McAfee Active Response

V dnešní době organizace požadují snadněji použitelné a lehce integrovatelné nástroje, které pomáhají účinněji detekovat přítomnost škodlivých aktivit a následně umožní rychlé předání informací pro analýzu, kategorizaci a odstranění nežádoucího kódu/aktivity. McAfee Active Response umožňuje velmi dobrou out-of-the-box automatizovanou interakci se stávajícími řešeními pro správu a zabezpečení koncových stanic. Dále také poskytuje soubor nástrojů pro eliminaci bezpečnostních hrozeb (ukončení procesu, odstranění souboru nebo klíče z registru apod.). Jedná se o ideální nástroj pro Security Operations Center ve velkých organizacích. Bez takového nástroje je Incident response na koncových strojích velmi časově náročná činnost, popř. vyžaduje mnoho součinnosti i koncových uživatelů.

Klíčové funkcionality:

- **Kolektory** – Pomáhají najít a vizualizovat data ze systému (soubory, síťový provoz, registry) – možnost definovat vlastní kolektory.
- **Triggery a perzistentní kolektory** – Průběžné sledování kritických událostí nebo změn pomocí jedné sady příkazů. Automatická reakce na události.
- **Reakce na události** – Provádění akcí pomocí předdefinovaných či přizpůsobitelných příkazů (ukončení procesu, odstranění souboru apod.).
- **Centralizovaný management ePO** – Jediná konzole pro kompletní správu zabezpečení.
- **Integrated Security Architecture** – Pomocí DXL nabízí real-time komunikace s ostatními bezpečnostními zařízeními McAfee.

Detekce a náprava pokročilých hrozeb

Automatizovaný – Zachytí a monitoruje události, soubory, host flow, objekty, souvislosti a změny stavu systému, které mohou být identifikátorem útoku (IoAs) či skrytých hrozeb. Informace pak poskytuje dále pro forenzní analýzy.
Adaptabilní – Administrátor dostává okamžitá upozornění, díky kterým může adekvátně reagovat na vyvíjející se (samoučící se) hrozby spuštěním standardních i optimalizovaných nástrojů pro vyhledávání hrozeb, drill-down operací nad specifickými IoAs, a umožní porozumět jejich rozsahu a eliminovat jeho působení.
Kontinuální – Definuje perzistentní kolektory – schopnost, která umožňuje být stále ve střehu (Always ON), analyzuje vnitřní data systému a spouští výstrahy při detekci útočných aktivit, předvídá možné budoucí ohrožení a poskytuje účelné monitorovací nástroje.
Reaktivní - Po obdržení upozornění, že koncový bod může být infikován, poskytne nástroje pro reakci (triggery či skripty) na tyto nálezy (zastavení procesů, odstranění souborů, či složitější operace na bázi skriptů).
Proaktivní – Prostřednictvím ePO umožňuje zasílat dotazy na koncové stanice (dotaz na seznam aktuálních procesů, existující klíč v registru apod.). Nabízí real-time vyhledávání podle metadat procesů, síťového provozu atd. a na výsledek vyhledávání je možné navázat reakcí (spuštěním skriptů), ty se dají automatizovat pomocí triggerů.

Advanced Threat Defense (ATD)

McAfee ATD je sofistikované řešení kombinující několik přístupů k identifikaci (ne)známého (zero-day), pokročilého škodlivého kódu (Advanced Malware). Integruje se se stávající McAfee infrastrukturou od perimetru až po koncová zařízení a ve větších organizacích maximalizuje schopnost detekovat jakýkoli malware i efektivně na nákazu reagovat v minimálním časovém rozpětí. Využívá koncepci *Find, Freeze, Fix* v boji proti pokročilým hrozbám.
Find: Metoda, která pro odhalení nebezpečného kódu využívá dynamickou (sandboxing) i statickou analýzu.
Freeze: Zabraňuje dalšímu šíření škodlivého kódu. ATD buď přímo nebo pomocí TIE umožňuje neprodleně zakročit proti škodlivému malware a zamezí tak dalšímu šíření.
Fix: Umožňuje napravit napáchané škody. V této fázi se jedná o odstranění dopadů malwaru na koncových strojích skrze McAfee ePolicy Orchestrator, jako jsou změny v registrech, soubory zapsané na disk, úpravy konfigurací, aj.

