Curso Intensivo sobre Repuestas a Incidentes (DFIR)

Los ciberataques son cada vez más sofisticados y afectan a todo tipo de instituciones, siendo una tendencia común en la región.

Desde las organizaciones ya no basta con la prevención, debemos asumir que puede producirse el compromiso de parte o toda la infraestructura de nuestra organización.

Estar preparados para reaccionar es un paso fundamental frente a esta nueva realidad.

De esto se encarga el *DFIR (Digital Forensics and Incident Response)*, detectar, analizar, contener y responder frente a un incidente.

SEGU.INFO
SEGURIDAD DE LA INFORMACION

Objetivos generales

Este curso tiene como objetivo brindar a los asistentes los conocimientos mínimos para que una organización pueda realizar una adecuada investigación forense de incidentes de seguridad en redes (DFIR).

Está dividido en distintas etapas, incluyendo un desarrollo modelos de defensa, modelos de ataque, modelos mixtos, acercamiento al SOC y perfilamiento de los atacantes.

Requisitos previos

Conocimiento básico sobre Seguridad de la Información, análisis forense y redes.

Público Objetivo

El curso está orientado a administradores de IT, responsables de seguridad, área de legales y cualquier persona comprometida con el análisis forense interno o externo de seguridad en una organización. También está orientado a personas interesadas en la investigación del cibercrimen.

Material a entregar

Presentaciones utilizadas durante el curso en formato impreso y digital.

Instructores

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security. Se ha graduado como Especialista de Seguridad en la Universidad de Corea del Sur. Actualmente es Director de Segu-Info, Segu-Kids y Cofundador de ODILA: Observatorio de Delitos Informáticos de Latinoamérica. Se desempeña como consultor independiente en Seguridad de la Información. Ha trabajado en la investigación de malware durante más de 20 años y escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información. Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática y es expositor y conferencista en Jornadas, Congresos y Eventos relacionados a la Seguridad de la Información. Ha sido asesor en proyectos de Ley sobre delitos informáticos para el Honorable Senado de la Nación Argentina.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **8 horas** y la modalidad de cursada es presencial. También puede ser desarrollado ***in-company***.

Temario

INCIDENTES

- Necesidad de respuesta al incidente
- Política de respuesta a incidentes, plan y creación de procedimientos
- RFC 2828, RFC 3227, NIST 800-61
- Incident and Response (IR)
    - Modelos de defensa
    - Metodología
    - Ejemplo de implementación - NIST
- Modelos de ataque
    - MITRE ATT&CK
    - ¿Por qué son necesarios?
- Acercamiento al SOC
- Investigando un caso. Fileless attack
- Buscando indicadores de compromiso (IOC's)

Perfilando al Atacante

- HTTP profiling avanzado.
    - Inspección avanzada
    - Ruido vs IOC's
    - Forensia. Investigando un caso de APT
- Investigando el DNS
    - Passive DNS
    - Fast Flux DNS
- Network Forensics
    - Netflow deep inspection
    - Arquitectura
    - Artefactos
    - Open source tools para obtener IOC's
- Open Source Intelligence (OSINT)
    - Threat Intelligence 101
    - Arquitecturas y herramientas
- Laboratorios prácticos
- Lecciones aprendidas

PRÁCTICAS Y LABORATORIOS