Příloha č. 1 výzvy k podání nabídky

**TECHNICKÁ SPECIFIKACE A POŽADAVKY**

k veřejné zakázce malého rozsahu s názvem

**„Systém pro ochranu koncových stanic a serverů – EDR“**Registrační číslo projektu: CZ.06.01.01/00/22\_010/0002965

1. **Účastník zpracuje technickou část nabídky** podle této osnovy, která bude nedílnou součástí nabídky a připojí ji jako přílohu č. 1 návrhu smlouvy.
2. **Účastník zpracuje** **v technické části nabídky detailní popis EDR řešení**, zejména:

- specifikaci technických údajů (výrobce, typ licence…) včetně technického popisu;

**-** rozsah a způsob poskytování technické podpory (detailní popis, který bude v souladu s čl. XI. návrhu smlouvy);

**-** předpokládaný rozsah součinnosti objednatele (detailní popis, který bude v souladu s čl. VII. návrhu smlouvy);

**-** předpokládaný termín dodávky.

**Součástí technické části nabídky zpracované účastníkem bude vyplněná verifikační tabulka uvedená níže, která bude podkladem pro provedení akceptačních testů (viz čl. V návrhu smlouvy).**

**Zadavatel požaduje:**

- dodávku systému pro zvýšení kybernetické bezpečnosti koncových stanic a serverů – EDR řešení (Endpoint Detection & Response Software) pro 300 koncových stanic a 50 virtuálních serverů včetně instalace a implementace do prostředí IS ÚMČ Praha 12 a vytvoření nezbytné dokumentace;

- následné zajištění technické a záruční podpory v délce trvání 36 měsíců.

Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze systému, funkce zařazené na tzv. roadmapu nebudou akceptovány. Pokud jakákoli níže uvedená funkcionalita vyžaduje licenci, tak tato licence musí být součástí nabídky i nabídkové ceny.

**Nabízené EDR řešení musí splňovat parametry dle níže uvedené verifikační tabulky:**

Nabízené EDR řešení musí splňovat parametry dle níže uvedené verifikační tabulky. **Účastník je povinen vyplněnou tabulku přiložit do své nabídky.**

Účastník vyplní vždy sloupec „Nabízené zařízení splňuje minimální požadavky: „ANO/NE“. V případě, uvedení slova „ANO“ specifikuje blíže naplnění parametru (pokud je bližší specifikace možná).

V případě uvedení slova „NE“ může být nabídka vyloučena ze zadávacího řízení z důvodu nesplnění povinných požadavků pro účast v zadávacím řízení.

|  |  |  |
| --- | --- | --- |
| **Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno) a požadované funkce** | **Splněno ANO/NE** | **Stručný popis plnění** |
|  |  |  |
| **1.      Konzole pro centrální správu řešení:** |  |  |
|  |  |  |
| Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Konzole pro centrální správu je kompletně multi-tenantní | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Základní vlastnosti** |  |  |
| Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 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 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Úlohy správy bezpečnosti** |  |  |
| Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Centralizované místo pro záznam všech úloh | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 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) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Reportování** |  |  |
| Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost zasílání vygenerovaných reportů e-mailem | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Karanténa** |  |  |
| Vzdálená obnova či smazání souboru v karanténě | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost automaticky přidat soubor do výjimky při obnově z karantény | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Uživatelé** |  |  |
| Více předdefinovaných rolí: |  |  |
| Root, administrátor, reportér |  |  |
| 1.       Root: spravuje komponenty řešení | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 2.       Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 3.       Reportér: spravuje a vytváří reporty | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Logy** |  |  |
| Zaznamenávání uživatelských akcí | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detailní log pro každou akci | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Komplexní vyhledávání v logách | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Správa a instalace ochrany** |  |  |
| Instalace může být provedena několika způsoby, alespoň: |  |  |
| 1.       Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 2.       Instalace vzdáleně přímo z konzole správy | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 3.       Distribuce instalačního balíčku pomocí GPO či SCCM | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 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 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Konzole správy obsahuje detailní informace o chráněných strojích | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost spustit Network discovery z kteréhokoli již instalovaného klienta | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
|  |  |  |
| **1.      Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):** |  |  |
|  |  |  |
| Podpora operačních systémů: |  |  |
| Windows 11 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows 10 1507 a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Embedded POSReady 7 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2022 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2022 Core | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2019 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2019 Core | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2016 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2016 Core | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2012 R2 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2012 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2008 R2 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Ubuntu 16.04 LTS a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Red Hat Enterprise Linux 7xx | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| CentOS 7.0 a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| SUSE Linux Enterprise Server 12 SP4 a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Fedora 31-36 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Debian 9.0-11.0 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Oracle Linux 7.x-8.x | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Mac OS X Sierra (10.12) a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Automatické skenování paměti procesů v reálném čase | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce na základě virových definicí (tzn. signatur) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day útoků na základě odhalování anomálního chování | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day bezsouborových útoků | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je toto CVE uvedeno | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 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 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje analýzu vektoru útoku | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje vzdálené připojení na příkazové řádek koncového bodu (Powershell, Zshell, Bash/výchozí CLI v Linux) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost skenovat archivy | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost rozšíření na XDR - sonda síťového provozu | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost rozšíření na XDR - sonda do AD, Azure AD, MS Intune | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost rozšíření na XDR - sonda do Office365/Microsoft365 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost rozšíření na XDR – sonda do Azure | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost rozšíření na XDR – sonda do AWS | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost rozšíření na XDR – sonda do Google Workspace | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Karanténa** |  |  |
| Možnost obnovy souboru do originální či do nově zadané lokality | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| **Kontrola přístupu k internetu** |  |  |
| Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
|  |  |  |
| **1.      Ochrana virtualizovaných koncových bodů (Windows, Linux)** |  |  |
|  |  |  |
| Podpora operačních systémů: |  |  |
| Windows 11 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows 10 1507 a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Embedded Compact 7 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2022 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2022 Core | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2019 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2019 Core | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2016 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2016 Core | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2012 R2 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2012 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Small Business Server 2011 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Windows Server 2008 R2 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Ubuntu 16.04 LTS a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Red Hat Enterprise Linux 7xx | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| CentOS 7.0 a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| SUSE Linux Enterprise Server 12 SP4 a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Fedora 31-36 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Debian 9.0-11.0 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Oracle Linux 7.x-8.x | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Mac OS X Sierra (10.12) a vyšší | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce na základě virových definicí (tzn. signatur) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Automatické skenování paměti procesů v reálném čase (včetně ochrany proti 0-day útokům) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day útoků na základě odhalování anomálního chování | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day bezsouborových útoků | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| 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 | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje analýzu vektoru útoku | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje vzdálené připojení na příkazové řádek koncového bodu (Powershell, Zshell, Bash/výchozí CLI v Linux) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Možnost skenovat archivy | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci) | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |
| Dodavatel prohlašuje, že neobchoduje se sankcionovaným zbožím, které se nachází v Rusku nebo Bělorusku či z Ruska nebo Běloruska pochází a nenabízí takové zboží v rámci plnění veřejných zakázek. | DOPLNÍ ÚČASTNÍK | DOPLNÍ ÚČASTNÍK |