možnosťou komunikácie s konzolou centrálnej správy, automatická dezinfekcia a odstránenie škodlivého |
| - | obsahu, remote shell). |
| - | Riešenie musí byť schopné logovania procesov, systémových a sieťových aktivít v dobe detegovania incidentu pre ďalšiu investigáciu. |
| - | Riešenie umožňuje analýzu sieťovej komunikácie. |
| - | Riešenie umožňuje detekciu na základe automatizovaného hľadania IoCs Threat Intelligence v nespracovaných údajoch zbieraných EDR senzorom. |
| - | Riešenie ukladá zdrojové údaje o incidentoch (RAW data) minimálne na 7 dní a umožňuje rozšíriť ukladané údaje o bezpečnostných incidentoch na 90,180, až 365 dní. |
| - | Možnosť preverovať HTTP prevádzku. |
| - | Možnosť preverovať prevádzku šifrovanú pomocou SSL. |
| - | Možnosť nastavenia hesla pre odinštalovanie EPP klientskej aplikácie z koncových staníc. |
| - | Automatické skenovanie emailov na úrovni pracovnej stanice, bez ohľadu na použitie emailového klienta, pre odchádzajúce (SMTP) aj prichádzajúce emaily (POP3). |
| - | Podpora skenovania archívov, možnosť nastavenia maximálnej hĺbky a veľkosti skenovaných archívov. |
| - | Riešenie u vytvorených incidentov generuje tzv. full execution tree model a časovú os útoku. |

| | |
|---|---|
| - | Riešenie umožňuje analýzu vektoru útoku. |
| - | Riešenie umožňuje logovanie sieťových aktivít v dobe zachyteného incidentu za účelom ďalšieho preverovania. |
| - | Ochrana proti podvodným a phishingovým webovým stránkam. |
| - | Detekcia používaných zariadení (device) na koncových bodoch, možnosť blokovania zariadení podľa typu, možnosť povoliť len konkrétne zariadenie podľa Device ID. |
| - | Všetky vrstvy ochrany implementované do jednej aplikácie (t. z. bez nutnosti inštalácie viac ako jednej aplikácie). |
| - | Podpora detekcie nových vzorov ransomvéru pred jeho spustením aj počas neho. |
| 2.2 Patch management | Súčasťou riešenia musí byť možnosť bezdotykovej a vzdialenej distribúcie bezpečnostných záplat. |
| - | Automatická distribúcia konkrétnej záplaty pre definovanú zraniteľnosť. |
| - | Distribúcia konkrétnej záplaty pre definovanú zraniteľnosť z konzoly na vyžiadanie administrátorom. |
| - | Riešenie musí mať možnosť definovať úložisko v lokálnej sieti pre zníženie dopadu konektivity do internetu. |
| - | Možnosť zobraziť aktuálny stav nainštalovaných / chýbajúcich / nefunkčných záplat na koncových zariadeniach. |
| - | Súčasťou záplat musí byť popis a detailne informácie (CVE, BuletinID). |
| - | Riešenie umožňuje distribúciu záplat na fyzické a virtuálne servery platformy Windows, Golden Image, pracovné stanice OS Windows a aplikácie tretích strán. |
| - | Možnosť odloženia reštartu pre záplaty. |
| - | Dostupné záplaty pre platformu Windows – desktopy a servery. |
| - | Dostupné záplaty pre aplikáciu MS Office. |
| - | Dostupné záplaty pre aplikácie výrobcov: Adobe Acrobat, Adobe Reader, Google Chrome, Mozilla Firefox, Opera, Zoom client, WinZIP, VMware tools, Cisco WebEx. |
| 2.3 Firewall | Firewall modul musí byť možné voliteľne hocikedy inštalovať a odinštalovať bez nutnosti reštartovania OS. |
| - | Možnosť definovania vlastných firewall pravidiel na konkrétnu aplikáciu. |
| - | Možnosť detekcie a blokovania pokusov o skenovanie stavu portov. |
| - | Firewall obsahuje systém IDS vrátane funkcie odhaľovania neznámych hrozieb. |
| - | Možnosť vypnutia/zapnutia IDS. |
| - | Možnosť nastaviť profily známych sietí. |
| - | Možnosť kompletného blokovania Network Discovery (vrátane spojenia v LAN), alebo len pre spojenia z internetu. |
| 2.4 Karanténa | Pri každej aktualizácii bezpečnostného obsahu sú automaticky znovu preskenované súbory v karanténe. |
| - | Možnosť obnovy súboru do originálnej, alebo do novo zadanej lokality. |
| - | Automatické mazanie súborov v karanténe starších než zadaná maximálna doba životnosti (maximum nemôže byť kratšie než 30 dní). |
| 2.5 Kontrola prístupu k internetu | Možnosť zablokovania prístupu na internet pre špecifické stanice / skupiny staníc. |
| - | Zablokovanie prístupu ku konkrétnym webom pre špecifické koncové stanice / skupiny staníc. |
| - | Zablokovanie prístupu na internet v určený čas. |

