

Projektová dokumentace

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU
KOLÍN - zpracování projektové dokumentace“***

TECHNOLOGICKÁ ČÁST JCE IB

D.1.4.9. Technologie a řešení JCE IB

***D.1.4.9.09. ENDPOINT DETECTION AND RESPONSE
(EDR) - ŠKOLA***

Zpracoval:

Petr Lacina

9 ENDPOINT DETECTION AND RESPONSE (EDR) - ŠKOLA

9.1 POPIS

EDR je určeno pro zvýšení ochrany před kybernetickými útoky na koncových zařízeních. Nástroj je určen pro detekci pokročilých hrozeb a rozšiřuje nebo nahrazuje standardní antivirová řešení, která tyto hrozby dnes plně nepokrývají. Detekuje pokročilé typy hrozeb na základě setrvalého monitoringu na koncových zařízeních. Vyhodnocuje nezvyklé chování a pokusy o napadení systému hackery prostřednictvím identifikátorů kompromitace. Dále umožňuje reagovat na vzniklé hrozby prostřednictvím automatizované reakce a zabránit útočníkovi v hlubším průniku do infrastruktury.

V rámci provozního prostředí Školy a s ohledem na MBS EDR bude zajišťovat schopnost detekce hrozeb na koncových stanicích a serverech.

V rámci realizačního projektu je požadavkem, aby řešení bylo propojitelné s dalšími technologiemi. V rámci Školy se jedná o sběr a archivaci logů v rámci LM.

V rámci provozního prostředí Školy EDR zvýší schopnosti detekce hrozeb na koncových stanicích a serverech a reakce na ně. Toto stávající antivirové řešení nepokrývá v dostatečné míře.

Není ale uvažováno kompletní nahrazení antivirového řešení pouze samotným EDR. EDR by mělo antivirové řešení doplnit, nebo tuto část obsahovat. V případě dodávky kombinace AV + EDR jsou požadovány následující vlastnosti níže.

9.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

9.2.1 Požadavky na antivirové řešení

Požadovaná funkcionalita	Specifikace minimálních požadavků
Podporované klientské platformy - OS: Windows, Linux, MacOS, Android, vše v českém jazyce	
Nativní podpora architektur pro platformy Windows a MacOS:	x86
	x64
	ARM64
Antimalware, antiransomware, antispysware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.	
Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebírání pravidel z brány Windows Firewall.	
Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.	
Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému.	
Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.	
Systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:	síťové protokoly,
	Flash Player,
	Javu,
	Microsoft Office,
	webové prohlížeče,
	e-mailové klienty,
	PDF čtečky...
	Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě.
	Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS...).
Anti-phishing se schopností detekce homoglyph útoků.	

Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.	
Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů.	
Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.	
Kontrola souborů při zapisování na disku a extrahování archivačních souborů	
Detekce s využitím strojového učení.	
Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.	
Ochrana před síťovými útoky skenující síťovou komunikaci a blokuji pokusy o zneužití zranitelností na síťové úrovni.	
Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.	
Lokální sandbox.	
Modul behaviorální analýzy pro detekce chování nových typů ransomwaru.	
Systém reputace pro získání informací o závadnosti souborů a URL adres.	
Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.	
Technologie pro detekci rootkitů obvykle se maskujících za součásti operačního systému.	
Skener firmwaru BIOSu a UEFI.	
Skenování souborů v cloudu OneDrive.	
Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal	
IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent.	
Funkcionalita pro klienty MacOS – Personal Firewall, Device control, autoupgrade.	
Možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek.	
Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem.	
Podpora automatického vytváření dump souborů na stanici na základě nálezů.	

Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze).	
Duální aktualizací profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky).	
Možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovníctvím.	
Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP.	
Možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích.	
Automatické aktualizace bezpečnostního softwaru s možností odložení restartu stanice.	
„Zmražení“ na požadované verzi – produkt je možné nakonfigurovat tak, aby nedocházelo k automatickému povyšování majoritních a minoritních verzí zejména na stanicích, kde se vyžaduje vysoká stabilita.	
Počet licencí	Požadovaný počet licencí pro účely školy ke 295 ks.
Záruka a servisní podpora	Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.