COMGUARD security & networking
COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

Threat Inteligence Exchange

Společná inteligence pro eliminaci cílených útoků

McAfee Threat Intelligence Exchange (TIE) *poskytuje adaptivní detekci hrozeb a reakci na ně, čímž umožňuje proaktivně reagovat a eliminovat bezpečnostní hrozby na Vašich koncových zařízeních, síťových branách i datacentrech. Ochrana pomocí agentů (distribuovaných na koncových zařízeních), dokáže prakticky v řádech milisekund provést kroky, které vedou ke kategorizaci a odstranění hrozeb. Zkracuje tím tak životní cyklus malware na minimum. TIE je součástí spolupracujícího ekosystému, který využívá Data Exchange Layer (DXL) pro kombinaci a synchronizaci vstupů z vícero bezpečnostních zařízení (koncová zařízení, perimetrové appliance, sandboxing, GTI atd.), který okamžitě sdílí tato data se všemi napojenými bezpečnostními zařízeními, a to včetně řešení třetích stran.*

Spolupracující ekosystém

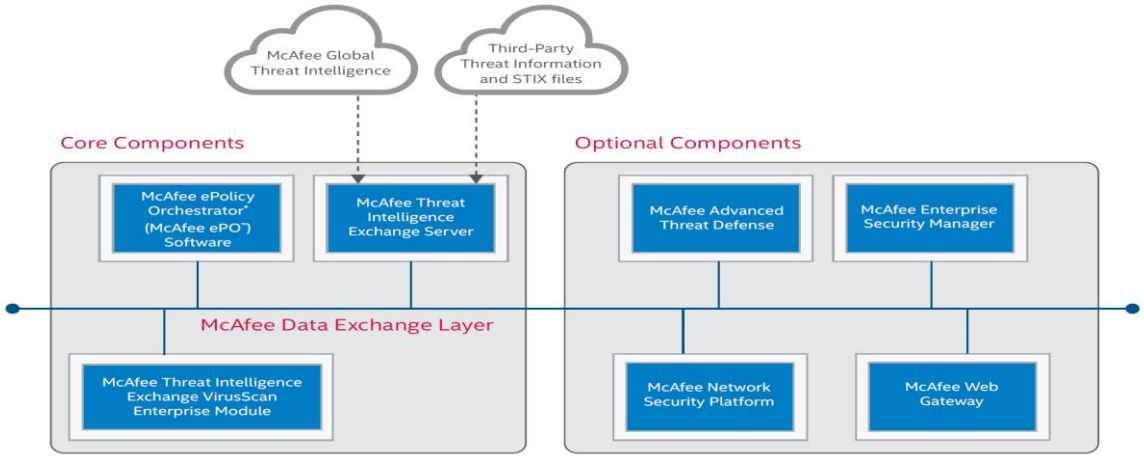
Spolupráce všech bezpečnostních prvků, které vystupují jako jeden celek. Integrovaná inteligence z různých zdrojů dat (i ze zdrojů řešení třetích stran) v kombinaci s kontextovými daty a signaturami umožňuje snadnější a rychlejší rozhodovací proces. Kombinuje data z GTI (Global Threat Intelligence), řešení třetích stran a STIX souborů s informacemi shromažďovanými z lokálních bezpečnostních zařízení a poté tyto informace vyhodnocuje a sdílí napříč všemi řešeními.

Blokace na základě reputace

Veškeré soubory jsou spuštěny pouze na základě reputace (pomocí DXL je odeslán hash ke kontrole a následně obdrží informaci s ohodnocením stupně důvěryhodnosti). Soubor s neznámou reputací nelze spustit a je odeslán na podrobnou analýzu do sandbox appliance, která ověří jeho chování. Veškerým souborům se špatnou (nízkou) reputací je zabráněno spuštění. Posbírané reputace z interní sítě může administrátor procházet a ovlivňovat centrálně pomocí ePO serveru.

Data Exchange Layer (DXL)

McAfee Threat Intelligence Exchange pro výměnu dat využívá Data Exchange Layer (DXL). Jedná se o specializovanou technologii na výměnu velkého množství informací (kontexty, signatury apod.) mezi všemi bezpečnostními zařízeními napojenými na DXL. Platforma DXL je vysoce škálovatelná a nabízí nízkou latenci pro transakce, prostřednictvím trvalého připojení a synchronizování, což umožňuje real-time komunikaci a reakci na zjištěné incidenty napříč všemi připojenými zařízeními. To představuje novou éru v oblasti bezpečnosti, kde všechny bezpečnostní komponenty spolupracují jako jeden soudržný systém, bez ohledu na výrobce nebo architekturu. Veškerá správa se provádí prostřednictvím ePolicy Orchestratoru.



COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz