**Příloha č. 1 - Technická a věcná specifikace**

**Pokročilá ochrana koncových bodů včetně ochrany virtualizačních platforem a EDR**

ÚVOD

Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux a mobilních zařízení s OS Android a iOS.

Základní požadavky na řešení

Na základě hodnocení rizik Zadavatel vylučuje technické a programové prostředky výrobců, kteří jsou předmětem varování NUKIB (Varování před hrozbou v oblasti kybernetické bezpečnosti spočívající v nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů.

Je požadována licence pro ochranu 250 koncových stanic/uživatelů, celkem 50 serverů (ve virtuálním prostředí VMware a fyzických Windows serverů) a 50 mobilních zařízení Android a iOS na 5 let.

Detailní požadavky na správu a funkcionalitu naleznete podle kategorií a funkcí níže.

Následující funkce jsou bezvýhradně nutné k splnění podmínek výběrového řízení:

1. **Konzole pro centrální správu řešení:**

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE[[1]](#footnote-1) | Popis jak je řešeno |
| Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů |  |  |
| Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí |  |  |
| Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení |  |  |
| Konzole pro centrální správu je kompletně multi-tenantní |  |  |
| Podpora produktů výrobcem nástroje bude poskytována v českém jazyce |  |  |
| **Základní vlastnosti** |  |  |
| Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu |  |  |
| Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem |  |  |
| Možnost zasílat upozornění napojením na Syslog server |  |  |
| Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce |  |  |
| **Úlohy správy bezpečnosti** |  |  |
| Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích. |  |  |
| Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery |  |  |
| Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity |  |  |
| Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy |  |  |
| Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy |  |  |
| Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy |  |  |
| Centralizované místo pro záznam všech úloh |  |  |
| Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici) |  |  |
| **Nastavení úrovně bezpečnosti** |  |  |
| Více možností přiřazení pravidel:  podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD |  |  |
| Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně dle sekcí a subsekcí nastavení bezpečnostních pravidel |  |  |
| **Reportování** |  |  |
| Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě |  |  |
| Možnost zasílání vygenerovaných reportů e-mailem |  |  |
| Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv |  |  |
| Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen |  |  |
| **Karanténa** |  |  |
| Vzdálená obnova či smazání souboru v karanténě |  |  |
| Možnost automaticky přidat soubor do výjimky při obnově z karantény |  |  |
| **Administrátor řešení** |  |  |
| Více předdefinovaných rolí:  Root, administrátor, reportér   1. Root: spravuje komponenty řešení 2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení 3. Reportér: spravuje a vytváří reporty |  |  |
| Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví) |  |  |
| Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny |  |  |
| Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení |  |  |
| Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat |  |  |
| **Logy** |  |  |
| Zaznamenávání uživatelských akcí |  |  |
| Detailní log pro každou akci |  |  |
| Komplexní vyhledávání v logách |  |  |
| **Správa a instalace ochrany** |  |  |
| Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány |  |  |
| Instalace může být provedena několika způsoby, alespoň:   1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 3. Distribuce instalačního balíčku pomocí GPO či SCCM |  |  |
| Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN |  |  |
| Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou |  |  |
| Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci |  |  |
| Konzole správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích |  |  |
| Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů |  |  |
| Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou |  |  |
| Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat |  |  |
| Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti |  |  |
| Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci) |  |  |
| Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body |  |  |
| Možnost spustit Network discovery z kteréhokoli již instalovaného klienta |  |  |

