**Příloha č. 6b zadávací dokumentace ve veřejné zakázce**

**„ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI MĚSTA LOVOSICE“**

**ČÁST 02: ANTIVIRUS**

**TECHNICKÁ SPECIFIKACE**

# PŘEDMĚT PLNĚNÍ

Zadavatel požaduje nasazení nástroje pro ochranu 140 koncových stanic a 40 serverů před škodlivým kódem s rozšířenými možnostmi reakce na bezpečnostní incidenty (Endpoint Detection & Response – EDR nebo eXtended Detection & Response – XDR) na období 60 měsíců. Řešení musí být tvořeno jedním agentem instalovaným na koncových systémech a centralizovanou správou prostřednictvím jedné webové konzole umožňující komplexní administraci. Agent nesmí ke své funkci vyžadovat připojení do cloudu ani k centrální správě za účelem poskytování ochrany proti škodlivému kódu.

Dodávané řešení Endpoint Detection & Response musí minimálně splňovat dále uvedené funkce a parametry.

**Popis plnění:**

Projekt je koncipován jako ucelené řešení zadavatele, nikoliv jako dodávka technologie. Skládá se z následujících provázaných celků:

* Technologie: dodání konkrétního produktu dle technické specifikace.
* Implementace: implementace řešení tak, aby v plné funkcionalitě běželo na všech systémech Zadavatele zapojených do projektu (včetně případné analýzy a řešení takových zařízení, kde nástroj bude vykazovat problémy s instalací nebo po instalaci).
* Integrace: integrace na stávající provozní a bezpečnostní systémy v síti Zadavatele, vyladění konfigurace tak, aby nedošlo k omezení funkčnosti interních informačních systémů a zároveň na daných serverech byl agent nainstalován a provozován.
* Automatizace: návrh a realizace automatizačních scénářů pro abstrakci práce s technologií formou snadno použitelných předpřipravených akcí pro operátory bez nutnosti manuálního zásahu do konfigurace technologie.
* Technická podpora: zajištění technické podpory dodavatele, která bude zahrnovat asistenci při řešení provozních incidentů, konzultace při nasazení nových funkcí EDR a pravidelné aktualizace softwaru a zodpovídání dotazů.

Nastavení konfigurace a uvedení do ostrého provozu musí být rozplánováno s ohledem na kapacitní možnosti Zadavatele, případně servisní okna daného prostředí dle dopadů na funkcionalitu.

# TECHNICKÁ SPECIFIKACE

Zadavatel požaduje nástroj pro ochranu koncových stanic před škodlivým kódem s rozšířenými možnostmi reakce na bezpečnostní incidenty (Endpoint Detection & Response – EDR nebo eXtended Detection & Response – XDR). Požadované řešení musí být tvořeno jedním agentem instalovaným na koncových systémech a centrální správou poskytovanou formou SaaS, která disponuje jednotnou webovou konzolí pro komplexní správu. Agent nesmí pro zajištění ochrany před škodlivým kódem vyžadovat připojení ke cloudu ani k centrální správě. Dodávané řešení Endpoint Detection & Response musí splňovat alespoň níže uvedené funkce a parametry.

## Výrobce a řešení

|  |  |
| --- | --- |
| **Výrobce a řešení** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Vzhledem k rozsáhlosti trhu s řešeními pro ochranu koncových zařízení není v možnostech zadavatele provést detailní analýzu všech dostupných produktů. Z tohoto důvodu zadavatel požaduje, aby nabízené řešení bylo evaluováno alespoň jednou z renomovaných analytických společností – Gartner nebo Forrester – a aby se v jejich aktuálních srovnáních – Gartner Magic Quadrant for Endpoint Protection Platforms 2025 nebo The Forrester Wave™: Extended Detection And Response Platforms, Q2 2024 – umístilo v kategorii „Leaders“. Tento požadavek zajišťuje, že nabízené řešení splňuje vysoké standardy odborného hodnocení a odpovídá osvědčeným bezpečnostním trendům. |  |
| Zadavatel dále požaduje, aby se výrobce s nabízeným produktem účastnil alespoň jednoho ze dvou posledních testů MITRE ATT&CK Evaluations (2023, 2024) pro účely srovnání detekčních schopností EDR dle kapitoly „Kvalita detekce a úroveň visibility“. |  |