| | |
|---|---|
| - | Obmedzenie prístupu k špecifickým typom webových stránok podľa výrobcom spravovaných kategórií (napr. násilie, hazard a iné). |
| - | Obmedzenie prístupu ku konkrétnym webovým stránkam (vrátane podpory tzn. „wildcards“ pre možnú inklúziu či exklúziu subdomén). |
| 3. Ochrana virtualizovaných koncových bodov | |
| 3.1 Všeobecná definícia | Riešenie nepotrebuje VMware vShield či NSX, aby poskytol tzv. bezenginové skenovanie – režim klienta, keď na klientskom VM beží len ľahký klient a všetky úlohy skenovania sú realizované iným, |
| - | špeciálnym „skenovacím“ zariadením; toto „skenovacie“ zariadenie môže byť virtualizované, ale nie je nutné aby bolo umiestnené na samotnom hypervisore ako chránená klientska VM. Počet týchto |
| - | špeciálnych virtuálnych zariadení nesmie byť licenciou nijako obmedzený. |
| - | „Skenovacie“ zariadenia sú spravované z konzoly centrálnej správy – aktualizácie, reštart, priradenie jednotlivých klientov ku „skenovacím“ virtuálnym zariadením. |
| - | „Skenovacie“ zariadenie musí byť možné prevádzkovať v režime vysokej dostupnosti a rovnomerného rozloženia záťaže. |
| - | Produkt musí hlásiť aktuálny stav zabezpečenia – VM chránený/nechránený, a stav „skenovacieho“ zariadenia. |
| - | Riešenie musí umožňovať optimalizáciu dátových prenosov medzi VM a „skenovacím“ zariadením pomocou deduplikácie skenovacích procesov – t. z. ten istý súbor (podľa hashu) nebude skenovaný na dvoch |
| - | rôznych VM (za predpokladu, že sa medzitým nezmenila verzia bezpečnostnej klientskej aplikácie). |
| - | Automatické skenovanie dát, pri ich manipulácií – t. z. otvorenie súborov, kopírovanie súborov, prenášanie súborov (LAN, WAN, zdieľané úložisko, prenosné média, pevný disk...). |
| - | Automatické skenovanie súborov v reálnom čase môže byť nastavené ku skenovaniu len špecifických typov súborov. |
| - | Automatické skenovanie súborov v reálnom čase môže byť obmedzené na maximálnu veľkosť súborov. |
| - | Aktualizácie bezpečnostného obsahu minimálne raz za hodinu. |
| - | Detekcie na základe vírusových definícií (tzv. signatúr). |
| - | Threat Emulation Technologia (v cloudovom prostredí dodávateľa alebo lokálne). |
| - | Pokročilá analýza spúšťaných procesov ešte pred ich spustením a ich zablokovanie v prípade vykázania škodlivého chovania (vrátane ochrany proti 0-day útokom). |
| - | Pokročilá analýza bežiacich procesov v reálnom čase a ich zablokovanie v prípade detekcie škodlivého chovania (vrátane ochrany proti 0-day útokom). |
| - | Detekcia 0-day útokov na základe cloudového i lokálneho (100% funkčnosť i v prípade výpadku pripojenia k internetu) strojového učenia. |
| - | Detekcia 0-day útokov na základe odhaľovanie anomálií. |
| - | Dynamická detekcia 0-day útokov, botnetových sietí, DDoS a exploit útokov v cloudových službách dodávateľa pomocou umelej inteligencie a pokročilých algoritmov strojového učenia. |
| - | Detekcia 0-day bez súborových útokov. |
| - | Detekcia 0-day útokov na úrovni sieťových prenosov (útoky na RDP, pokusy o zistenie dostupnosti, detekcia laterálneho pohybu útočníka). |
| - | Možnosť automatickej kontroly koncových bodov na nesprávnu konfiguráciu a neaktuálnosť bezpečnostných záplat aplikácií na známe zraniteľnosti. |