1. **Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):**

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE[[2]](#footnote-2) | Popis jak je řešeno |
| Požadujeme následující podporu OS, které na úřadě využíváme, nebo je máme v plánu v budoucnu využívat:  Windows 11 a vyšší  Windows 10 a vyšší  Windows 10 IoT Enterprise  Windows Server 2019 a vyšší  Windows Server 2019 Core  Windows Server 2016 a vyšší  Windows Server 2016 Core  Windows Server 2012 R2  Windows Server 2012 a vyšší  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 skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...) |  |  |
| Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů |  |  |
| Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru |  |  |
| Aktualizace bezpečnostního obsahu alespoň jednou za hodinu |  |  |
| Možnost plné ochrany včetně aktualizace pro koncové body trvale bez přístupu k internetu v rámci LAN/WAN sítě |  |  |
| Detekce na základě virových definicí (tzn. signatur) |  |  |
| Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně) |  |  |
| Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům) |  |  |
| Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům) |  |  |
| Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení |  |  |
| Detekce 0-day útoků na základě odhalování anomálního chování |  |  |
| Detekce s využitím strojového učení |  |  |
| Modul behaviorální analýzy pro detekce chování nových typů ransomwaru |  |  |
| Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP |  |  |
| Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení |  |  |
| Detekce 0-day bezsouborových útoků |  |  |
| Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka) |  |  |
| Ochrana proti neautorizovanému šifrování s automatickou zálohou dat na nepřístupnou část pevného disku s možností automatické obnovy dat po zastavení útoku. Využití stínová kopie svazku ani jiná řešení statického zálohování nejsou z důvodu možnosti jejich odstranění útočníkem přípustné |  |  |
| Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.) |  |  |
| Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně |  |  |
| Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno |  |  |
| Schopnost pravidelné automatické detekce bezpečnostně rizikových konfiguračních zranitelností operačního systému koncového bodu pomocí vlastního agenta |  |  |
| Schopnost pravidelné automatické detekce zranitelností instalovaného SW vybavení na koncovém bodě pomocí vlastního agenta chyběj včetně detailního CVE ke každé takové zranitelnosti |  |  |
| Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky |  |  |
| Možnost automatické detonace podezřelých souborů v Sandboxu s neomezeným počtem detonací |  |  |
| Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne |  |  |
| Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu |  |  |
| Možnost ručního vložení vzorku do Sandboxu |  |  |
| Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení |  |  |
| Řešení musí obsahovat funkce EDR / XDR integrované do jedné klientské aplikace spolu s EPP |  |  |
| Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy |  |  |
| Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. |  |  |
| Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty. |  |  |
| Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem |  |  |
| Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku |  |  |
| Řešení umožňuje analýzu vektoru útoku |  |  |
| Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování |  |  |
| Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR) |  |  |
| Možnost prověřovat http provoz |  |  |
| Možnost prověřovat provoz šifrovaný pomocí SSL |  |  |
| Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic |  |  |
| Možnost šifrovat obsah pevného disku pro notebooky s platformou Windows |  |  |
| Ochrana agenta před neautorizovanou změnou nastavení, vyřazení z provozu, odinstalací antimalware řešení a kritických nastavení |  |  |
| Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3) |  |  |
| Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů |  |  |
| Ochrana proti podvodným a phishingovým webovým stránkám |  |  |
| Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID |  |  |
| Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci) |  |  |
| Řešení musí umožňovat vzdálené připojení na konzoli koncové stanice s možností výpisu procesů, registrů a souborů, vytvoření, změnu či výmaz souborů či registrů a ukončení procesu a to i ve stavu izolace stanice od sítě při použití bezpečnostního řešení |  |  |
| Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. |  |  |
| Podpora offline prostředí, technologie EDR/XDR vyhodnocuje a reaguje na události lokálně, nevyžaduje pro svou činnost připojení k internetu |  |  |
| Grafické zobrazení událostí, které nastaly na koncové stanici při spuštění objektu/procesu (jaký byl sled událostí příkazů, procesů, které procesy, co spouštěly, s jakými komunikovali IP adresami, doménami a tak dále) |  |  |
| Přehled všech detekovaných technik/taktik MITRE ATT&CK  včetně přímého navázání do zobrazeného kybernetického incidentu a linkem do databáze MITRE |  |  |
| **Firewall** |  |  |
| Možnost blokovat skenování portů |  |  |
| Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS |  |  |
| Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb |  |  |
| Možnost vypnout IDS |  |  |
| Možnost nastavit profily známých sítí |  |  |
| Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu |  |  |
| **Karanténa** |  |  |
| Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě |  |  |
| Možnost obnovy souboru do originální či do nově zadané lokality |  |  |
| Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní) |  |  |
| **Kontrola přístupu k internetu** |  |  |
| * Zablokování přístupu na internet pro specifické stanice / skupiny stanic * Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic * Zablokování přístupu k internetu v určený čas * Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné) * Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén) |  |  |

1. **Ochrana virtualizovaných koncových bodů (Windows, Linux)**

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE[[3]](#footnote-3) | Popis jak je řešeno (volitelné) |
| Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen |  |  |
| „Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením |  |  |
| „Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže |  |  |
| Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení |  |  |
| Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace) |  |  |
| Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...) |  |  |
| Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů |  |  |
| Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru |  |  |
| Aktualizace bezpečnostního obsahu alespoň jednou za hodinu |  |  |
| Detekce na základě virových definicí (tzn. signatur) |  |  |
| Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně) |  |  |
| Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům) |  |  |
| Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům) |  |  |
| Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení |  |  |
| Detekce 0-day útoků na základě odhalování anomálního chování |  |  |
| Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení |  |  |
| Detekce 0-day bezsouborových útoků |  |  |
| Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka) |  |  |
| Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností |  |  |
| Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.) |  |  |
| Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně |  |  |
| Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno |  |  |
| Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky |  |  |
| Možnost automatické detonace podezřelých souborů v Sandboxu |  |  |
| Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne |  |  |
| Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu |  |  |
| Možnost ručního vložení vzorku do Sandboxu |  |  |
| Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení |  |  |
| Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP |  |  |
| Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy |  |  |
| Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. |  |  |
| Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty. |  |  |
| Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku |  |  |
| Řešení umožňuje analýzu vektoru útoku |  |  |
| Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování |  |  |
| Možnost prověřovat http provoz |  |  |
| Možnost prověřovat provoz šifrovaný pomocí SSL |  |  |
| Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic |  |  |
| Modul pro ochranu mailboxů lokálně provozované Microsoft Exchange proti malwaru, spamu a phishingovým útokům |  |  |
| Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3) |  |  |
| Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů |  |  |
| Ochrana proti podvodným a phishingovým webovým stránkám |  |  |
| Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID |  |  |
| Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR) |  |  |
| Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní |  |  |
| Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci) |  |  |

