Incident Response Training

Requisitos para los participantes:

- Conocimientos básicos de sistemas operativos (Windows, Linux)
- Conocimientos básicos de sistemas de archivos
- Conocimientos básicos de los principios fundamentales de las redes
- Manejo básico de máquinas virtuales

¿A quién está dirigido?:

Estudiantes y profesionales con conocimientos básicos de sistemas operativos, sistemas de archivos y principios fundamentales de redes. Se valorará muy positivamente la experiencia en programación en cualquier lenguaje basado en scripts (Python, Bash, PowerShell, etc.).

¿Qué aprenderá?

Durante este curso los estudiantes aprenderán los fundamentos de la respuesta a incidentes y la ciencia forense digital.

La formación está orientada a la práctica y permite a los alumnos adquirir las habilidades necesarias de detección y respuesta a amenazas, análisis en tiempo real de sistemas comprometidos y uso de métodos avanzados de detección de ciberataques.

Duración: 40 horas / 5 días

Nuestros Expertos:

Eduardo Chavarro Ovalle

DFIR Group Manager – GERT LATAM

MSc en Seguridad de la Información, DFIR Group Manager para Americas del equipo global de Respuesta a Emergencias de Kaspersky, con más 20 años de experiencia en temas de investigación digital forense, eDiscovery, Análisis de Malware, Inteligencia de amenazas en los sectores defensa, telecomunicaciones, financiero e industrial. Cuenta con certificaciones internacionales en temas de Investigación digital forense, Investigación y defensa de entornos industriales, Gestión de la seguridad del Información, Test de Intrusión entre otras. Certificaciones: GCIH | GRID | GCFA | CHFI | CISM | CPTE | SFPC

Temas principales

En el mundo moderno, cada día aparecen nuevos ciberataques. Para los especialistas en ciberseguridad, esto significa que la capacidad de respuesta ante ciber incidentes y el análisis inicial en tiempo real del rendimiento de un ordenador comprometido, así como la recopilación y el análisis de pruebas, ya no son un lujo, sino una necesidad.

Todas estas habilidades son extremadamente importantes para los profesionales de la seguridad informática, ya que se enfrentan a ciberataques selectivos bien planificados de organizaciones de diversos perfiles: financiero, gubernamental, industrial y muchos otros.

En este curso, ofrecemos a los estudiantes la posibilidad de aprender la recopilación de datos de diversos tipos de pruebas y el análisis de la información recopilada.

Contenido práctico

Conceptos generales de Ciberseguridad, ataques dirigidos y amenazas comunes, vectores de ataque y servicios de seguridad.

Respuesta a incidentes: términos y definiciones, proceso de análisis y etapas. Detección de incidentes, recopilación de pruebas, análisis de archivos de registro con expresiones regulares, Indicadores de Compromiso (IoC), análisis de redes.

Análisis forense digital Introducción al análisis forense digital, organización de un laboratorio forense digital, virtualización, análisis del registro, artefactos del sistema operativo Windows, análisis forense del navegador, estructura del disco duro, análisis forense digital de soluciones en la nube.

Contenido:

- Introducción a la Respuesta a Incidentes
- Principales incidentes de hacking recientes

- Ataques APT
- Cyber Kill Chain
- Respuesta a Incidentes
- Escenarios de ataque
- ¿Cómo lo hacen?
- Escenario de ataque 1 (Ejercicio Práctico)
- Detección de incidentes
    - Detección basada en Red y Host
- Adquisición de evidencia
- Forense Digital
- Análisis de Memoria
- Análisis de logs
- Cyber Threat Intelligence (CTI)
- Análisis de Malware
- Análisis de Red
- Reportes
- Costrucción de un CSIRT
- Exámen Final (Ejercicio teorico práctico)

Resultado del curso

- Material altamente técnico
- Certificado de participación
-

Más Información en: https://academy.kaspersky.com/courses/incident-response-and-digital-forensics/

KATA Security Analyst

Requisitos para los participantes:

- Conocimientos básicos del dashboard de KATA
- Conocimientos básicos de sistemas de archivos
- Conocimientos básicos de los principios fundamentales de las redes

¿A quién está dirigido?:

Analistas y profesionales encargados de actividades de monitoreo, inteligencia de amenazas, respuesta a incidentes y análisis digital forense.

Analistas de ciberseguridad en general.

¿Qué aprenderá?

Durante este curso los estudiantes aprenderán los fundamentos generales de KATA, su arquitectura y componentes y se presentarán diferentes escenarios de investigación y respuesta, planteando ejercicios de investigación y análisis tradicionales versus actividades de detección, investigación y respuesta ejecutados con los componentes de KATA y EDR.

La formación está orientada a la práctica y permite a los alumnos adquirir las habilidades necesarias de detección y respuesta a amenazas, análisis en tiempo real de sistemas comprometidos y uso de métodos automatizados de detección de ciberataques.

Nuestros Expertos:

Eduardo Chavarro Ovalle

DFIR Group Manager – GERT LATAM

MSc en Seguridad de la Información, DFIR Group Manager para Americas del equipo global de Respuesta a Emergencias de Kaspersky, con más 20 años de experiencia en temas de investigación digital forense, eDiscovery, Análisis de Malware, Inteligencia de amenazas en los sectores defensa, telecomunicaciones, financiero e industrial. Cuenta con certificaciones internacionales en temas de Investigación digital forense, Investigación y defensa de entornos industriales, Gestión de la seguridad del Información, Test de Intrusión entre otras. Certificaciones: GCIH | GRID | GCFA | CHFI | CISM | CPTE | SFPC

Contenido

- Introducción a KATA
- Fundamentos de KATA
    - KATA / KEA colección y detección
    - Arquitectura
    - Alertas
    - Motores de Detección
- Ejercicio de Análisis (Duke Backdoor)
    - Investigación y remediación local en host
    - Investigar mediante EDR
    - Remediar mediante EDR
- Ejercicio de Análisis (A keyboard & clipboard logger)
    - Investigación y remediación local en host
    - Investigar mediante EDR
    - Remediar mediante EDR
- Ejercicio de Análisis (MSWord Exploit)
    - Investigación y remediación local en host
    - Investigar mediante EDR
    - Remediar mediante EDR
- Hands on Lab KATA/EDR
- Reglas de detección personalizadas (IOA & YARA)
- Hands on Lab Reglas personalizadas
- Reglas de detección personalizadas (IDS & IOC)
- Ejercicio Final, ¿dónde encontrar evidencia de la amenaza (En Kata)?

Duración: 8 horas / 1 día

Resultado del curso

- Material altamente técnico
- Certificado de participación