Diseño Completo de un SOC Open Source

#SOC #OpenSource #Ciberseguridad #SIEM #SOAR

Este documento describe un diseño completo para un SOC (Security Operations Center) basado íntegramente en herramientas de código abierto. Está destinado a organizaciones pequeñas o medianas que buscan una solución eficaz, escalable y sin costos de licenciamiento. Incluye la estructura de red, equipos de trabajo por niveles y herramientas necesarias.

1. Estructura de Red

1. Internet

2. Firewall Perimetral

3. Red DMZ (Honeypots: Honeyd, Cowrie)

4. Red Interna Monitoreada

5. Servidor Central del SOC con:

   - SIEM (ELK Stack, Wazuh)

   - IDS/HIDS (Suricata, OSSEC)

   - Gestión de Logs (Graylog)

   - SOAR (Shuffle)

   - Gestión de Incidentes (TheHive, Cortex)

   - Visualización (Kibana, Grafana)

2. Equipos de Trabajo del SOC

Nivel 1: Analistas de Monitoreo

- Monitoreo en tiempo real

- Filtrado de alertas

- Escalamiento de incidentes

Nivel 2: Analistas de Incidentes

- Investigación de amenazas

- Análisis forense

- Respuesta a incidentes

Nivel 3: Ingenieros de Seguridad / Threat Hunters

- Threat hunting

- Desarrollo de reglas

- Investigación avanzada

3. Herramientas Open Source por Nivel

Nivel 1:

- Wazuh, ELK Stack, Suricata, OSSEC

- Graylog, Shuffle

Nivel 2:

- TheHive, Cortex, Volatility, Autopsy, Cuckoo Sandbox

Nivel 3:

- MISP, YARA, Arkime, Wireshark, OpenEDR

4. Dashboards, Honeypots y Automatización

- Dashboards: Kibana, Grafana

- Honeypots: Cowrie, Honeyd

- Automatización: Shuffle, Ansible

- Simulación: Atomic Red Team, MITRE Caldera