CYBERIUM ARENA

Descripción

Sumérgete en el ámbito de la Caza de Amenazas con esta formación completa y práctica. Comienza con conceptos fundamentales, luego domina técnicas avanzadas, desde la informática forense de puntos finales hasta el análisis de redes. Participa en escenarios y laboratorios del mundo real, explorando todo, desde aplicaciones de aprendizaje automático hasta consideraciones éticas. Al final, emergerás como un cazador de amenazas hábil, adepto a identificar y mitigar los desafíos cambiantes de la ciberseguridad.

NX223 - CAZA DE AMENAZAS

Módulo 1: Introducción a la Caza de Amenazas

Sumérgete en la configuración y estrategias de caza de amenazas. Entiende la ciberseguridad proactiva versus reactiva, explora las estructuras de Cyber Kill Chain y MITRE ATT&CK, y domina herramientas como SIEM y EDR. Aprovecha las fuentes de inteligencia de amenazas y simula amenazas del mundo real en laboratorios configurados.

Configuración del Entorno de Caza

Ciberseguridad Proactiva vs. Reactiva
Cyber Kill Chain y Estructura MITRE ATT&CK
SIEM, EDR y Plataformas de Inteligencia de Amenazas
Configuración de un Laboratorio para Amenazas Simuladas
Logs, Tráfico de Red y Datos de Punto Final
Fuentes de Inteligencia de Amenazas
Alimentando Inteligencia en Herramientas de Caza

Módulo 2: Simulaciones Prácticas

Profundiza en metodologías avanzadas de caza de amenazas, desde tácticas basadas en hipótesis hasta enfoques heurísticos. Domina el arte de detectar movimientos laterales en la red, comunicaciones de Comando y Control (C2), y tentativas de exfiltración de datos. Mejora tus habilidades en forenses de memoria, descubriendo mecanismos de persistencia e identificando técnicas elusivas de malware sin archivos.

Técnicas y Tácticas de Caza

Caza Basada en Hipótesis
Detección de Patrones y Anomalías
Enfoques Heurísticos
Detectando Movimiento Lateral dentro de una Red
Comunicaciones de Comando y Control (C2)
Identificando Intentos de Exfiltración de Datos
Análisis y Forenses de Memoria
Detectando Mecanismos de Persistencia
Descubriendo Técnicas de Malware Sin Archivos

Módulo 3: Caza en Redes

Sumérgete en la caza de amenazas en redes, desde la inspección profunda de paquetes hasta el monitoreo de DNS. Identifica tráfico sospechoso, amenazas encriptadas y aprovecha técnicas de aprendizaje automático. Explora la detección de amenazas internas, estrategias de honeypots y análisis de brechas reales.

Inspección y Análisis Profundo de Paquetes

Estableciendo Comportamiento Basal de la Red
Monitoreo y Análisis de DNS
Identificando Patrones de Tráfico Sospechoso
Descubriendo Amenazas Encriptadas
Caza de Amenazas usando Aprendizaje Automático
Caza de Amenazas Internas
Honeypots y Tecnologías de Engaño
Análisis de Brechas Reales y APTs

Módulo 4: Respuesta y Remediación

Emprende un viaje a través de la caza de amenazas y respuesta a incidentes, profundizando en análisis forense y estrategias de contención. Domina evaluaciones post-incidente, asegura monitoreo continuo e integra inteligencia de amenazas en prácticas de caza. Concluye con protocolos robustos de respaldo y recuperación ante desastres.

Caza de Amenazas y Respuesta a Incidentes

Análisis Forense
Estrategias de Contención y Mitigación
Análisis Post-Incidente
Monitoreo Continuo
Inteligencia de Amenazas en la Caza de Amenazas
Respaldos y Recuperación ante Desastres

Defensa NX | NIVEL: 5 | DURACIÓN: 40h