## Architektura řešení

|  |  |
| --- | --- |
| **Architektura řešení** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Centrální správa řešení musí být provozována jako SaaS cloudové řešení. Je nutné, aby data byla uložena a zpracovávána na serverech v EU. |  |
| Agent musí podporovat následující operační systémy:  Windows 7 SP1, 10, 11 a případné novější verze  Windows Server 2008 R2 SP1, 2012 R2, 2016, 2019, 2022, 2025 a případné novější verze  Linux distribuce RHEL (7, 8, 9), CentOS (7, 8), Rocky Linux (8, 9), Debian (11, 12), Ubuntu (20.04, 22.04) a případné novější verze  Běžný provoz agenta nesmí mít dopad na výkon koncové stanice (předpokládá se maximálně 5 % CPU, 500 MB RAM).  Instalace ani aktualizace agenta nesmí vyžadovat restart koncového systému pro provozování plnohodnotné ochrany. |  |
| Agent musí podporovat následující operační systémy:   * Windows 7 SP1, 10, 11 a případné novější verze * Windows Server 2008 R2 SP1, 2012 R2, 2016, 2019, 2022, 2025 a případné novější verze * Linux distribuce RHEL (7, 8, 9), CentOS (7, 8), Rocky Linux (8, 9), Debian (11, 12), Ubuntu (20.04, 22.04) a případné novější verze |  |
| Běžný provoz agenta nesmí mít dopad na výkon koncové stanice (předpokládá se maximálně 5 % CPU, 500 MB RAM). |  |
| Instalace ani aktualizace agenta nesmí vyžadovat restart koncového systému pro provozování plnohodnotné ochrany. |  |

## Ochrana proti škodlivému kódu

|  |  |
| --- | --- |
| **Ochrana proti škodlivému kódu** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Řešení nesmí spoléhat primárně na signaturní detekci nebo reputační engine. |  |
| Řešení musí umět detekovat pokročilé hrozby, alespoň:   * souborový malware, * fileless útoky, * neznámý malware, * exploity, * ransomware, * cryptominer malware, * škodlivé skripty, * lateral movement, * pokusy o exploitaci zranitelností, * pokusy o zajištění persistence, * pokusy o neoprávněnou eskalaci privilegií, * známé ransomwarové techniky (například mazání shadow copies). |  |
| Výše uvedené musí dokázat agent detekovat i bez nutnosti konektivity do cloudu nebo centrální správy. |  |
| Detekci malware musí řešení umožňovat ve dvou fázích, jak před samotným spuštěním (preexecution), tak i za běhu (run-time). |  |
| Řešení musí umožňovat automatizovanou reakci na detekované hrozby, alespoň:   * notifikace o detekované hrozbě uživateli i administrátorovi řešení; * vynucené ukončení škodlivého/podezřelého procesu; * přesunutí škodlivých/podezřelých souborů do karantény; * odpojení napadené stanice od sítě a zachování komunikace pouze s centrální správou; * kompletní remediace útočníkových aktivit (vynucené ukončení procesů, smazání zdrojových souborů útočníkových aktivit, obnovení konfigurace OS do původního stavu). |  |
| Řešení musí umožňovat provést jakoukoliv z výše uvedených aktivit také manuálně z centrální správy. |  |
| Agent na koncových systémech musí být schopen detekovat a zabránit pokusům o jeho vypnutí, poškození nebo jakoukoliv manipulaci s jeho soubory. |  |
| Odinstalace nebo vypnutí agenta musí být umožněna pouze po zadání hesla. Zadavatel požaduje možnost specifického hesla pro každého nainstalovaného agenta. Řešení musí podporovat funkci hromadné odinstalace za využití jednotného hesla, kterou ale je nutné nejprve zapnout. |  |
| Systém musí umožnit vytváření politik s možností výběru detekčních enginů/modulů. |  |
| Zadavatel požaduje, aby řešení bylo rozšířitelné o vlastní sandboxovou technologii pro manuální i automatickou aktualizaci (tato funkce ale není předmětem dodávky, předpokládá se, že řešení však takovou funkci nabízí například jako add-on licenci, kterou může Zadavatel do budoucna nakoupit a využívat). |  |

## Device Control

|  |  |
| --- | --- |
| **Device Control** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Funkce Device Control je požadována pro zařízení s operačním systémem Windows a macOS. |  |
| Agent musí poskytovat možnost spravovat připojitelná zařízení (device control modul) alespoň pro USB rozhraní. |  |
| EDR musí zobrazovat informace o používaných USB zařízeních napříč celým prostředím (výrobce, typ zařízení, datum a čas připojení). |  |
| EDR musí poskytnout informace o souborech zapsaných na USB zařízení (například formou analýzy telemetrických dat). |  |
| Pro vyměnitelné velkokapacitní disky (USB flash disky, externí disky apod.) musí řešení umožnit specifikovat politiku přístupu. Řešení musí umožnit vynutit:   * zákaz takových zařízení, * připojení pouze pro čtení, * specifikovat výjimky z dvou výše uvedených pravidel. |  |

