McAfee Security Information and Event Management (SIEM)

Enterprise řešení pro sběr, analýzu, korelaci a reporting událostí

Bezpečnost IT lze považovat za efektivní, pokud máte přehled o všech aktivitách Vašich systémů, sítí, databází a aplikací v reálném čase. A právě řešení McAfee Enterprise Security Manager Vám dává kompletní přehled nad Vaší sítí a napomáhá tak identifikovat hrozby, patřičně na ně reagovat a zajišťovat tak neustálou shodu s mezinárodními bezpečnostními standardy.

SC MAGAZINE AWARDS 2014 Honored in the U.S.

McAfee Enterprise Security Manager (ETM)

Dává jasný globální pohled o událostech ve Vaší síti a umožňuje snadné provádění auditů a udržování shody se standardy. Je revolučním nástrojem v oblasti SIEM (Security Information and Event Management), jelikož v reálném čase propojuje informace o vnějších hrozbách, jako jsou nové zranitelnosti a reputace dat s aktuálním stavem vnitřního systému a dat.

Kritické informace během několika minut

Díky unikátnímu databázovému systému je možné shromažďovat a zpracovávat miliardy logů/událostí i několik let zpětně, a to vše s rychlostí naplňující požadavky největších korporací. Právě rychlý přístup a dlouhodobé uchovávání dat je klíčem k odhalení dlouhodobých útoků typu Advanced Persistent Threats.

Integrace s ostatními produkty

Integrace s řešením McAfee Risk Advisor (MRA) umožňuje řízení rizik v reálném čase. Navíc propojení s technologií McAfee Global Threat Inteligence (GTI) dovoluje posouzení vnějších rizikových faktorů. V důsledku je pak každé události přiděleno skóre na základě vnějších (GTI) i vnitřních (MRA) kritérií. Pro administrátora je potom jednoduché udělat si přehled o závažnosti jednotlivých událostí.

Vylepšený Event Management

Součástí systému jsou i automatické akce, které lze využít pro stanovení priority při správě zabezpečení. Například je možné využít ePolicy Orchetrator na prosazování nápravných bezpečnostních opatření, jako je distribuce konfigurací, zavádění nových politik či nasazení aktualizace softwaru. McAfee Enterprise Security Manager rovněž poskytuje integrované nástroje pro konfiguraci a řízení změn, case management a centralizované řízení politik. Tedy vše potřebné ke zlepšení pracovních postupů a usnadnění každodenních operací spojených s bezpečností IT.

Klíčové vlastnosti - ETM

- **Jednotný a komplexní pohled na bezpečnost sítě.**
- **Reakce na vývoj hrozeb** – možnost integrace s McAfee Global Threat Inteligence dokáže řešení reagovat na neustále se vyvíjející hrozby.
- **Korelace síťových a bezpečnostních událostí s reálnými business procesy a politikami.**
- **Jednoduché nastavení prahových hodnot pro generování výstrah vedoucích ke snižování rizik.**
- **Snížení náročnosti auditů** – integrace aktivit pro audity a dosažení shody se standardy díky vestavěné možnosti průběžné kontroly a pravidelného reportingu.
- **Integrace s ePolicy Orchestrator** – rozšiřuje přehled a kontrolu nad správou celého Vašeho IT.
- **Leader v Gartner Magic Quadrant**

Gartner

McAfee Enterprise Log Manager (ELM)

Hlavní funkcí tohoto řešení je zajištění integrity a compliance log záznamů. Všechny záznamy, které zařízení uchová, jsou označeny, taky aby nemohlo dojít k manipulaci s nimi a byl k nim zajištěn okamžitý přístup. Hlavní výhodou celého řešení je, že jsou podporovány prakticky všechny formáty log záznamů a to Microsoft Windows event logs, database logs, application logs a syslogs.

Inteligentní Log Management

Jednotlivé záznamy jsou ukládány dle jejich významu. To znamená, že jsou ukládány logy prokazující shodu se standardy, pro analýzy či pro bezpečnost. Velkou výhodou je, že veškeré log záznamy je možno uchovávat v jejich původní podobě a po libovolně dlouhou dobu, například pro naplnění shody s firemní politikou. Délku uchování informací je možno stanovit v závislosti na zdrojovém protokolu či firemní politice. McAfee Enterprise Log Manager používá snadno přizpůsobitelných úložišť, tak aby zajistily, že vaše záznamy jsou uloženy na správném místě a na správné časové období.

