Especialización en Ciberseguridad (Desde Cero)

Esta especialización está diseñada para proporcionar una base sólida y progresiva en el campo de la ciberseguridad, comenzando por los conceptos fundamentales hasta llegar a aspectos más técnicos y prácticos.

Requisitos para Cursar:

Nivel 1: No se requieren conocimientos previos específicos. Se recomienda tener habilidades básicas de manejo de ordenadores y navegación por internet.

Nivel 2-4: Haber completado satisfactoriamente el nivel anterior o demostrar conocimientos equivalentes. Para el Nivel 4 se recomienda tener un interés activo en la resolución de problemas técnicos y la seguridad informática.

Nivel 1: Fundamentos de la Ciberseguridad

El primer nivel establece una comprensión básica de los conceptos clave de la ciberseguridad, las amenazas comunes y las mejores prácticas para la protección personal y organizacional. Con una duración de 15 horas, este nivel es accesible para todos los interesados en iniciarse en este campo, incluyendo estudiantes, profesionales de TI que desean especializarse y personas sin conocimientos técnicos que buscan proteger sus activos digitales.

Introducción a la Ciberseguridad

Conceptos fundamentales de confidencialidad, integridad y disponibilidad. Panorama actual de amenazas y legislación básica de protección de datos. Historia y evolución de la ciberseguridad, importancia en el mundo digital actual y roles profesionales en el sector.

Amenazas Comunes

Malware, phishing, ingeniería social, ataques a contraseñas y ataques de denegación de servicio. Análisis de casos reales, vectores de ataque más utilizados, tendencias emergentes en ciberdelincuencia y métodos de identificación de amenazas potenciales.

Principios de Protección

Gestión de contraseñas seguras, autenticación multifactor, navegación segura, protección contra malware y firewalls. Configuración de herramientas de seguridad básicas, respaldos de información, actualizaciones de software y prácticas recomendadas para dispositivos móviles.

Seguridad en la Vida Digital

Protección de la privacidad en redes sociales, seguridad en el correo electrónico, compras seguras en línea, protección de la identidad digital y configuración de privacidad en aplicaciones y servicios habituales. Evaluación de riesgos personales y creación de un plan de seguridad básico.

Al finalizar este nivel, los participantes serán capaces de identificar las principales amenazas de seguridad, implementar medidas básicas de protección en sus dispositivos personales y comprender los fundamentos que servirán como base para niveles más avanzados de la especialización.

Nivel 2: Seguridad en Sistemas y Redes

El segundo nivel introduce los conceptos técnicos fundamentales de la seguridad en sistemas operativos y redes, así como las herramientas básicas para su protección y análisis. Con una duración de 15 horas, este módulo profundiza en aspectos más técnicos de la ciberseguridad, proporcionando conocimientos esenciales para identificar vulnerabilidades, implementar controles de seguridad básicos y comprender cómo funcionan los ataques a nivel de sistema y red. Está diseñado para participantes que ya dominan los fundamentos básicos y desean avanzar hacia roles más técnicos en el campo de la ciberseguridad.

Sistemas Operativos y Seguridad

Principios de seguridad en sistemas operativos Windows y Linux, gestión de usuarios y permisos (RBAC), implementación de políticas de seguridad robustas, configuración y análisis de auditoría y logs del sistema para detección de actividades sospechosas, introducción a la seguridad en línea de comandos y scripts de seguridad básicos. Aprenderás también sobre hardening de sistemas y reducción de superficie de ataque.

Fundamentos de Redes y Seguridad

Conceptos básicos de redes TCP/IP, análisis detallado de los modelos OSI y TCP/IP, protocolos comunes y sus vulnerabilidades inherentes, configuración segura de dispositivos de red como routers y switches, implementación de firewalls y reglas efectivas, diseño de segmentación de red para protección por capas, y conceptos de VPN y comunicaciones cifradas. Incluye laboratorios prácticos de configuración segura.

Detección de Intrusiones

Sistemas IDS/IPS (diferencias, tipos y configuración básica), técnicas avanzadas de análisis de logs de red, uso profesional de herramientas de monitorización como Wireshark y Suricata, configuración de alertas efectivas, correlación de eventos de seguridad para identificar patrones de ataque, creación de reglas personalizadas y respuesta inicial ante posibles intrusiones. Se incluyen ejercicios con tráfico de red real para análisis.

Seguridad Web Básica

Identificación y mitigación de vulnerabilidades comunes en aplicaciones web según OWASP Top 10, técnicas detalladas de prevención de inyección SQL, Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF), implementación de buenas prácticas de desarrollo seguro, configuración de servidores web, uso de HTTPS y certificados SSL/TLS, y evaluación básica de seguridad en sitios web. Incluye demostraciones prácticas de ataques y defensas.