## EDR funkce

|  |  |
| --- | --- |
| **EDR funkce** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Telemetrická data jsou po celou dobu jejich uchovávání indexována, lze v nich vyhledávat a standardně s nimi pracovat. To předpokládá minimálně následující:   * vyhledávat aktivity dle níže uvedeného bodu 3 (Prohledávání telemetrických dat); * vyhledávání IoCs (SHA256 a MD5 hashe, IP adresy, doménové názvy) z konzole. |  |
| Je požadováno, aby všechna telemetrická data byla přístupná ze stejné konzole, aby se analytik nemusel přepínat mezi konzolemi (například prohledávání dat z posledních 7 dní v jedné konzoli a prohledávání starších dat v druhé konzoli). |  |
| Prohledávání telemetrických dat je možné pomocí jednoho dotazu nad celou databází, tedy nad všemi daty ze všech agentů za celou dobu retence dat. |  |
| Agent v rámci telemetrických dat musí umožňovat sbírat informace v rozsahu alespoň:   * vytvoření, ukončení procesu, * vytvoření, smazání, modifikace a přejmenování souboru, * IP adresa síťové komunikace (TCP i UDP protokol), * DNS requesty, * informace o přihlášení a odhlášení uživatele, * aktivity v rámci Windows registry – vytvoření a modifikace klíče a vytvoření a modifikace hodnoty (alespoň pro startup/run klíče), * vytvoření a spuštění nové plánované úlohy, * logování příkazů zadávaných v CLI ručně nebo skriptem (bash, powershell, příkazový řádek). |  |
| Řešení musí umět korelovat alespoň výše uvedené spolu související události a pro takové související události umožňovat jejich vyčítání (například pomocí unikátního ID) i pro události, které nebyly detekované jako podezřelé nebo škodlivé. |  |
| Nabízené řešení musí umožnit pokročilé vyhledávání a dotazování nad shromážděnými telemetrickými daty z endpointů, a to pro účely threat huntingu a manuální analýzy bezpečnostních incidentů. Řešení musí podporovat:   * vytváření komplexních dotazů nad bezpečnostními daty včetně možností filtrování, řazení a kombinování podmínek; * vyhledávání podle široké škály atributů (např. procesy, síťová komunikace, registr, souborový systém, knihovny v paměti, načtené moduly); * možnost zpětného dotazování na historická data alespoň 7 dní; * tvorbu uživatelských dotazů pomocí SQL-like syntaxe nebo předdefinovaných filtrů; * automatizované dotazy pro opakovanou detekci anomálií (např. alerting na podezřelé aktivity na základě dotazů); * možnost exportu výsledků do CSV případně JSON; * možnost uložení již vytvořených vyhledávacích queries. |  |
| Řešení musí umožňovat v rámci investigace incidentu zobrazení tzv. process tree a časové osy událostí. |  |
| Řešení musí podporovat tvorbu vlastních detekčních / alert pravidel na základě alespoň níže uvedených parametrů:   * vytvoření definovaného procesu, * vytvoření definovaného souboru, * komunikace na definovanou doménu. |  |
| Řešení na základě výše uvedených vlastních detekčních pravidel dokáže kromě hlášení detekce aktivity také preventovat (terminace procesu, blokace spuštění procesu). |  |
| Řešení musí umožňovat alespoň následující manuální response aktivity:   * vzdálené terminálové připojení k stanici; * síťovou izolaci stanice se zajištěním komunikace do cloudové centrální správy a s možností využívat základní protokoly pro úspěšnou síťovou komunikaci (DNS, DHCP apod.); * stažení libovolných souborů z koncové stanice pro účely detailní analýzy; * nahrání skriptů na koncovou stanici a jejich vzdálené spuštění; * procházení souborového systému, zjišťování hashe vybraných souborů; * zobrazit běžící procesy; * terminace vybraného běžícího procesu; * procházet Windows registry. |  |
| Výše uvedené terminálové připojení ke stanici musí být plně auditováno (který uživatel se připojoval, na jakou stanici, jaké aktivity prováděl). |  |
| Jednotná konzole pro správu firewall politik napříč všemi podporovanými operačními systémy (Windows, Linux, macOS) z téže konzole jako EDR funkce |  |
| Zadavatel požaduje možnost vzdáleně se připojit k terminálové relaci pouze uživatelům s příslušným oprávněním. |  |

