Security Information & Event Management

AEC

Máte prehľad, čo sa vo vašej infraštruktúre deje?

Rozmanitosť technológií v infraštruktúre narastá, správcov pribúda a nezriedka sú niektoré prvky administrované externou organizáciou. Tým sa povedomie o bezpečnostnej situácii „drobí“ a chýba komplexný pohľad. Väčšina IT pracovníkov sa obvykle zaoberá informáciami uvedenými v logu až po nahlásení nejakého neštandardného stavu. Udalosti nie sú sledované minútu po minúte, dvadsaťštyri hodín denne, každý deň v týždni. A pritom v ktoromkoľvek zariadení pripojenom do infraštruktúry sa môže ukrývať dôležitá informácia, ktorá nám umožní rozšíriť pohľad na nežiaducu situáciu.

Úlohou SIEM riešení je poskytnúť z jednotlivých informácií celkový obraz o bezpečnostnej situácii v infraštruktúre.

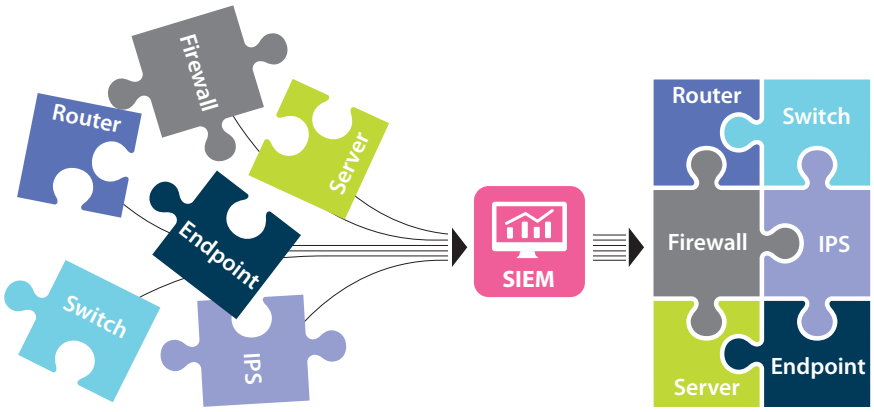
www.aec.sk

Security Information and Event Management je riešenie konsolidujúce informácie o bezpečnostných udalostiach a incidentoch z mnohých rôznych zdrojov rozmiestnených po celej infraštruktúre do jedného centrálneho miesta. Pre potreby detailnej investigácie nežiaducich situácií ukladá zbierané informácie v nezmenenej podobe ako záznamy (logy), chráni ich proti neoprávnenej modifikácii a vytvára nad nimi logické väzby s cieľom odlíšiť reálne hrozby od falošných poplachov. Bezpečnostným analytikom a operátorom tak poskytuje prístup k informáciám o bezpečnostných udalostiach a incidentoch v reálnom čase, ale tiež spätne pre potreby hĺbkovej analýzy.

Klíčové přínosy SIEM řešení

- Zhromažďovať, normalizovať, kategorizovať, ukladať udalosti a iné informácie pre potreby vyšetrovania, hĺbkovej a forenznej analýzy, a umožňuje tak dosiahnutie súladu s regulatívnymi požiadavkami.
- Analyzovať tieto informácie spracované v reálnom čase, teda včas odhaľovať cielené útoky, pokročilé hrozby, narušenie bezpečnosti infraštruktúry a včas na ne reagovať.
- Reportovať odchýlky od regulatórnych nariadení a tým upozorňovať na vznikajúce nedostatky a vývoj bezpečnostnej situácie.

