

Hacking, DFIR y Threat Hunting cuando las alertas guardan silencio

Duración: 40 Hrs.

SINOPSIS DEL CURSO

La jornada comienza como cualquier otra. Los sistemas están disponibles, los usuarios trabajan con normalidad y las herramientas de seguridad no reportan incidentes. Incluso las soluciones que incorporan inteligencia artificial parecen indicar que todo está bajo control.

Sin embargo, un atacante podría estar utilizando credenciales válidas, ejecutando herramientas legítimas y desplazándose entre equipos sin generar una alerta evidente. Entonces surge la pregunta: **si nuestras herramientas no detectan nada, ¿cómo sabemos dónde buscar?**

La respuesta comienza por comprender al adversario. Aprender hacking permite conocer cómo identifica oportunidades, explota vulnerabilidades, escala privilegios, obtiene credenciales y mantiene acceso. Este conocimiento ayuda a reconocer las huellas que puede dejar y a formular preguntas concretas para investigar.

DFIR transforma esas preguntas en una respuesta basada en evidencia. Aporta la metodología y las herramientas para realizar el triage, adquirir información relevante, delimitar el alcance del incidente y orientar las decisiones de contención, erradicación y recuperación.

Threat Hunting conecta ambas perspectivas. Cuando no existe una alerta que marque el punto de partida, permite buscar proactivamente comportamientos, patrones y artefactos asociados con una posible intrusión. Durante la respuesta a incidentes, ayuda a enfocar la investigación, priorizar sistemas y encontrar actividad relacionada, con el objetivo de responder con mayor rapidez y precisión.

La correlación de registros, artefactos y líneas de tiempo también puede ayudar a identificar al **posible paciente cero —el primer equipo comprometido— sin realizar inicialmente un análisis forense completo de cada sistema**. Estos hallazgos permiten dirigir la adquisición de evidencia y concentrar los esfuerzos de investigación donde resultan más útiles.

Pero la historia no termina cuando los servicios se recuperan. Un mecanismo de persistencia, una credencial comprometida o un equipo afectado que pasó inadvertido pueden permitir que el adversario regrese. Por ello, el hunting posterior al incidente busca **riesgo residual** y aporta evidencia para evaluar si la erradicación fue suficiente.

Integrar los tres temas permite comprender cómo ocurre un ataque, investigar sus consecuencias y buscar activamente aquello que podría permanecer oculto.

¿A QUIÉN VA DIRIGIDO?

El curso está dirigido a personas que buscan desarrollar o fortalecer sus capacidades de seguridad ofensiva, investigación y detección de amenazas:

- **Personas que inician en ciberseguridad:** quienes desean comprender la relación entre las técnicas de ataque, la evidencia digital y la respuesta defensiva.
- **Analistas SOC L1:** profesionales que buscan mejorar la interpretación de alertas, identificar actividad sospechosa y orientar el escalamiento de incidentes.
- **Analistas SOC L2:** profesionales que requieren profundizar en la investigación, correlación de eventos, delimitación del alcance y búsqueda de amenazas.
- **Analistas SOC L3:** especialistas interesados en fortalecer investigaciones avanzadas, desarrollar hipótesis de hunting y apoyar decisiones de respuesta.
- **Integrantes de Red Team:** profesionales que desean conectar las técnicas ofensivas con las evidencias y oportunidades de detección que generan.

Hacking, DFIR y Threat Hunting

cuando las alertas guardan silencio

- **Integrantes de Blue Team:** profesionales que buscan fortalecer la detección, el triage, la investigación y la respuesta a incidentes.
- **Integrantes de Purple Team:** profesionales que buscan integrar el conocimiento ofensivo y defensivo para mejorar la visibilidad y las capacidades de detección y respuesta.

HACKING

Descripción

Comprende cómo un atacante obtiene información, identifica vulnerabilidades y amplía su acceso dentro de un entorno. Este módulo aborda las etapas del ataque, desde el reconocimiento hasta el movimiento lateral, e incorpora el uso de inteligencia artificial como apoyo en las actividades de reconocimiento y análisis.

Conocer estas técnicas permite interpretar el comportamiento del adversario, reconocer sus posibles huellas y orientar las hipótesis de investigación utilizadas en DFIR y Threat Hunting.

