Introducción a los SIEM

- **SIM (Security Information Management)**: Sistema de gestión de recursos que incorpora toda la información recolectando y almacenando los logs
- **SLM/SEM(Security Log/Event management)**: Monitorización en tiempo real, notificaciones y dashboards
    - **SEC (Security Event Correlation)**: Busca patrones en los registros de seguridad de forma que detecten eventos de que de otra forma serían eventos independientes.
- **SIEM (Security Information and Event Management)**: Unifica todo lo anterior bajo una sola herramienta.

Un siem nos permite buscar la información entre la inmensa cantidad de logs que tenemos. Para ello se usan reglas, expresiones regulares y machine learning. También dispone de un sistema de alertas y notificaciones. De por si, los SIEM por definición son pasivos, no responden a ataques, aunque muchas veces tienen añadidos que permiten que también respondan a incidentes.