Instituto Tecnológico de Cancún

Ingeniería en sistemas computacionales

Fundamentos de telecomunicación

“SIEM”

Docente:

Ing. Ismael Jiménez Sánchez

Alumna:

Moen Ake Geraldy María

SIEM o Gestión de Eventos e Información de Seguridad (*Security Information and Event Management*, por sus siglas en inglés) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas.

Un software SIEM realiza un análisis centralizado de datos de seguridad, obtenidos desde múltiples plataformas, que incluyen aplicaciones como los antivirus, firewalls, y soluciones para la detección y prevención de intrusiones (IDS/IPS), entre otros.

El principio de un sistema SIEM es que los datos relevantes sobre la seguridad de una entidad se producen en múltiples ubicaciones, y al ser capaz de gestionar toda la información desde un único punto de vista, es más fácil detectar tendencias y ver patrones fuera de lo común.