## Automatizace

|  |  |
| --- | --- |
| **Automatizace** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Řešení musí umožnit automatizaci incident response playbooků alespoň v rozsahu:   * síťová izolace zařízení v případě definovaného incidentu (např. kritická závažnost, ransomware, lateral movement a podobně); * přiřazení striktnějších prevenčních politik v případě detekovaného incidentu; * automatické získání hashe procesu identifikovaného v incidentu a jeho přiřazení do custom IOCs. |  |
| Další návrh automatizačních scénářů je předmětem plnění dodavatele. |  |

## Kvalita detekce a úroveň visibility

|  |  |
| --- | --- |
| **Kvalita detekce a úroveň visibility** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Za rozhodující faktor se považuje hodnocení z MITRE ATT&CK Evaluations. |  |
| Řešení musí alespoň v jednom z posledních dvou kol (2023 – 5. kolo označené Turla, 2024 – 6. kolo označené Enterprise 2024) splňovat:   * řešení v testech nevynechalo scénáře zaměřené na Linux platformu; * řešení musí úspěšně detekovat (kategorie Technique, Tactic, General) alespoň 90 % realizovaných technik (substeps) v testech Detections; * řešení musí úspěšně zablokovat alespoň 90 % realizovaných testovacích scénářů v testech Protections. |  |

## Centrální správa

|  |  |
| --- | --- |
| **Centrální správa** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Centrální správa musí umožňovat hierarchické dělení zařízení do skupin. |  |
| Řešení musí umožňovat snadné a efektivní nastavení výjimek na definované skupiny zařízení. Je požadováno, aby vybrané zařízení mohlo být členem více skupin. |  |
| Řešení pro aplikaci výjimek nesmí vyžadovat restart zařízení. |  |
| Zadavatel požaduje, aby bylo možné vynutit vícefaktorovou autentizaci do centrální správy alespoň pomocí TOTP. |  |
| Řešení musí umožňovat zasílat alespoň následující notifikace pomocí SMTP:   * detekce podezřelého nebo škodlivého incidentu / události, * odinstalace agenta, * otevření terminálového remote shell spojení, * provedení síťové karantény zařízení, * odebrání zařízení ze síťové karantény. |  |
| Řešení poskytuje detailní auditování uživatelských aktivit. |  |
| Řešení musí poskytovat alespoň následující typy reportů:   * management report s počtem detekovaných hrozeb, stavem mitigace a změnou oproti předchozímu období / reportu, počtem instalovaných agentů; * přehled hrozeb, typ hrozby, způsob detekce, způsob mitigace, datum a čas detekce, infikované systémy, verdikt analytika (true vs false positive) a stav incidentu; * seznam všech agentů se zobrazením alespoň IP adresy, OS, skupiny, verze agenta, poslední konektivity do centrální správy. |  |

## Integrace

|  |  |
| --- | --- |
| **Integrace** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Řešení musí disponovat rozhraním API pro integraci s interními systémy zákazníka. |  |
| Řešení musí být schopno integrace na systémy sbírající a korelující logy. |  |
| Řešení umožňuje integraci na Threat Intelligence služby za účelem ověřování vůči aktuálním reputačním databázím (minimálně IP adresy a hashe). |  |

**Konkrétní typ a označení nabízeného řešení:**

1. **NABÍZENÉ ŘEŠENÍ:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE VÝROBKU NEBO NABÍZENÉHO ŘEŠENÍ (HW i SW SOUČÁSTI UVEĎTE SAMOSTATNĚ) JE PŘEDMĚTEM JEHO NABÍDKY – minimálně uvede název výrobce, obchodní název výrobku, typ nebo verzi]

## Analýza a implementace

|  |  |
| --- | --- |
| **Analýza a implementace** | |
| **MINIMÁLNÍ POŽADAVKY** | **ANO/NE** |
| Provedení a zpracování vstupní analýzy. |  |
| Zprovoznění SaaS centrální správy. |  |
| Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory zadavatele. Nastavení SSO. |  |
| Nastavení skupin zařízení, konfigurace politik, známých výjimek. |  |
| Instalace na pilotní vzorek zařízení, vyladění politik a vytvoření potřebných výjimek na 3rd party software. |  |
| Podpora během hromadného nasazování agentů. |  |
| Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting. |  |
| Vytvoření uživatelské dokumentace. |  |
| Realizace akceptačních testů. |  |
| Školení pro administrátory řešení v rozsahu 2 dní. |  |

# PROHLÁŠENÍ DODAVATELE

**Dodavatel podáním nabídky potvrzuje, že předmět nabídky se plně shoduje s výše uvedenými požadavky.**

V [DOPLNÍ DODAVATEL] dne [DOPLNÍ DODAVATEL]

................................................

[DOPLNÍ DODAVATEL]