SIEM

Security Information and Event Management

3 DÍAS

Objetivos

Durante el curso se analizarán los diferentes aspectos del SIEM y las razones por las que nos permiten detectar ataques e intrusiones de una forma más rápida.

En la parte práctica, se trabajará con los componentes Open Source de OSSIM y se utilizará la consola de incidencias de AlientVault OSSIM para analizar ataques, información de correlación y generar informes que nos permitan auditar el estado de la seguridad y el cumplimiento con las normativas como DDS-PCI y RGPD de nuestra organización.

Para quién

Este curso está orientado a los ingenieros de sistemas, programación o equipos con una metodología Agile que quieran integrar sus sistemas con un SIEM

1. CONCEPTOS SIEM

Necesidad de los SIEM
Análisis de datos
Representación
Que es un SIEM
Tareas: Gestión de registro, eventos y correlación
Respuesta activa
Cumplimiento de normativas

2. RGPD

Como afecta a las compañías
Legislación, plazos y requerimientos
Análisis de riesgo

Modelos
Implantación
Proceso continuo y el DPO

3. MODELOS DE SEGURIDAD

Confidencialidad, integridad y disponibilidad
Clasificación de entornos y modelos

4. APT - ADVANCED PERSISTENT THREATS

Reconocimiento
Militarización
Entrega
Instalación
Command and Control

5. COMPONENTES

Descubrimiento de activos y recursos en la red
IDS
HIDS
Netflow/Sflow
DPI
Sistemas de análisis de vulnerabilidades

6. PANORAMA DEL MERCADO DE SIEM

AlienVault
QRadar
Logrhythm
TAP
FortiSIEM

7. HERRAMIENTAS OPEN SOURCE

NMAP
PRADS
OSSEC
Suricata
OpenVAS

8. ALIEN VAULT

Introducción: OSSIM, USM Appliance y USM Anywhere
Instalación: Cloud vs On premise
Gestión de activos y Políticas
Análisis de seguridad
Creación de reglas
Correlación de eventos
Creación de plugins
Conformidad de seguridad
Informes y Auditorías
Adaptaciones a la RGPD

Obten un 15% de descuento al introducir el código **cabalier18**

Cabalier
Intelligent Software