Operaciones Cibernéticas Ofensivas y Defensivas

Purple Teaming, Threat Hunting e Inteligencia de Amenazas

Presented By:
BSides Colombia

Acerca del Entrenamiento

Descripción

Domina el arte de la defensa y el ataque cibernético en este curso integral que cubre Purple Teaming, Emulación de Adversarios, Threat Hunting, Ingeniería de Detección y Ciberinteligencia de Amenazas. Aprende a replicar tácticas avanzadas de atacantes, detectar amenazas en tiempo real y fortalecer las defensas organizacionales con inteligencia procesable.

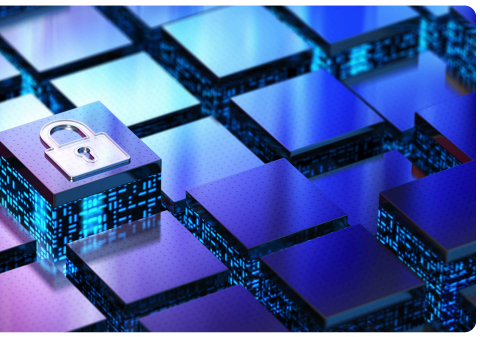
A través de laboratorios prácticos y escenarios del mundo real, desarrollarás habilidades para identificar, analizar y mitigar amenazas cibernéticas utilizando marcos como MITRE ATT&CK y TTPs de actores de amenazas avanzados. Ya sea que busques mejorar tus habilidades ofensivas o defensivas, este curso te transformará en un especialista capaz de anticipar, detectar y neutralizar amenazas con precisión.

BSIDES COLOMBIA

Temas Clave

- Metodologías avanzadas de Purple Team.
- Emulación de adversarios y detección proactiva de amenazas.
- Threat Hunting impulsado por inteligencia de amenazas.
- Ingeniería de detección para mejorar operaciones de seguridad.
- Análisis de TTPs y respuesta estratégica a incidentes.

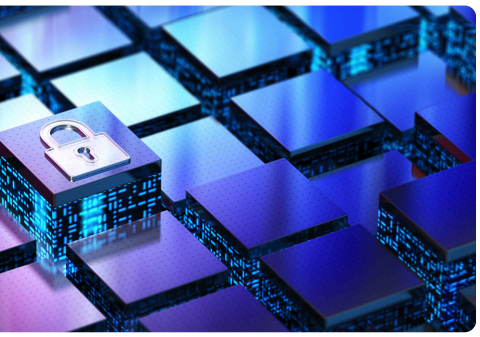
Temario del Curso



Módulo 1: Fundamentos del Framework ATT&CK®

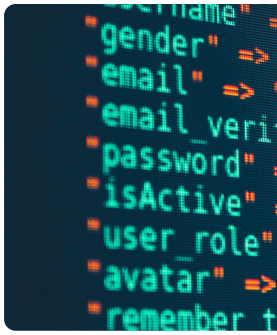
- Introducción a ATT&CK®
- Comprensión de matrices y plataformas
- Descripción general de tácticas, técnicas y sub-técnicas
- Implementación de mitigaciones en operaciones de seguridad
- Fuentes de datos y estrategias de detección
- Identificación de actores de amenazas y su software
- Perspectivas comunitarias:
  - Establecimiento de un lenguaje común
  - Puntuación cuantitativa para análisis de amenazas
  - Navegación en ATT&CK con ATT&CK Navigator
- Aplicación práctica:
  - Integración de inteligencia de amenazas cibernéticas
  - Técnicas de detección y análisis
  - Emulación de amenazas para Red & Blue Team
  - Evaluaciones de ingeniería para mejora de detecciones
  - Resumen del curso