| | |
|---|---|
| - | Umožňuje zhodnotenie celkového skóre rizika spoločnosti na základe nesprávne nakonfigurovaných nastavení systému, známych zraniteľností aktuálne nainštalovaných aplikácií a potencionálnych rizík |
| - | spôsobených aktivitou a správaním používateľov. |
| - | Možnosť upozornení pred rizikovým chovaním používateľa (prihlasovanie na nezabezpečených weboch, používanie podobného hesla na rôznych weboch, používanie podobného hesla v interných a externých |
| - | aplikáciách, apod.). |
| - | „Risk score“ používateľov a koncových bodov umožňujúcich administrátorom priorizovať pri riešení detegovaných incidentov. |
| - | Riziká sú ohodnotené podľa závažnosti a pokiaľ sú spájané s konkrétnym CVE, tak je to uvedené. |
| - | Možnosť automatickej opravy vybraných rizík, prípadne uvedenie návodu k odstráneniu rizík, ktoré nemožno odstrániť automaticky. |
| - | Možnosť automatického spustenia podozrivých súborov v Sandboxe. |
| - | Možnosť špecifických nastavenia Sandboxu – dĺžka pozorovania po spustení, počet opakovaných spustení, prístup k internetu počas spustení áno/nie. |
| - | Možnosť manuálneho vloženia vzorky do Sandboxu. |
| - | Sandbox po analýze vygeneruje rozsiahly report o vykonanej forenznej analýze vrátane:- sumárna časť zrozumiteľná pre laikov,- podrobné zhrnutie udalostí diania v systéme pre expertov, |
| - | - časové osi spustených procesov a zrealizovaných systémových zmien,- zoznam a geolokačná analýza sieťových pripojení,- prehľad všetkých vytvorených, zmenených a mazaných súborov, |
| - | - snímky obrazovky prípadných chybových hlásení. |
| - | Riešenie musí obsahovať funkcie EDR integrované do jednej klientskej aplikácie spolu s EPP. |
| - | Riešenie musí podporovať možnosť izolácie infikovaných koncových bodov. (Odpojenie od siete s možnosťou komunikácie s konzolou centrálnej správy, automatická dezinfekcia a odstránenie škodlivého |
| - | obsahu, remote shell). |
| - | Riešenie musí byť schopné logovania procesov, systémových a sieťových aktivít v dobe detegovania incidentu pre ďalšiu investigáciu. |
| - | Riešenie umožňuje analýzu sieťovej komunikácie. |
| - | Riešenie umožňuje detekciu na základe automatizovaného hľadania IoCs Threat Intelligence v nespracovaných údajoch zbieraných EDR senzorom. |
| - | Riešenie umožňuje ukladať údaje o bezpečnostných incidentoch až 90 dní. |
| - | Možnosť preverovať http traffic. |
| - | Možnosť preverovať traffic šifrovaný pomocou SSL. |
| - | Možnosť nastavenia hesla pre odinštalovanie EPP klientskej aplikácie z koncových staníc. |
| - | Automatické skenovanie emailov na úrovni pracovnej stanice, bez ohľadu na použitie emailového klienta, obidve pre odchádzajúce (SMTP) a prichádzajúce emaily (POP3). |
| - | Možnosť skenovať archívy, možnosť nastavenia maximálnej hĺbky skenovaných archívov a maximálnu veľkosť skenovaných archívov. |
| - | Riešenie u vytvorených incidentov generuje tzv. full execution tree model a časovú os útoku. |
| - | Riešenie umožňuje analýzu vektoru útoku. |