Security Information & Event Management



Ako prebieha implementácia SIEM riešení od AEC

Analýza
Na samom začiatku projektu je potrebné urobiť detailnú analýzu všetkých väzieb a špecifík organizácie, business modelu, používaných technológií a procesov. Analýza je neoddeliteľnou súčasťou nasadenia riešení SIEM. Analytici vychádzajú z analýzy rizík, ktorá dokumentuje možné riziká a ich dopady. Ďalej sa zameriavajú na modelovanie hrozieb a na analýzu na mieru vytvorených aplikácií a ich možností poskytovať potrebné informácie. Vyhodnocujú, aké legislatívne požiadavky sú na zákazníka kladené, a definujú spôsob zaistenia kontroly súladu.

Výber riešení
Na základe poznatkov a požiadaviek zhromaždených pri analýze navrhujeme vhodné riešenie, ktoré presne zodpovedá špecifickým podmienkam konkrétnej organizácie vrátane detailnej sumarizácie výhod a nevýhod jednotlivých variantov.

Implementácia a konfigurácia
Urobíme implementáciu všetkých komponentov SIEM riešení, integrujeme ich so systémami v infraštruktúre zákazníka, pomôžeme s pripojením zdrojov logov, ich vyparsovaním a kategorizáciou.

Optimalizácia vyhodnocovania
Zahŕňa optimalizáciu zberu, vyhodnocovanie získaných dát a vytvorenie vlastných/unikátnych detekčných a korelačných pravidiel, ktoré reflektujú analýzou rizík či modelovaním hrozieb identifikované skutočnosti.

Pilotná prevádzka
V rámci pilotnej prevádzky robíme preškolenie pracovníkov, testujeme dodané riešenie v spolupráci so zákazníkom. Ponúkame takisto preverenie detekcie formou penetračných testov simulujúcich reálny útok.

Odovzdanie riešenia
Po ukončení pilotnej prevádzky odovzdávame riešenie do operatívy, ktorú rieši zákazník vo svojej réžii alebo môže využiť možnosti poskytovania profesionálneho bezpečnostného dohľadu formou služby. AEC v tejto oblasti ponúka služby oddelenia AEC Cyber Defense Center, ktoré zaisťuje monitoring, detekciu a eskaláciu bezpečnostných incidentov.

Technická podpora
Poskytujeme službu technickej podpory na dodané riešenie, v ktorej sa takisto venujeme jeho ďalším úpravám a rozvoju, prípadne preškoľovanie nových pracovníkov.

Certifikácia

Naši bezpečnostní špecialisti disponujú týmito odbornými osvedčeniami:

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

Prínosy riešenia

- Zníženie reakčného času na incident (zvýšenie efektivity), teda zmiernenie dopadu bezpečnostného incidentu (zníženie nákladov na obnovu).
- Centralizácia informácií o bezpečnosti do jedného bodu.
- Prehľad o aktuálnej bezpečnostnej situácii chránenej infraštruktúry.
- Minimalizácia možnosti pochybenia operátorov (automatizácia bezpečnosti), a to vďaka vopred definovaným postupom riešenia bezpečnostných incidentov.
- Pokrytie komplexného portfólia bezpečnostných hrozieb (prostredníctvom integrácie viacerých zdrojov a vytvorením korelácií). Reflektovanie známych aj zero-day hrozieb.

Prečo AEC

- Disponujeme skúsenými a certifikovanými špecialistami v oblasti SIEM riešení, ale aj v ďalších oblastiach informačnej bezpečnosti.
- Máme skúsenosti z desiatok úspešných implementácií SIEM riešení.
- Spolupracujeme s lídrami v oblasti SIEM riešení. Neobmedzujeme sa na konkrétneho výrobcu riešení, hľadáme to najvhodnejšie riešenie pre konkrétny prípad.
- Neinštalujeme servery a aplikácie, vytvárame riešenia, ktoré zákazníkom reálne pomáhajú.
- V našich implementáciách reflektujeme legislatívne požiadavky, ako napríklad ZoKB, ISO, PCI DSS a ďalšie.
- Nasadením riešenia sa naša práca nekončí, ďalej ho udržujeme a rozvíjame.

Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283
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