Temario del Curso

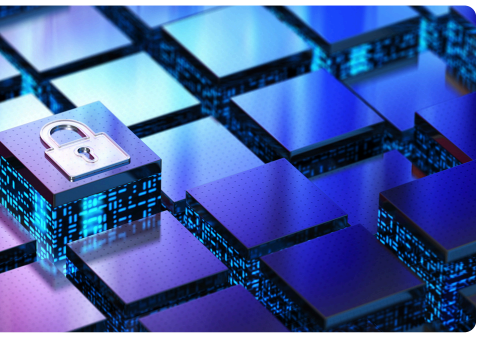


Módulo 2: Emulación de Adversarios y Simulación de Ataques

- Fundamentos de la emulación de adversarios
- Marcos y metodologías de emulación de adversarios
- Definición de objetivos operativos y alcance de compromisos
- Creación de un plan efectivo de emulación de adversarios
- Laboratorios prácticos:
  - Exploración de la biblioteca de emulación de adversarios
  - Configuración del entorno de laboratorio para simulación

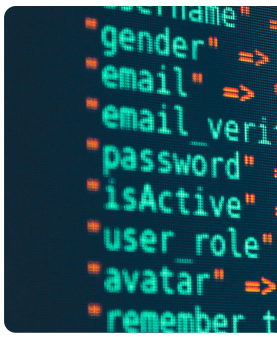


Temario del Curso

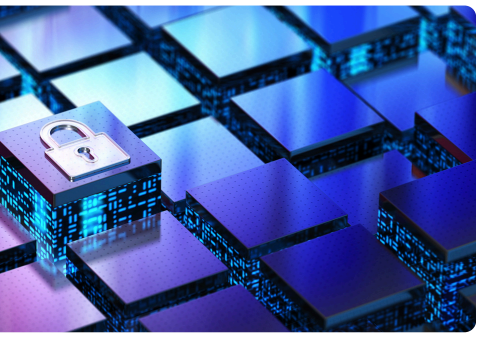


Módulo 3: Ciberinteligencia de Amenazas (CTI) en Emulación de Adversarios

- Investigación de amenazas y TTPs:
  - Selección de TTPs relevantes
  - Análisis de brechas de inteligencia y mitigación
- Planificación estratégica en CTI:
  - Definición de alcance, reglas de compromiso y autorización
- Implementación y automatización de TTPs:
  - Planificación e implementación de TTPs adversarios
  - Automatización de estrategias de emulación
  - Identificación de detecciones y estrategias de mitigación
- Ejecución y documentación en el mundo real:
  - Manejo de situaciones inesperadas
  - Desarrollo y refinamiento de planes de emulación de adversarios

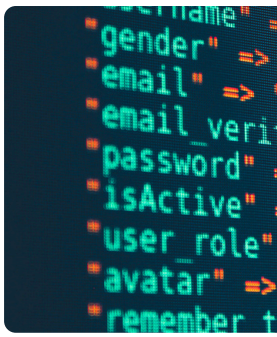


Temario del Curso

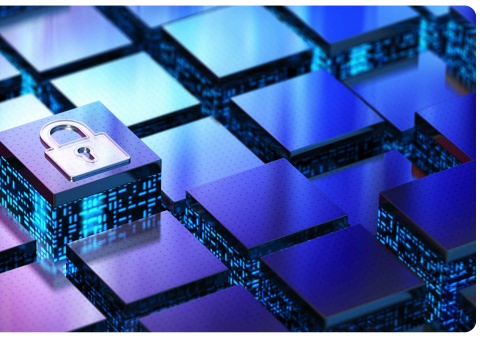


Módulo 4: Threat Hunting e Ingeniería de Detección

- Conceptos clave de Threat Hunting:
  - Metodologías de detección basadas en TTPs
  - Priorización de amenazas y alertas
  - Revisión de metodologías y marcos
- Desarrollo de hipótesis de caza de amenazas:
  - Técnicas de investigación y análisis
  - Refinamiento de hipótesis y creación de analíticas
- Recolección y análisis de datos:
  - Identificación de fuentes de datos críticas
  - Abordaje de brechas en la recolección de datos
  - Desarrollo de estrategias de sensores y análisis alternativos
- Optimización y ajuste de detecciones:
  - Implementación y validación de analíticas
  - Mejora del rendimiento, precisión y recall

