Security Information & Event Management

AEC

Máte přehled co se ve vaší infrastruktuře děje?

Rozmanitost technologií v infrastruktuře narůstá, správců přibývá a nezřídka jsou některé prvky administrovány externí organizací. Tím se povědomí o bezpečnostní situaci „drobí“ a chybí komplexní pohled. Většina IT pracovníků se obvykle zabývá informacemi obsaženými v logu až po nahlášení nějakého nestandardního stavu. Události nejsou sledovány minutu po minutě, dvacet čtyři hodin denně, každý den v týdnu. A přitom v kterémkoli zařízení připojeném do infrastruktury se může ukrývat důležitá informace, která nám umožní rozšířit pohled na nežádoucí situaci.

Úlohou SIEM řešení je poskytnout z jednotlivých informací celkový obraz o bezpečnostní situaci v infrastruktuře.

www.aec.cz

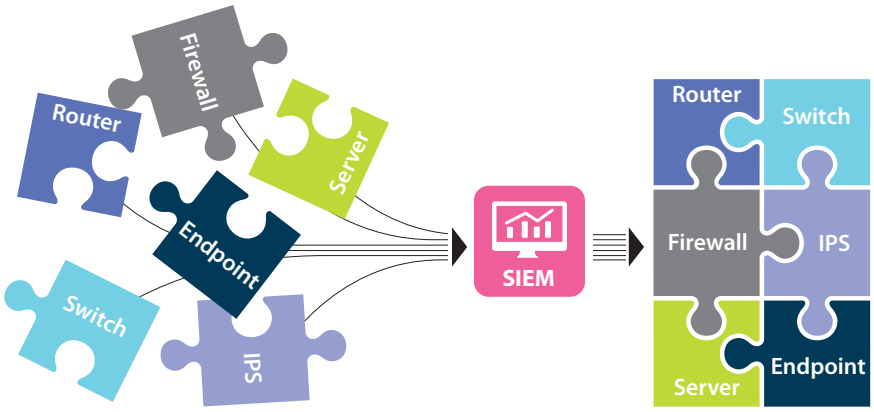
Security Information and Event Management je řešení konsolidující informace o bezpečnostních událostech a incidentech z mnoha různých zdrojů rozmístěných napříč celou infrastrukturou do jednoho centrálního místa. Pro potřeby detailní investigace nežádoucích situací, ukládá sbírané informace v nezměněné podobě jako záznamy (logy), chrání je proti neoprávněné modifikaci, a vytváří nad nimi logické vazby za účelem odlišit reálné hrozby od falešných poplachů. Bezpečnostním analytikům a operátorům tak poskytuje přístup k informacím o bezpečnostních událostech a incidentech v reálném čase, ale také zpětně pro potřeby hloubkové analýzy.

Klíčové přínosy SIEM řešení

- Shromažďovat, normalizovat, kategorizovat, ukládat události a jiné informace pro potřeby vyšetřování, hloubkové a forenzní analýzy a umožňuje tak dosažení souladu s regulativními požadavky.
- Analyzovat tyto informace zpracované v reálném čase, tedy včas odhalovat cílené útoky, pokročilé hrozby, narušení bezpečnosti infrastruktury a včas na ně reagovat.
- Reportovat odchylky od regulatorních nařízení a tím upozorňovat na vznikající nedostatky a vývoj bezpečnostní situace.

Security Information & Event Management

AEC



Jak probíhá implementace SIEM řešení od AEC

Analýza
Na samém počátku projektu je třeba provést detailní analýzu veškerých vazeb a specifik organizace, business modelu, používaných technologií a procesů. Analýza je nedílnou součástí nasazení řešení SIEM. Analytici vychází z analýzy rizik, která dokumentuje možná rizika a jejich dopady. Dále se zaměřují na modelování hrozeb a na analýzu na míru vytvořených aplikací a jejich možností poskytovat potřebné informace. Vyhodnocují, jaké legislativní požadavky jsou na zákazníka kladeny, a definují způsob zajištění kontroly souladu.

Výběr řešení
Na základě poznatků a požadavků shromážděných při analýze, navrhujeme vhodné řešení, které přesně odpovídá specifickým podmínkám konkrétní organizace, včetně detailní sumarizace výhod a nevýhod jednotlivých variant.

Implementace a konfigurace
Provedeme implementaci veškerých komponent SIEM řešení, integrujeme je se systémy v infrastruktuře zákazníka, pomůžeme s připojením zdrojů logů, jejich vyparsováním a kategorizací.

Optimalizace vyhodnocování
Zahrnuje optimalizaci sběru, vyhodnocování získaných dat a vytvoření vlastních/unikátních detekčních a korelačních pravidel, která reflektují analýzou rizik či modelováním hrozeb identifikované skutečnosti.

Pilotní provoz
V rámci pilotního provozu provádíme proškolení pracovníků, testujeme dodané řešení ve spolupráci se zákazníkem. Nabízíme rovněž prověření detekce formou penetračních testů simulujících reálný útok.

Předání řešení
Po ukončení pilotního provozu předáváme řešení do operativy, kterou řeší zákazník ve své režii nebo může využít možnosti poskytování profesionálního bezpečnostního dohledu formou služby. AEC v této oblasti nabízí služby oddělení AEC Cyber Defense Center, které zajišťuje monitoring, detekci a eskalaci bezpečnostních incidentů.

Technická podpora
Poskytujeme službu technické podpory na dodané řešení, ve které se rovněž věnujeme jeho dalším úpravám a rozvoji, případně proškolování nových pracovníků.

Certifikace

Naši bezpečnostní specialisté disponují těmito odbornými osvědčeními:

IBM Certified Associate Administrator
IBM Certified Deployment Professional
IBM Certified SOC Analyst
IBM Certified Associate Analyst
RSA Certified Analyst
RSA SE Professional
RSA SE Master
RSA Certified Administrator

Přínosy řešení

- Snížení reakční doby na incident (zvýšení efektivity), tedy zmírnění dopadu bezpečnostního incidentu (snížení nákladů na obnovu).
- Centralizace informací o bezpečnosti do jednoho bodu.
- Přehled o aktuální bezpečnostní situaci chráněné infrastruktury.
- Minimalizace možnosti pochybení operátorů (automatizace bezpečnosti) a to díky předem definovaným postupům řešení bezpečnostních incidentů.
- Pokrytí komplexního portfolia bezpečnostních hrozeb (prostřednictvím integrace více zdrojů a vytvořením korelací).
- Reflektování známých i zero-day hrozeb.

Proč AEC

- Disponujeme zkušenými a certifikovanými specialisty v oblasti SIEM řešení, ale i v dalších oblastech informační bezpečnosti.
- Máme zkušenosti z desítek úspěšných implementací SIEM řešení.
- Spolupracujeme s lídry v oblasti SIEM řešení. Neomezujeme se na konkrétního výrobce řešení, hledáme to nejvhodnější řešení pro konkrétní případ.
- Neinstalujeme servery a aplikace, vytváříme řešení, která zákazníkům reálně pomáhají.
- V našich implementacích reflektujeme legislativní požadavky, jako například ZoKB, ISO, PCI DSS, a další.
- Nasazením řešení naše práce nekončí, dále jej udržujeme a rozvíjíme.

Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283