| | |
|---|---|
| - | Riešenie umožňuje logovanie sieťových aktivít v dobe zachyteného incidentu za účelom ďalšieho preverovania. |
| - | Ochrana proti podvodným a phishingovým webovým stránkam. |
| - | Detekcia používaných zariadení (device) na koncových bodoch, možnosť blokovania zariadení podľa typu, možnosť povoliť len konkrétne zariadenie podľa Device ID. |
| - | Všetky požadované vrstvy ochrany na koncovom bode musia byť implementované jednou aplikáciou (t.z. bez nutnosti inštalácie viac ako jednej aplikácie). |
| 4. XDR | |
| 4.1 Všeobecná definícia | Riešenie obsahuje sieťovú sondu a sondu identít. |
| - | Riešenie obsahuje pomocníka pre riešenie incidentov, ktorý automaticky pri vytvorení incidentu analyzuje, čo sa v rámci incidentu stalo, označí jednoznačne príčinu incidentu a navrhne remediačné |
| - | kroky; taktiež pri dokorelovani akejkoľvek ďalšej skutočnosti/kroku útoku túto analýzu aktualizuje o tieto novo vykonané útočné akcie. |
| - | Riešenie zbiera dáta zo všetkých sond – koncové body, identita a sieť - na jednom mieste. |
| - | Riešenie dokáže vytvárať incidenty na základe hlásenia z akejkoľvek sondy a dokorelováva do tohoto incidentu všetky relevantné údaje zo všetkých dostupných sond. |
| - | Riešenie vizualizuje prehľadne priebeh útoku naprieč celou sieťou vrátane časovej osy detegovaných krokov útoku a roztriedenia týchto krokov do útočných fáz. |
| - | Sieťová sonda funguje v tzn. Neinvazívnom režime – pracuje s kópiou sieťovej prevádzky a nie je tzn. „prietoková“. |
| - | Sieťová sonda je dodávaná ako hotové virtuálne zariadenie do VMware alebo Hyper-V. |
| - | Sonda identít podporuje integráciu s Microsoft Active Directory či Azure Active Directory. |
| - | Sonda identít umožňuje nápravné akcie aspoň: zablokovanie užívateľského účtu, vyresetovanie hesla užívateľského účtu alebo označenie (otagovanie) užívateľského účtu ako „kompromitovaný“. |

2.3 Osobitné požiadavky na plnenie:

| **Názov** |
|---|
| V cene predmetu kúpnej zmluvy (zmluva) sú zahrnuté všetky náklady súvisiace s predmetom zmluvy (nadobudnutie softvéru pre antivírusovú ochranu, poskytnutie licencie, dodanie, inštalácia, otestovanie ,implementácia, automatické aktualizácie, podpora, školenia a pod.) v súlade s bodmi 10.3 až 10.5 Obchodných podmienok elektronickej platformy účinných od 03.11.2022 (ďalej len "OPEP"). |
| Dodávateľ predloží na elektronickú adresu objednávateľovi do troch (3) pracovných dní od nadobudnutia účinnosti zmluvy v elektronickej forme: |
| a) podrobný aktualizovaný rozpočet v rozsahu jednotková cena bez DPH, DPH a cena s DPH, |
| b kontaktné údaje osoby oprávnenej konať vo veciach súvisiacich s plnením predmetu tejto zmluvy za dodávateľa (meno a priezvisko, elektronickú adresu, telefónne číslo), |
| c) štandardné licenčné podmienky koncového používateľa („End User Licence Agreement“ - ďalej len „EULA“) určené výrobcom/zhotoviteľom softvéru pre antivírusovú ochranu, s ktorými je softvér pre antivírusovú ochranu bežne predávaný a distribuovaný na trhu v slovenskom jazyku, |
| d) detailný harmonogram implementácie antivírusového softvéru a zaškolenia určených zamestnancov objednávateľa, |
| e) všetkých známych subdodávateľov v rozsahu podľa tohto bodu. |
| Dodávateľ musí byť v čase účinnosti zmluvy zapísaný v registri partnerov verejného sektora v zmysle zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. |
| Čiastkové plnenie sa nepripúšťa. Dodávateľ musí dodať celý predmet zmluvy a všetky požadované tovary, tzn. softvér pre antivírusovú ochranu vrátane licencií podľa technickej špecifikácie a musia byť od jedného výrobcu/zhotoviteľa. |

