Cerinţele funcţionale faţa de SIEM

Monitorizarea și audit al evenimentelor de securitate informațională – SIEM (Security Information Event Management)

SIEM funcționează pentru a atinge următoarele obiective de securitate:

- Reducerea abuzului de drepturi de acces și a riscurilor de acces neautorizat.
- Limitarea partajării parolelor între utilizatori.
- Identificarea amenințărilor și posibilelor încălcări;
- Colectarea jurnalelor de audit pentru securitate și conformitate;
- Efectuarea investigațiilor

Sistemul de monitorizare și audit trebuie să asigure următoarele capabilități de securitate:

- Agregarea datelor: administrarea log-urilor din mai multe surse, inclusiv Active Directory, sisteme de securitate, servere, baze de date, aplicații, oferind posibilitatea de a consolida și monitoriza evenimentele
- Corelarea datelor: căutarea atributelor comune și conexiunea evenimentelor. Această tehnologie oferă posibilitatea de a efectua o varietate de tehnici de corelare pentru a integra diferite surse, pentru a transforma datele în informații utile.
- Alertarea: analiza automată a evenimentelor corelate și producerea alertelor, pentru a informa administratorii despre problemele identificate.

Evenimentele transmise către SIEM pentru identificarea incidentelor:

- încercări de autentificare cu succes și nereușite
- adăugarea, ștergerea și modificarea conturilor și a grupurilor
- utilizarea privilegiilor
- pornirea și oprirea serviciilor
- modificări importante ale configurației și a setărilor de securitate
- Evenimente de securitate de la routere, firewall, IPS, WEB Proxy, WAF, VPN Gate

Sisteme care trebuie integrate în SIEM:

- AD (Microsoft Active Directory)
- Print Server
- File Server
- Email Server
- WSUS,
- SCCM,
- NPS,
- Switches Cisco
- Sisteme de operare: Linux, Microsoft Windows
- Web servers
- Aplicații
- Databases (Baze de date)

- Sisteme de securitate: VPN Gate, Tacacs+, Firewall, Sistemul de prevenire a intruziunilor IPS, Firewall pentru aplicații web WAF, Application Control, Antivirus

Vendori posibili de SIEM: IBM Qradar, Splunk, McAfee

- **Prezenţa interfeței de administrare, analizarea informațiilor comune cu alte sisteme EndPoint Protection, SIEM, DLP reprezintă un avantaj important în comparație cu alte soluții.**
- **Disponibilitatea și poziția produsului în "Gartner Square" reprezintă un avantaj puternic față de alte soluții.**