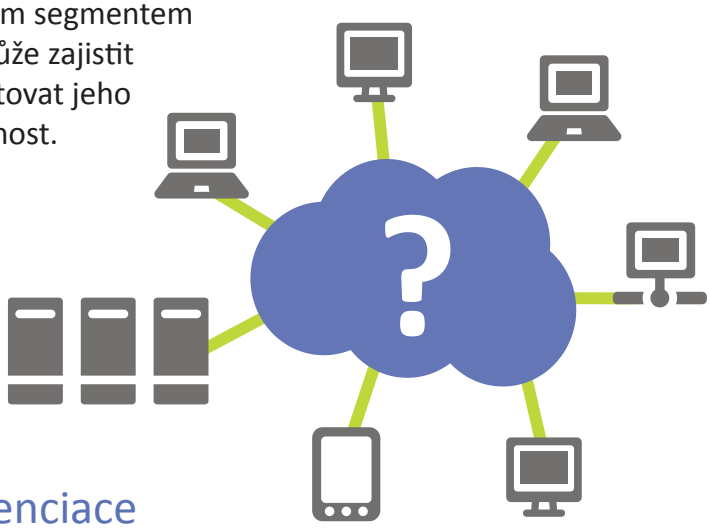
Security Information and Event Management

SIEM řešení je auditní a monitorovací nástroj pro zajištění a garanci úrovně bezpečnosti provozovaného segmentu IT.

Tento nástroj zajišťuje logické oddělení bezpečnosti a provozu IT. SIEM řešení monitorují definované události na zařízení a jsou schopny interpretovat potenciální i reálné bezpečnostní incidenty a také aktivitu administrátorů a uživatelů. Vyhodnocení těchto událostí je automatické dle definovaných parametrů.

Nástroje monitoringu se stávají nepostradatelnou součástí světa IT, protože ten, kdo nevyužívá automatickou formu vyhodnocení událostí nad svěřeným segmentem IT, nemůže zajistit a garantovat jeho bezpečnost.



Diferenciace

Analýza nasazení SIEM řešení

Analýza stávajících potřeb na bezpečnostní monitoring, detailní návrh vhodného řešení v souladu s nároky na infrastrukturu.

Implementace zvoleného SIEM řešení

Implementace analýzou zvoleného řešení, dle detailních návrhů.

Support/rozvoj SIEM řešení

Support/rozvoj SIEM řešení v úrovni pokročilé integrace zařízení a maximální možné využití jeho vlastností, dále kontakt s výrobcem, řešení nestandardních událostí, případně celková podpora zajištění funkce SIEM řešení včetně vyhodnocení událostí.

Pronájem SIEM řešení (jako služby)

Muže obsahovat jak implementaci, tak support/rozvoj dle parametrů smlouvy o pronájmu.

Přínosy, výsledky

- Výrazné snížení rizikovosti aplikací (možnost kompromitace).
- Detailní přehled provozu nad sledovanými aplikacemi.
- Real time přehled nad událostmi z mnoha zařízení.
- Možnost forensní analýzy nad událostmi z mnoha typů zařízení.
- Automatické korelace a následné interakce

Reference

Česká pošta, Konsolidace nastavení SIEM systému

Cílem bylo konsolidovat nastavení a zároveň využití již implementovaného SIEM systému; naplánovat další rozvoj této technologie a zároveň upravit postupy a požadavky pro identifikaci incidentu a další nakládání s bezpečnostním incidentem.

Při konsolidaci nastavení došlo k úpravám konfigurace alertů a reportů; byl vytvořen dokument obsahující aktuální stav technologie a doporučený rozvoj této technologie. Dále došlo k definici/úpravám některých pracovních postupů pro zlepšení efektivity práce s bezpečnostními incidenty.

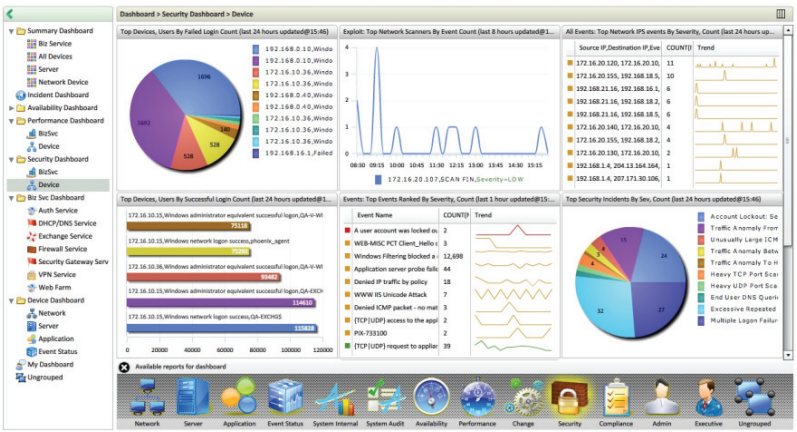
Metodika, nástroje, technologie

Přístup k analýze či nasazení SIEM řešení vychází z best practices uváděných výrobci jednotlivých SIEM řešení.

Case study

Implementované řešení se nacházelo ve stavu základní konfigurace, zařízení neanalyzovalo výstupy z core systémů, výstupy byly velice omezené, zařízení nebylo využito v procesu incident managementu. (Chyba nastala v době po implementaci, kdy byl naprosto zanedbán jakýkoliv vývoj integrace řešení, tím pádem nebylo možné dále definovat a upravovat úroveň monitorování bezpečnosti, kvalitu výstupů a zapracování dalších provozních podnětů). Zařízení zcela zjednodušeně neplnilo svou primární funkci.

Větší a střední organizace, které zatím nevlastní žádné řešení SIEM systémů, zpravidla provádějí částečnou analýzu událostí za pomoci skriptů, tyto skripty často automaticky upozorňují na identifikaci bezpečnostního incidentu, a jsou tedy zapojeny do procesu incident managementu. Nevýhodou těchto skriptů bývá omezení jen na určité typy zařízení (zpravidla Linux/Unix) a to, že neumožňují další konsolidované výstupy incidentů (formou tabulek či grafů). Výstupy těchto skriptů rovněž nejsou dále interpretovány a vyhodnocovány napříč organizací.



Hlavní nevýhodou je omezená funkce z pohledu definice analyzovaných událostí a omezená funkce z pohledů výstupů. V podstatě je zde absence nezávislé kontroly administrátorů vzhledem k bezpečnosti a nemožnosti analyzovat vývoj bezpečnostních incidentů za časový úsek.

Proč AEC?

Členové našeho týmu mají mnohaleté zkušenosti s analýzami, integrací a rozvojem SIEM technologií. Nejsme závislí na výrobci SIEM řešení.

Postupujeme dle prověřených postupů, tak aby byla zajištěna maximální efektivita a minimalizace rizika při integraci či provozu SIEM nástroje.

Certifikace

2x RSA System Engeneer

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY

www.aec.cz