

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.1.4.9.16. ENDPOINT DETECTION AND RESPONSE
(EDR) - CYLAB***

Zpracoval:

Petr Lacina

16 ENDPOINT DETECTION AND RESPONSE (EDR) - CYLAB

16.1 POPIS

Technologie Endpoint Detection and Response (EDR) bude určena v rámci CYLAB k výukovým účelům, kde studentům umožní pochopit princip fungování procesů a koncových stanicích a serverech a způsoby detekce útočníka, který se v nich pohybuje.

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 CYLAB je plánován provoz řešení v rámci virtualizace, která má pro tyto účely dostatečné kapacity. Vybrané řešení tedy musí umožňovat nasazení jako virtuální appliance.

Základním požadavkem je také integrovatelnost s LM+SIEM, který bude v rámci CYLAB provozovaný.

16.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

16.2.1 Technické vlastnosti řešení

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 CYLAB ke 114 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.