Klíčové vlastnosti - ELM

- **Splnění standardů o uchovávání log záznamů, compliance a integrity.**
- **Pravidla pro ukládání a uchovávání záznamů** definovatelná separátně na každý zdroj logů.
- **Přístup k originálním log záznamům na jedno kliknutí.**

COMGUARD security & networking

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

Integrace s McAfee Enterprise Security Manager

Zatímco Enterprise Log Manager uchovává log záznamy v surové podobě, Enterprise Security Manager může tyto záznamy normalizovat, klasifikovat a hloubkově analyzovat. Výsledné informace jsou potom k dispozici v reálném čase pro bezpečnostní analýzy. Jednotlivé bezpečnostní události jsou navázány na konkrétní log záznamy, které jsou zpřístupněny na jedno kliknutí.

McAfee Event Receiver (ERC)

Je nezbytnou součástí SIEM řešení, jelikož zajišťuje sběr logů, jejich normalizaci, klasifikaci a případné korelace. Zpracované záznamy dále předává do **McAfee Enterprise Security Manager případně McAfee Log Manageru** pro jejich vlastní zpracování. Díky takto zvolené architektuře řešení není sebemenší problém pokrýt i ty nejrozsáhlejší sítě.

Rozšiřující moduly pro McAfee Enterprise Security Manager

McAfee Advanced Correlation Engine sleduje data v reálném čase a umožňuje odhalit rizika a hrozby dříve, než k nim dojde. Advanced Correlation Engine je možno nasadit ve dvou režimech, a to v real-time nebo v historickém módu. Engine identifikuje uživatele, skupiny, aplikace, konkrétní servery a podsítě. Upozorní Vás, pokud by došlo k jejich ohrožení. Napomáhá s identifikací a ohodnocením bezpečnostních událostí v reálném čase, a to s pohledu firemních pravidel a rizik.

McAfee Application Data Monitor analyzuje sedmou vrstvu síťového modelu a poskytuje tak kompletní přehled o využívaných aplikacích, například je možno zjistit jejich obsah včetně textů a příloh. Tento detailní pohled poskytuje administrátorům přesnou představu o využívání aplikací a jejich neblahém dopadu na provoz sítě.

Modul dovoluje zamezit vynášení citlivých dat ze společnosti pomocí emailů, přenosu souborů přes protokol http nebo s využitím dalších aplikací. Napomáhá tak zmírnit ztráty spojené s únikem dat. Celé řešení funguje tak, že dokáže rozpoznat citlivá data, následně upozorní odpovídající osobu o prováděné transakci s daty. Veškeré sesbírané informace je potom možno využít při auditech a forenzních analýzách.

Další důležitou funkcí tohoto řešení je, že dokáže odhalovat hrozby cílené právě na aplikační vrstvu a uzavírá tak důležitou mezeru v bezpečnosti sítě.

McAfee Database Event Monitor je produkt, který sleduje veškeré úkony v databázi. Tyto údaje jsou následně ukládány do centrálního úložiště, které poskytuje funkce normalizace, korelace, analýzy a podávání zpráv o událostech v databázi. Jednotlivé události lze analyzovat v porovnání s ostatními informacemi, jako jsou uživatelská data, informace a interakce, činnost OS, zranitelnosti a dokonce i umístění v síti.

Model	Sběr a normalizace logů	Uchovávání logů v surové podobě	Zpracovávání událostí a reporting	Zpracovaných Event/log za sekundu - EPS	Vestavěná paměť
ESM5700-ELM,ERC	✓	✓	✓	3 500	32 TB + 800 GB SSD
ESM6050-ELM,ERC	✓	✓	✓	7 000	40 TB + 800 GB SSD
ESM5700			✓	65 000	32 TB + 800 GB SSD
ESM6050			✓	90 000	40 TB + 800 GB SSD
ETM X7			✓	200 000	16 TB SSD + 2 TB SSD (PCIe)
ETM X9			✓	300 000	19 TB SSD + 8 TB SSD (PCIe)
ETM X11			✓	400 000	19 TB SSD + 8 TB SSD (PCIe)
ERC-1270	✓			7 500	4 TB
ERC-2650	✓			14 000	12 TB
ERC-3500	✓			20 000	12 TB + 400GB SSD
ERC-4700	✓			30 000	5.6 TB SSD
ELM-4700		✓		55 000	5.6 TB SSD
ELM-5700		✓		75 000	32 TB + 800GB SSD
ELM-6050		✓		100 000	40 TB + 800GB SSD
ACE-2650			✓	<75,000	N/A
ACE-4700			✓	<225,000	N/A

Poznámka: Řešení ETM, ERC a ALL in ONE je možno pořídit v podobě Virtual appliance