[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: