SIEM: Security Information and Event Management

19, 20 y 21 de Marzo 2018 (9:00 - 15:00 h.)

Conceptos SIEM
- Que es un SIEM. Necesidad
- Datos: Análisis, Representación
- Registro, Eventos, Correlación
- Cumplimiento de Normativas

SIEM y GDPR/RGPD
- Cómo afecta a las compañías
- Legislación, Requerimientos
- Análisis de Riesgo
- Modelos e Implantación, DPO

Modelos de Seguridad
- Confidencialidad, Integridad y Disponibilidad
- Entornos y Modelos

APT –Persistent Threats
- Reconocimiento y Militarización
- Entrega e Instalación
- Comando y Control

Componentes
- Descubrimiento de activos y recursos en la red
- IDS, HIDS, Netflow/Sflow, DPI
- Análisis de Vulnerabilidades

Mercado de SIEM
- AlienVault, Qradar, Logrhythm, TAP, FortiSIEM

Herramientas Open Source
- NMAP, PRADS, OSSEC
- Suricata, OpenVAS

Alien Vault
- Introducción: OSSIM,
- USM Appliance y USM Anywhere
- 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

Prácticas con herramientas freeware

"Cumplimiento de las normativas europeas de Seguridad RGPD"

Con la aparición de la nueva normativa Europea de protección de datos GDPR (RGPD o Reglamento General de Protección de Datos), han aparecido una serie nuevas necesidades y requerimientos que las empresas han de cumplir.

La necesidad de mantener una política de seguridad de datos y privacidad requiere de herramientas avanzadas que agreguen la información que se encuentra distribuida entre los diversos sistemas de información.

La RGPD también requiere que los incidentes de seguridad sean reportados en un periodo de 72 horas, cuando el tiempo actual para la detección de una intrusión está en 65 días.
Con normativas como la RGPD, PCI DSS o la misma ISO-27001, los SIEM son herramientas indispensables para la gestión y auditoría, pero también son cada vez más necesarios para tratar y correlar la gran cantidad de información de seguridad que generan los dispositivos y aplicaciones.

Análisis, tratamiento y respuesta en tiempo real de alertas de Seguridad.

El uso de herramientas freeware como SIEM OSSIM AlienVault no solo nos permite tener una mayor visibilidad de la seguridad de la red, sino que podemos realizar las auditorías en las áreas clave de la evaluación de las vulnerabilidades, inspección de paquetes, correlación de los eventos de seguridad y con más herramientas de código abierto.

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.