

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.

From:

<http://www.knoppia.net/> - Knoppia



Permanent link:

http://www.knoppia.net/doku.php?id=master_cs:gsi:siem&rev=1763994359

Last update: **2025/11/24 14:25**