Monitorovanie a manažment bezpečnostných incidentov

eTrust Security Command Center
Významným faktorom efektívneho bezpečnostného systému je jeho schopnosť poskytnúť informácie o aktuálnom stave bezpečnostných opatrení, implementovaných na ochranu aktív. Centralizovaná prezentácia zabezpečenia a stavu služieb v rámci informačného systému predstavuje predpoklad rýchlej identifikácie a reakcie na vzniknuté udalosti, alebo ohrozenia. Možnosť spätnej analýzy, korelácií a reportingu dáva možnosť spätných šetrení a poskytuje ucelený pohľad na informačný systém.

Popis riešenia
SCC (Security Command Center) je centrálny monitorovací nástroj renomovanej spoločnosti Computer Associates, ktorá dlhodobo patrí ku svetovým lídrom v oblasti softvérového riešenia bezpečnosti informačných systémov. Riešenie SCC využívajú bankové inštitúcie, štátne úrady a organizácie, ako aj iné rôzne nadnárodné spoločnosti na celom svete.

SCC umožňuje centrálne sledovanie množstva informácií o vzniknutých udalostiach v rámci informačného systému a zabezpečuje ich komplexné a dôkladné vyhodnotenie.
SCC reprezentuje nástroj centrálneho manažmentu bezpečnosti s jadrom, podporujúcim uchovávanie zvolených typov zaznamenávaných udalostí a ich analytickým vyhodnotením, poskytujúcim podporu pri návrhu opatrení na eliminovanie bezpečnostných rizík.

Prínos riešenia
SCC predstavuje centrálny modulárny systém zberu udalostí naprieč rôznymi platformami operačných systémov, zariadení a aplikácií. Centrálnym zberom s prístupom na základe rolí užívateľov sa napĺňa základný predpoklad bezpečnosti - oddelenie funkcií správcu systému od správy bezpečnosti. SCC poskytuje priorizáciu udalostí, ich vizualizáciu, reprezentovanie stavov, generovanie alertov a reportov. Eliminuje možnosť modifikácie zaznamenaných udalostí a poskytuje nástroj na vyšetrenie a vyvodenie dôsledkov v prípade pokusov, či reálnych neoprávnených aktivít v rámci informačného systému.

SCC, ako nástroj Centrálneho monitorovania bezpečnosti (CMB) je súborom úloh, zabezpečujúcich:

- Minimalizovanie pravdepodobnosti vzniku bezpečnostných incidentov
- Ich včasnú identifikáciu
- Realizáciu adekvátnych protiopatrení po ich odhalení
- Vedenie záznamu o incidentoch
- Analýzu priebehu bezpečnostných incidentov

Použitie produktu
Produkt SCC je silným a modulárnym riešením najmä pre veľké a stredné firmy, ktoré majú heterogénne prostredie s množstvom zariadení, pričom udalosti z týchto systémov sú roztrúsené jednotlivo v rámci informačného systému bez možnosti centrálneho náhľadu, alebo ich komplexnej analýzy.

EMM®
EMM, spol. s r.o., Sekurisova 16, 841 02, Bratislava 42, Slovensko
tel: +421 (2) 60 254 111, fax: +421 (2) 60 254 901
www.emm.sk

BEZPEČNOSŤ IS

Produkt SCC je však určený každému, kto vyžaduje:

- Prevenciu vzniku bezpečnostných incidentov (BI)
- Identifikáciu a eliminovanie BI
- Včasnú reakciu na BI
- Dokumentovanie a štatistiky BI
- Analýzu priebehu BI
- Splnenie legislatívnych požiadaviek

EMM®

EMM, spol. s r.o., Sekurisova 16, 841 02, Bratislava 42, Slovensko
tel: +421 (2) 60 254 111, fax: +421 (2) 60 254 901
www.emm.sk