[NEG] Security Operations Center

Las principales funciones de un SOC son las siguientes:

- Monitorización y gestión de todos los activos de la empresa en tiempo real
- Securización y fortificación de activos
- Respuesta ante amenazas proactiva y reactiva
- Toma de decisiones frente a incidentes
- Recuperación y mantenimiento del negocio
- Evaluación del riesgo y cumplimiento normativo.
- Evaluación del riesgo y cumplimiento normativo
- Reporting y procesos de mejora.

Para poder implementar un SOC es necesaria la transferencia de conocimiento, estrategia, procesos y políticas de la organización, conocimiento de los sistemas y dispositivos y una cadena de mando y comunicación. El problema es que es muy costoso. Un SOC puede ser implementado de varias maneras:

- On-Premise
- Hybrid
- Outsourcing

Fases de la implementación de un SOC On-Premise

1. Tecnología: Pernsal encargado de analizar la organización para ver que herramientras son necesarias para poder obtener datos apra el SOC
2. Securización: Securizar los equipos y documentarlos.
3. Políticas: Revisar políticas de seguridda de la empresa. Se recomienda basarlas en la ISO 27002.
4. Operación: Monitorización y testeo de equipos, respuesta a incidentes…. Permite conocer el funcionamiento de la organización y aplicar los cambios previstos en la política de seguridad
5. Inteligencia: Uso de herramientras de inteligencia que pueden anticipar problemas proactivamente.

Inputs de un SOC

- Eventos: Observaciones registrables. Puede generarse un log u otra fuente de entradas con eventos
  - Muchos eventos pueden ser configurados para emitir una alerta. Esto se hace para eventos de interés que deben ser vigilados y pueden requerir intervención. Se suelen configurar en la herramienta SIEM
  - Las alertas generan incidentes que deben ser registrados a través de herramientas de ticketing o Service Desk.
- Prolemas: Uno o más incidentes que no tienen una causa raíz identificada.
  - La gestión de problemas se ocupa de investigar y solucionar la casa raíz de los incidentes y encontrar soluciones permanentes y así intervenirlos en el futuro.

Infraestructura de un SOC

- Infraestructura de seguridad en la organización: Dispositivos que permiten mantener confidencialidad, disponibilidad e integridad.
  - NAC: Network Access Control
  - DLP: Data Loss Prevention
  - IDS: Intrusion Detection System
- Infraestructura de seguridad en el SOC: Dispositivos y herramientas para revisar y analizar la información recibida en el SOC.
  - SIEM: Sistemas de gestión de eventos de seguridad (Security Information and Evento Management)
  - Ticketing: Sistemas de gestión de incidencias
  - Herramientas de ayuda instaladas en equipos específicos (Honeypots)

Las principales fuentes de datos suelen ser los logs y el SIEM

- Logs: Permiten realizar un triage y diagnóstico de amenazas y anomalías como errores de hardware, servicios anómalos, fallos de autenticación, registro de tareas de administración... Los aspectos importantes del log son los siguientes:
  - Monitorizar el log para garantizar su correcto funcionamiento
  - Revisar el almacenamiento y rendimiento
  - Sincronización con NTP para el registro cronológico.
  - Proteger la información que no debe aparecer en un log (contraseñas, información personal...)
  - La información debe clasificarse en niveles de severidad para su filtrado.
  - Los logs se pueden utilizar para detectar fraudes, realizar análisis forense y para auditorías
- SIEM: Puede llevar a cabo tareas y detecciones más complejas derivadas de los procesos de correlación e inteligencia.