siem_strategy

SIEM Estrategia eta Inplementazioa - Zabala Gailetak

1. Helburua

Zabala Gailetak-eko azpiegituran gertatzen diren segurtasun gertaerak zentralizatu, korrelatu eta aztertzea, mehatxuak denbora errealean detektatzeko.

2. Aukeratutako Soluzioa

- **Softwarea:** Wazuh / ELK Stack (Elasticsearch, Logstash, Kibana) edo AlienVault OSSIM.
- **Arrazoia:** Kostu-eraginkorra, open source, eta funtzionalitate zabalak (EDR, log analisia).

3. Arkitektura

- **Zentrala:** SIEM Zerbitzaria (DMZ-n edo kudeaketa sarean babestuta).
- **Agenteak:** Zerbitzari kritikoetan (Web, Datu-baseak, AD) eta OT sareko pasabideetan (Gateway).

4. Log Iturriak

1. **Firewallak:** Sarrera/Irteera trafikoa, blokeatutako konexioak.
2. **Zerbitzariak (Windows/Linux):** Autentikazioak (arrakastatsuak/huts egindakoak), pribilegio igoerak.
3. **Web Zerbitzaria (Apache/Nginx):** Access logs (SQLi saiakerak, XSS), Error logs.
4. **OT Sareko Gailuak:** PLC logs (posible bada), HMI sarrerak.

5. Alerta Arauak (Adibideak)

- **Brute Force:** 5 huts egindako login saiakera minutu batean IP beretik.
- **Scan Detekzioa:** Portu eskaneatzea firewall-ean blokeatuta.
- **Malware:** Wazuh FIM (File Integrity Monitoring) aldaketa susmagarriak sistema fitxategietan.
- **Pribilegioak:** Admin taldean erabiltzaile berri bat gehitzea.

6. Erantzuna

- Alertak posta elektronikoz bidaliko dira IT taldeari.
- Larritasun altuko alertak berehalako esku-hartzea eskatzen dute SOP-aren arabera.