Temario del curso: *Protección perimetral y detección de amenazas informáticas*

El monitoreo de seguridad de red en las organizaciones es una tarea muy importante para detectar ataques malware, problemas en la red y evaluar su estado actual, así como analizar los eventos de seguridad para dar una pronta respuesta ante amenazas con el fin de proteger los activos de información.

El participante conocerá el funcionamiento interno detrás de todo sistema para la detección y prevención de intrusiones (IDS/IPS). Será capaz de utilizar las herramientas que le permitan hacer la valoración de las alertas, eventos y tráfico de red para ayudarle a tomar una decisión de acuerdo con las políticas y necesidades de su organización ante una posible brecha de seguridad

Nivel:
Intermedio

Temario

1. Introducción al monitoreo de seguridad de red
1.1 Introducción
1.2 Conceptos de redes
1.3 Modelo OSI
1.4 Modelo TCP/IP

2. Herramientas de análisis de tráfico de red
2.1 Herramientas para captura y análisis de paquetes
2.2 Análisis de paquetes
2.3 Filtros y búsqueda de patrones

3. Herramientas de monitoreo de tráfico de red
3.1 Introducción
3.2 Herramientas de monitoreo

4. Firewall
4.1 TCP Wrappers
4.2 Iptables
4.3 Packet Filter

5. Proxy
5.1 Características
5.2 Tipos
5.3 Tecnologías

6. Detección de tráfico malicioso
6.1 Introducción
6.2 IDS/Snort
6.3 Creación de reglas para la detección de tráfico malicioso

7. Honetpots
7.1 Fundamentos de las tecnologías honeypot
7.2 Tipos de honeypot

7.3 Despliegue de honeypots
7.4 Tecnologías complementarias

8. Otras tecnologías
8.1 UTM