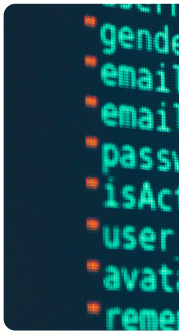


Temario del Curso

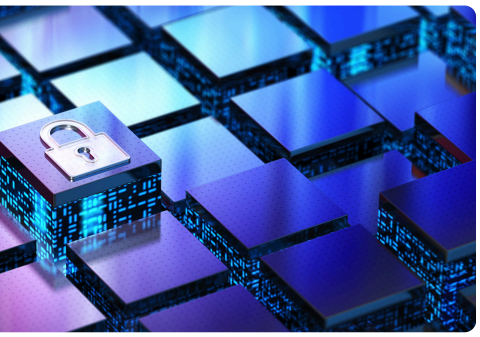


Módulo 5: Inteligencia de Amenazas para Detección y Respuesta

- Extracción de inteligencia desde informes narrativos:
  - Identificación y análisis de comportamientos
  - Mapeo de técnicas y sub-técnicas a ATT&CK®
  - Conciencia de sesgos y mitigación
- Procesamiento de datos en inteligencia accionable:
  - Mapeo de comportamientos desde datos en bruto
  - Traducción de datos en informes de amenazas
- Almacenamiento y análisis de inteligencia de amenazas:
  - Técnicas efectivas de almacenamiento y visualización de datos
  - Análisis comparativo con ATT&CK Navigator
- Desarrollo de estrategias defensivas:
  - Comprensión de cómo se explotan las técnicas
  - Alineación de capacidades organizacionales con medidas defensivas

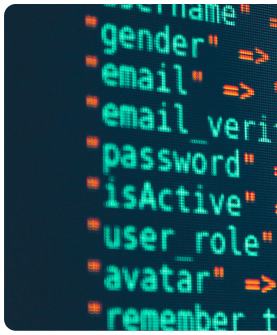


Temario del Curso



Módulo 6: Metodología de Purple Teaming e Implementación en el Mundo Real

- Fundamentos de Purple Teaming:
  - Introducción a la colaboración entre Red y Blue Teams
  - Planificación y estructuración de ejercicios de Purple Team
- Ejecución y mejora continua:
  - Simulación en vivo de adversarios y desarrollo de detecciones
  - Análisis post-compromiso y estrategias de seguimiento



Inversión

En este curso aprenderás a cazar amenazas, detectar ataques reales y desarrollar estrategias ofensivas y defensivas con herramientas y metodologías avanzadas.

El conocimiento avanzado en Purple Teaming, Threat Hunting & Intelligence Operations suele estar reservado para profesionales con grandes presupuestos.

En el mercado, este tipo de formación cuesta alrededor de $8.700.000 COP.

Pero en BSides Colombia, creemos en el acceso a la educación de calidad. Por eso, este curso estará disponible por solo $1.000.000 COP – una fracción de su valor real.

- Fecha: 11 y 12 de Junio de 2025
- Lugar: Universidad de Antioquia - BSides Colombia
- Entrenamiento presencial de 16 horas
- Certificación de asistencia avalada por BSides
- Impartido por Levi Reza, experto en ciberseguridad

¡Cupos limitados! No pierdas esta oportunidad.

Levi Reza

CISO | Consultant Senior | Trainer | Speaker

Es un investigador senior en ciberseguridad, con más de 15 años de experiencia y más de 25 certificaciones internacionales. Es especialista en DFIR, Pentest, Threat Hunting y Threat Intelligence, ha colaborado con las Big Four, así como con instituciones militares, financieras, policía cibernética, cancilleria mexicana, entidades financieras y empresas del sector privado. Su enfoque se centra en el diseño de estrategias efectivas para la protección de infraestructuras críticas y el fortalecimiento de la seguridad organizacional. Combina una sólida experiencia técnica con una visión estratégica, liderando iniciativas innovadoras para mitigar riesgos y responder a incidentes de manera práctica y efectiva. Ha sido galardonado en el Círculo de Excelencia de EC-Council como instructor en 2017, 2019, 2022, 2023 y 2024, reconocimiento que avala su compromiso con la excelencia en la capacitación.