Detección de amenazas con Cyber Threat Intelligence (CTI)

Objetivos

- Aprenda a aprovechar sus fuentes de datos existentes para extraer información útil y encontrar información complementaria de fuentes externas para la prevención de amenazas

- Aprenda a genera conocimiento de una amenaza y responder a preguntas claves como: ¿Quiénes?, ¿Qué?, ¿Cuándo?, ¿Por qué?, ¿Cómo? En relación con las amenazas.

Dirigido a

- Ingenieros en seguridad informática, entusiastas de ciberseguridad, técnicos, trabajadores de SOC, entre otros.

Metodología

- Curso virtual, 70% práctico, donde se explican conceptos relacionados y se realizan las prácticas con diferentes herramientas para ejemplificar los mismos.

Requisitos

- Equipos de computo.
- Maquinas virtuales que se darán previo al taller.

12 Horas

70% PRACTICO

30% TEORICO

CRlabsec Cyber Security

Contenido

Modulo 1 – Introducción al Data Collection

- Fuentes de Información Internas
- Fuentes de información externas
- Tipos de Feeds.
- Sacando provecho de OSINT

Modulo 2 – Administración y procesamiento de datos

- Procesamiento
- CTI estándar
- Formatos de compartición
- Threat Intelligence Platforms (TIP)

Modulo 3 – Análisis

- Introducción
- Modelo Cyber Kill Chain
- Curso de Acciones
- Definición de campañas
- Análisis de Heatmap

Modulo 4 – Atribución

- Introducción
- Sesgo cognitivo
- Errores lógicos
- Cómo gestionar los sesgos

Modulo 5 – Herramientas de CTI

- Introducción
- MISP
- MITRE
- Yeti
- Maltego
- Otros

Modulo 6 – Generación de inteligencia

- Inteligencia táctica
- Inteligencia Operacional
- Inteligencia Estratégica

Inscripción

Precio $250 + iva

Contacto: +506 83342943 / Info@crlabsec.com