Nivel 3: Análisis de Vulnerabilidades y Pruebas de Penetración

El tercer nivel introduce los conceptos y metodologías básicas del análisis de vulnerabilidades y las pruebas de penetración de forma ética y controlada. Este módulo de 15 horas permite a los estudiantes adentrarse en el mundo del pentesting, desarrollando habilidades prácticas en entornos controlados que simulan situaciones reales.

Análisis de Vulnerabilidades

Tipos de vulnerabilidades (técnicas, físicas, humanas, lógicas), metodologías de análisis estructurado (OSSTMM, PTES, OWASP), herramientas de escaneo automatizado como Nessus, OpenVAS y Qualys. Aprenderás a priorizar vulnerabilidades según su impacto potencial y probabilidad de explotación.

Fundamentos de Pentesting

Objetivos estratégicos y definición del alcance del pentesting, diferencias metodológicas entre pruebas de caja negra, caja blanca y caja gris. Conocerás las cinco fases esenciales: reconocimiento, escaneo, explotación, mantenimiento de acceso y eliminación de huellas.

Herramientas Básicas

Introducción exhaustiva a Kali Linux como plataforma especializada para seguridad, dominio de comandos avanzados de terminal, herramientas profesionales de reconocimiento (OSINT) como Maltego, theHarvester y técnicas de escaneo con Nmap y Metasploit Framework.

Informes y Documentación

Desarrollo de informes profesionales siguiendo estándares internacionales, metodologías de clasificación de riesgos (CVSS, DREAD, STRIDE), y elaboración de planes detallados de remediación con plazos y recursos necesarios.

Al finalizar este nivel, los participantes habrán adquirido las competencias necesarias para identificar, documentar y comunicar vulnerabilidades de seguridad de manera profesional, sentando las bases para especializaciones más avanzadas en el campo de la seguridad ofensiva.

Nivel 4: Respuesta a Incidentes y Seguridad Ofensiva

El nivel final introduce los conceptos avanzados de la respuesta a incidentes de seguridad y proporciona una visión profunda de las técnicas de seguridad ofensiva. Este módulo de 15 horas completa la formación con aspectos especializados de la ciberseguridad, preparando a los estudiantes para enfrentar situaciones reales y complejas en entornos profesionales.

Respuesta a Incidentes

Tipos de incidentes (malware, phishing, DDoS, ransomware), ciclo de vida completo de la respuesta (preparación, detección, análisis, contención, erradicación, recuperación, lecciones aprendidas), roles y responsabilidades del equipo de respuesta, herramientas especializadas como SIEM y EDR, técnicas de triage, comunicación efectiva y gestión de crisis.

- Planificación y documentación de procedimientos de respuesta
- Simulaciones y ejercicios prácticos de incidentes
- Coordinación con equipos externos y autoridades

Seguridad Ofensiva

Diferencias fundamentales entre seguridad defensiva y ofensiva, implementación práctica del marco MITRE ATT&CK, técnicas avanzadas de evasión de defensas, metodologías de post-explotación, inteligencia de amenazas estratégica y táctica, y simulación de adversarios (red teaming).

- Técnicas de reconocimiento avanzado y movimiento lateral
- Explotación de vulnerabilidades en entornos controlados
- Desarrollo de escenarios realistas de ataque

Análisis Forense Digital

Objetivos y principios fundamentales del análisis forense, tipos de evidencia digital (volátil y no volátil), procesos meticulosos de adquisición y preservación de evidencia, cadena de custodia, análisis de memoria RAM, recuperación de datos eliminados y herramientas especializadas como Autopsy, FTK y EnCase.

- Análisis de malware y técnicas de ingeniería inversa básica
- Investigación de incidentes en sistemas operativos Windows y Linux
- Extracción y análisis de artefactos forenses en dispositivos móviles

Tendencias Futuras

Desafíos de seguridad en entornos cloud híbridos y multi-nube, protección de ecosistemas de dispositivos IoT, aplicaciones de inteligencia artificial y machine learning en detección de amenazas, análisis predictivo de vulnerabilidades, tecnología blockchain y sus aplicaciones en ciberseguridad, y nuevos vectores de ataque emergentes.

- Seguridad en arquitecturas sin servidor y contenedores
- Evolución de las amenazas y grupos de APT (Advanced Persistent Threats)
- Impacto de la computación cuántica en la criptografía actual

Al finalizar este nivel, los estudiantes habrán adquirido una base sólida en respuesta a incidentes y seguridad ofensiva, complementando los conocimientos previamente obtenidos en los niveles anteriores. Esto les permitirá enfrentar situaciones reales con un enfoque metodológico y profesional, siguiendo las mejores prácticas de la industria y adaptándose a un panorama de amenazas en constante evolución.