FORMACION EN CIBERSEGURIDAD

Curso Core Networks en Gestión de Incidentes

Duración: 5 días -30 horas

Objetivos del curso:

✓ Conocer las metodologías más utilizadas en la gestión de incidentes.
✓ Capacitar para la elaboración de un plan de respuesta.
✓ Implantar herramientas que permitan detectar un incidente
✓ Cumplir con la normativa en relación a notificación y gestión de incidentes.

A quién está dirigido este curso:

- Personal de IT que esté implantando planes de gestión de incidentes o planee implantarlos.
- Personal de IT que quiera ampliar conocimientos en general y/o introducirse en el mundo del blue team.
- Administradores de red que quieran ampliar las herramientas para la detección de incidentes en su infraestructura.

Prerequisitos de conocimientos previos:

• Conocimientos de redes, protocolos TCP/IP, y protocolos estándar de aplicación, http, ftp, http, https, smtp, ssh, etc…

• Conocimientos a nivel de administración de Windows y Linux.

Contenidos:

1. Introducción y terminología.
2. Metodología de gestión de incidentes.
3. Detección de incidentes de seguridad. Logs y correlación.
4. Registros de eventos en Windows. Filtrado avanzado.
5. Extracción de logs de sistemas Windows.
6. Registros de eventos en Linux.
7. Extracción de logs de sistemas Linux.
8. Implantación de herramientas SIEM.
9. Intercambio de información, IoC.
10. Definición de casos de uso. El lenguaje Sigma.
11. Definición de procedimientos de actuación.
12. Notificación de incidentes. Obligaciones.