1. **Rozšířená funkce XDR**

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE[[4]](#footnote-4) | Popis jak je řešeno (volitelné) |
| **Sonda XDR pro analýzu Microsoft Active Directory** |  |  |
| Rozšiřující modul pro XDR – Sonda pro analýzu OnPremise Active Directory |  |  |
| Rozšiřující modul pro XDR – Provádí monitorování a zpracování informací o uživatelích z OnPremise Microsoft Active Directory |  |  |
| Rozšiřující modul pro XDR – analyzuje a doplňuje incidenty bezpečnostního řešení o informace získané z Microsoft Active Directory |  |  |
| Rozšiřující modul pro XDR – sonda pro MS Active Directory musí auditovat bezpečnostní politiky v AD, minimálně Account Logon, Account Management, Object Access, Policy Change a Privilege Use |  |  |
| Rozšiřující modul pro XDR – Sonda pro analýzu Microsoft Active Directory musí být plně integrována do řešení ochrany koncového bodu |  |  |
| Rozšiřující modul pro XDR – Sonda pro Microsoft Active Directory nesmí zasahovat do chodu MS AD |  |  |
| Z konzole bezpečnostního řešení je možno zakázat uživatelský účet nebo vynutit reset hesla v Microsoft AD, který byl použit v rámci bezpečnostního incidentu |  |  |
| **Sonda XDR pro analýzu síťové vrstvy** |  |  |
| Rozšiřující modul pro XDR – Síťová sonda analyzující provoz na síťové vrstvě, která je plně integrovaná do nabízeného řešení |  |  |
| Rozšiřující modul pro XDR – Síťová sonda musí monitorovat a analyzovat datové toky v rámci počítačové sítě |  |  |
| Rozšiřující modul pro XDR – Síťová sonda obohacuje incidenty bezpečnostního řešení o informace získané z datové sítě |  |  |
| Rozšiřující modul pro XDR – Síťová sonda je samostatná appliance minimálně pro Vmware ESXi a Microsoft Hyper-V |  |  |
| Rozšiřující modul pro XDR – Síťová sonda obsahuje minimálně jeden port pro zpracování síťového provozu |  |  |
| Rozšiřující modul pro XDR – Síťová sonda umožňuje připojení prostřednictvím TAP/SPAN portu |  |  |
| Rozšiřující modul pro XDR – Nabízená síťová sonda nesmí být na monitorovacím portu detekovatelná, nesmí zasahovat do síťového provozu |  |  |

1. **Ochrana mobilních zařízení**

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE[[5]](#footnote-5) | Popis jak je řešeno (volitelné) |
| Licence pro ochranu 50 mobilních zařízení na 5 let |  |  |
| Možnost nasazení na iOS a Android zařízení včetně Chromebook zařízení |  |  |
| Antiphishing ochrana na mobilních zařízeních |  |  |
| Ochrana zařízení před jailbreak/root, detekce zranitelností v OS zařízení, chybějících updatů |  |  |
| Web access kontrola |  |  |
| Detekce škodlivých aplikací v zařízení |  |  |
| Správa mobilních zařízení musí probíhat ze stejné konzole jako ostatních modulů XDR řešení |  |  |

1. Účastník vyplní splnění závazných požadavků zadavatele - ANO/NE. Účastník musí splňovat veškeré minimální technické požadavky zadavatele. [↑](#footnote-ref-1)
2. Účastník vyplní splnění závazných požadavků zadavatele - ANO/NE. Účastník musí splňovat veškeré minimální technické požadavky zadavatele. [↑](#footnote-ref-2)
3. Účastník vyplní splnění závazných požadavků zadavatele - ANO/NE. Účastník musí splňovat veškeré minimální technické požadavky zadavatele. [↑](#footnote-ref-3)
4. Účastník vyplní splnění závazných požadavků zadavatele - ANO/NE. Účastník musí splňovat veškeré minimální technické požadavky zadavatele. [↑](#footnote-ref-4)
5. Účastník vyplní splnění závazných požadavků zadavatele - ANO/NE. Účastník musí splňovat veškeré minimální technické požadavky zadavatele. [↑](#footnote-ref-5)