Temario

1. Reconocimiento: identificación de la superficie de ataque

- a) Inteligencia de fuentes abiertas (OSINT).
- b) OSINT asistido por inteligencia artificial.

2. Escaneo, enumeración y análisis de vulnerabilidades

- a) Escaneo: identificación de sistemas y servicios.
 - Escaneo asistido por inteligencia artificial.
- b) Enumeración: obtención de información sobre los servicios identificados.
 - Enumeración asistida por inteligencia artificial.
- c) Análisis de vulnerabilidades: identificación y evaluación de debilidades de seguridad.
 - Análisis de vulnerabilidades asistido por inteligencia artificial.

3. Explotación

- a) Escalación de privilegios.
 - Técnicas de evasión del Control de Cuentas de Usuario (UAC bypass).

4. Persistencia con LOLBAS

- a. Uso de PowerShell.
- b. Uso de Notepad++
- c. Obtención de credenciales de SAM y LSASS mediante:
 - Pwdumpx.
 - ProcDump.
 - RdrLeakDiag.
 - DumpMiniTool.
 - Mimikatz.

Hacking, DFIR y Threat Hunting cuando las alertas guardan silencio

5. Password Cracking

Análisis y recuperación de contraseñas mediante técnicas de cracking.

6. Movimiento lateral

- a) Movimiento lateral mediante PsExec.
- b) Uso de PowerShell para movimiento lateral.
- c) Acceso remoto mediante RDP.

DFIR — ANÁLISIS FORENSE DIGITAL Y RESPUESTA A INCIDENTES

Descripción

Desarrolla una visión estructurada de la investigación y la respuesta a incidentes mediante estándares, marcos de trabajo y herramientas de primera respuesta. Este módulo aborda la adquisición de evidencia volátil y no volátil, la recolección de artefactos y el uso de playbooks para organizar las acciones de respuesta.

Su integración con el conocimiento ofensivo y el Threat Hunting permite interpretar los hallazgos, enfocar el triage y priorizar los sistemas que requieren investigación, favoreciendo decisiones sustentadas en evidencia.

Temario

1. Estándares y marcos de trabajo para la respuesta a incidentes

a) NIST

- Preparación.
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades posteriores al incidente.

b) SANS

- Preparación.
 - Dwell Time
- Identificación y delimitación del alcance.
 - Time to Contain
- Contención y desarrollo de inteligencia.
 - Time to Remediate
- Erradicación y remediación.
- Recuperación.
- Lecciones aprendidas.

c) Cyber Kill Chain

Comprensión de las etapas de un ataque mediante el modelo Cyber Kill Chain.

2. MITRE ATT&CK

- a) Casos de uso del framework MITRE ATT&CK.
- b) Uso de ATT&CK Navigator.

Hacking, DFIR y Threat Hunting

cuando las alertas guardan silencio

3. Respuesta a incidentes y triage

a) First Response Toolkit: herramientas para la primera respuesta

- Adquisición de evidencia forense volátil y no volátil:
 - Magnet RAM Capture.
 - Belkasoft Live RAM Capture.
 - LiME.
 - FTK Imager Lite.
- Recolección de artefactos forenses:
 - KAPE.
 - Velociraptor.

b) Playbooks de respuesta a incidentes

Uso de procedimientos estructurados para guiar las actividades de respuesta a incidentes.

THREAT HUNTING

Descripción

Desarrolla capacidades para buscar indicios de compromiso de forma proactiva, incluso cuando las herramientas de detección no han generado alertas. Este módulo aborda reglas YARA y Sigma, así como herramientas para identificar patrones y actividad sospechosa.

Durante la respuesta a incidentes, el Threat Hunting permite contrastar hipótesis, localizar sistemas afectados y aproximarse al posible origen del compromiso. Después de la recuperación, ayuda a buscar persistencia, actividad remanente y riesgo residual.

Temario

1. Reglas YARA

- a) Creación de reglas YARA.
- b) Uso de YaraMemoryScanner.
- c) Generación de reglas con yarGen.

2. Reglas Sigma

- a. Análisis con Zircolite.
- b. Conversión de reglas mediante Uncoder.io.
- c. Uso de Sigma UI.

3. APT Hunter

Uso de APT Hunter para la búsqueda de actividad sospechosa.

4. THOR Lite y Cloud

Uso de THOR Lite y sus opciones en la nube para la búsqueda de amenazas.