ESPECIALISTA EN WINDOWS: HARDENING, DFIR Y ANÁLISIS FORENSE

Área: OFIMÁTICA_INFORMÁTICA_TICS
Modalidad: Presencial
Duración: 30 h
Precio: Consultar

Curso Bonificable
Contactar
Recomendar
Matricularme

DESTINATARIOS

La acción formativa está dirigida a profesionales interesados en reciclar su formación, con la finalidad de potenciar sus habilidades y destrezas en el desempeño de sus funciones laborales.

OBJETIVOS

- Conocer qué es DFIR.
- Qué es el análisis forense.
- Normativa legal del análisis forense, derechos fundamentales, cadena de custodia..
- Conocer la estructura de los ficheros esenciales.
- Análisis Forense en sistemas Windows.
- Conocer cómo proceder respetando el marco legal.
- Conocer diferentes herramientas forenses de adquisición y análisis.

CONTENIDOS

1.Respuesta ante Incidentes y Análisis Forense
2.Metodología y peritaje
3.Forense y DFIR en Windows:
a.Herramientas de adquisición de evidencias: Live Response
b.Herramientas de búsqueda selectiva
c.Artifacts: Registro, Eventos, Papelera, Prefetching, USBs, LNKs, Tareas programadas, VSS, Navegadores, Correo electrónico, aplicaciones, ficheros recientes, jumplists, etc, ...
d.Malware: características, ocultación, servicios y procesos de Windows, abuso de Svchost, persistencia
e.Técnicas típicas de persistencia en sistemas
f.Análisis de Memoria RAM, Técnicas de análisis remota o local, Volatility, volcado de archivos, Credenciales en memoria
g.Intrusión: Ficheros recientes, Descubrimiento de ataques laterales
h.Sistemas de ficheros: Interpretación de artefactos forenses de sistemas de ficheros NTFS
4.Hardening Windows: Aplicación de CCN-STICs

CONTROLES APRENDIZAJE

Al finalizar el curso, se celebrará una prueba teórica presencial, cuyo nivel será acorde con el de la formación impartida, y a la que sólo se podrán presentar aquellos participantes que hayan cumplido con los requisitos mínimos de asistencia y participación para la superación del curso expuestos en el siguiente punto de esta guía.
La prueba presencial consistirá en un examen tipo test multirespuesta, siendo sólo una de ellas la correcta. La puntuación de la prueba será numérica, valorando cada pregunta con un punto sobre el total si es correcta y cero puntos si no se contesta o es errónea. La puntuación final se calculará sobre una nota máxima de 10, y se considerará apto si obtiene un mínimo de 5 puntos.