9.2.2 Požadavky na sandbox

Požadovaná funkcionalita	Specifikace minimálních požadavků
Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě	
Sandbox umožňující spuštění vzorků malware pro:	Windows
	Linux
Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů	
Analýza neznámých vzorků v řádu jednotek minut.	
Optimalizace pro znemožnění obejití anti-sandbox mechanismy.	
Schopnost analýzy rootkitů a ransomwaru.	
Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.	
Řešení pracuje s behaviorální analýzou.	
Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru.	
Manuální odeslání vzorku do sandboxu.	
Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.	
Neomezené množství odesílaných souborů.	
Veškerá komunikace probíhá šifrovaným kanálem.	
Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu.	
Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.)	
Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.	
Výsledky analyzovaných souborů jsou dostupné a automatizovaně distribuované všem serverům a stanicím napříč organizací, tak aby nedocházelo k duplicitnímu testování.	

9.2.3 Požadavky na EDR

Požadovaná funkcionality	Specifikace minimálních požadavků
Možnost provozu centrálního serveru on-premise na platformě Windows Server	
Webová konzole pro správu a vyhodnocení	
Možnost provozu s databázemi:	Microsoft SQL, MySQL
Možnost provozu v offline prostředí	
Autonomní chování se schopností vyhodnotit podezřelou/škodlivou aktivitu a zareagovat na ni i bez aktuálně dostupného řídicího serveru nebo internetového připojení	
Logování činností administrátora (Audit Log)	
Podpora EDR pro systémy Windows, Windows server, MacOS a Linux	
Možnost autentizace do managementu EDR pomocí 2FA	
Možnost řízení managementu EDR prostřednictvím API, a to jak pro:	Přijímání informací z EDR serverů
	Zasílání příkazů na EDR servery
Integrovaný nástroj v EDR řešení pro vzdálené zasílání příkazů přímo z konzole	
Možnost izolace zařízení od sítě	
Možnost tvorby vlastních IoC.	
Možnost škálování množství historických dat vyhodnocených v EDR:	až 3 měsíce pro raw-data,
	3 roky pro detekované incidenty.
„učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům	
Indikátory útoku pracující s behaviorální detekcí.	
Indikátory útoku pracující s reputací.	
Řešení umožňuje analýzu vektorů útoku.	
Schopnost detekce:	škodlivých spustitelných souborů
	skriptů,
	exploitů,
	rootkitů,
	síťových útoků,
	zneužití WMI nástrojů,

	bezsuborového malwaru
	škodlivých systémových ovladačů / kernel modulů.
	Pokusů o dump přihlašovacích údajů uživatele
Schopnost detekovat laterální pohyb útočníka.	
Analýza procesů, veškerých spustitelných souborů a DLL knihoven.	
Náhled na spuštěné skripty použité při detekované události	
Možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR	
Schopnost automatizovaného response úkonu pro jednotlivá detekční pravidla v podobě:	izolace stanice,
	blokace hash souboru,
	blokace a vyčištění sítě od konkrétního souboru,
	ukončení procesu,
	restart počítače,
	vypnutí počítače.
Automatického vyřešení incidentu administrátorem	
Prioritizace vzniklých incidentů.	
Možnost stažení spustitelných souborů ze stanic pro bližší analýzu ve formátu archivu opatřeným heslem	
Integrace a zobrazení detekcí provedených antimalware produktem.	
Řešení je schopno generovat tzv. forest / full execution tree model.	
Vyhledávání pomocí nově vytvořených IoC nad historickými daty.	
Provázání s technikami popsány v knowledge base MITRE ATT&CK.	
Integrovaný vyhledávač VirusTotal s možností rozšíření o vlastní vyhledávač	
Počet licencí	Požadovaný počet licencí pro účely školy ke 295 ks.
Záruka a servisní podpora	Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.