| |
|---|
| V prípade zadania plnenia predmetu tejto zmluvy subdodávateľovi, dodávateľ v plnej miere zodpovedá za plnenie predmetu tejto zmluvy, akoby zmluvu plnil sám. |
| Dodávateľ v plnej miere zodpovedá za odbornú starostlivosť pri výbere subdodávateľa, predovšetkým za to, že subdodávateľ spĺňa všetky potrebné kvalifikačné a odborné predpoklady na riadne plnenie predmetu tejto zmluvy, vykonaného na základe zmluvy o subdodávke s dodávateľom z tejto zmluvy. |
| Podrobnosti dodania licenčného kľúča na aktiváciu softvéru pre antivírusovú ochranu budú dohodnuté elektronicky s určenou osobou objednávateľa, ktorej kontaktné údaje zašle po predložení harmonogramu kontaktná osoba objednávateľa. |
| Úhrada plnenia bude uskutočnená po kompletnom dodaní predmetu zmluvy na základe faktúry s uvedením celkovej ceny s DPH a jednotkových cien s DPH zaokrúhlenými max. na dve desatinné miesta. Faktúru je potrebné doručiť bezodkladne po dodaní predmetu zákazky na základe potvrdeného dodacieho listu. Splatnosť faktúry je 30 dní od doručenia objednávateľovi. |
| Požadované je komplexné zabezpečenie softvérom pre antivírusovú ochranu všetkých chránených koncových bodov, vrátane fyzických PC s OS Windows, Mac a Linux, virtuálnych PC (VDI) s OS Windows a Linux, fyzických serverov s OS Windows a Linux, virtuálnych serverov s OS Windows a Linux a mobilných zariadení s OS Android a iOS po dobu 24 mesiacov vrátane aktualizácie počas 24 mesiacov všetkých požadovaných licencií podľa tejto zmluvy. |
| Dodávateľ musí byť minimálne zlatým (gold) partnerom výrobcu/zhotoviteľa/predajného partnera (v závislosti od nastaveného procesu distribúcie softvéru pre antivírusovú ochranu zhotoviteľom) dodávaného softvéru pre antivírusovú ochranu. |
| Dodávaný softvér pre antivírusovú ochranu musel v období za posledné dva (2) roky dosiahnuť vo všetkých testoch nezávislej testovacej organizácie Virus Bulletin, zameraných na detekciu „in-the-wild“ vírusov a negenerovanie falošných poplachov (false positives) pri skenovaní neinfikovaných súborov pre rôzne platformy operačných systémov, certifikačnú známku VB100. |
| Dodávaný softvér pre antivírusovú ochranu musel v období za posledné dva (2) roky dosiahnuť vo všetkých Performance testoch nezávislej testovacej organizácie AV-Comparatives, zameraných na nízku spotrebu systémových prostriedkov pri používaní daného antivírusového produktu, najvyššiu certifikačnú známku Advanced+. |
| Dodávateľ je zodpovedný v plnom rozsahu za akúkoľvek škodu vrátane skutočnej škody, a iných priamo alebo nepriamo súvisiacich škôd, ktorá vzniknú objednávateľovi v dôsledku porušenia akýchkoľvek jeho záväzkov z tejto zmluvy, právnych predpisov alebo iných pravidiel, ktoré sú pre neho záväzné. |
| Dodávateľ bude predmet tejto zmluvy inštalovať vzdialeným bezpečným prístupom podľa interných bezpečnostných predpisov a pokynov objednávateľa, ktoré budú dodávateľovi poskytnuté do piatich (5) pracovných dní po nadobudnutí účinnosti tejto zmluvy. |
| Porušenie akejkoľvek povinnosti dodávateľa vyplývajúcej z tejto zmluvy sa považuje za podstatné porušenie a oprávňuje objednávateľa odstúpiť od tejto zmluvy. |
| Podmienky podľa EULA objednávateľ akceptuje pri inštalácii predmetu tejto zmluvy. V prípade rozporu medzi OPEP, ustanoveniami tejto zmluvy a EULA, majú prednosť EULA pred ustanoveniami tejto zmluvy. |

| Názov | Upresnenie |
|---|---|

2.4 Prílohy opisného formulára Zmluvy:

| Popis | Názov súboru |
|---|---|

## III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

| | |
|---|---|
| Štát: | Slovenská republika |
| Kraj: | Bratislavský |
| Okres: | Bratislava I |
| Obec: | Bratislava - mestská časť Staré Mesto |
| Ulica: | Dobrovičova 12 |

3.2 Čas / lehota plnenia zmluvy:

21.06.2024 00:00:00 - 21.07.2026 00:00:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

| | |
|---|---|
| Jednotka: | Celok uvedený v opisnom formulári |
| 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: 134 833,33 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 161 800,00 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 18.06.2024 10:38:01

Objednávateľ:
Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
S4B s.r.o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska