Networking Academy

Administración de Amenazas Cibernéticas

Alcance y secuencia

1.0

Contenido

Público Meta

El curso de Administración de Amenazas Cibernéticas es apropiado para estudiantes con nivel en lectura secundaria, conocimientos básicos en informática e interesados en buscar un trabajo de nivel de entrada en el campo de la seguridad cibernética.

Requisitos Previos

No hay requisitos previos para este curso, aunque los alumnos deben tener las siguientes habilidades básicas:

- Habilidades básicas de navegación del sistema operativo de PC
- Conocimiento de las redes TCP/IP, incluidos los protocolos, servicios y procesos de red.

Si bien no es obligatorio, se recomienda que los alumnos completen los siguientes cursos dentro de la ruta de aprendizaje de seguridad cibernética:

- Introducción a la Ciberseguridad
- Fundamentos de redes
- Seguridad de Terminales
- Defensa de la red

Alineación a Certificación

Este curso, de la Carrera Profesional de Analista de Ciberseguridad Junior, se alinea con la certificación de CCST Cybersecurity.

Descripción del curso

Administración de Amenazas Cibernéticas tiene muchas funciones para ayudar a los alumnos a comprender los conceptos de seguridad. El diseño del curso incluye:

- Seis módulos compuestos por temas clave.
- Los módulos enfatizan el pensamiento crítico, la resolución de problemas, la colaboración y la aplicación práctica de las habilidades.
- Cada módulo contiene actividades de práctica y evaluación, una actividad de Verifique su Comprensión, un laboratorio o una actividad utilizando nuestra herramienta de simulación de red, Cisco® Packet Tracer.
- Las actividades de nivel de tema están diseñadas para indicar el dominio de un alumno de las habilidades del curso, lo que permite a los alumnos evaluar la comprensión antes de realizar un cuestionario o examen calificado.
- El lenguaje que describe los conceptos está diseñado para que los estudiantes de secundaria lo entiendan fácilmente.
- Las evaluaciones y actividades de práctica enfocadas en competencias específicas están diseñadas para aumentar la retención y proporcionar flexibilidad en la ruta de aprendizaje.

- Las herramientas de aprendizaje multimedia, incluidos videos y cuestionarios, abordan una variedad de estilos de aprendizaje, estimulan el aprendizaje y promueven la retención de conocimientos.
- Las actividades de laboratorio y Packet Tracer ayudan a los estudiantes a desarrollar el pensamiento crítico y habilidades para resolver problemas complejos.
- Las evaluaciones innovadoras brindan retroalimentación inmediata para respaldar la evaluación del conocimiento y las habilidades.
- Los conceptos técnicos se explican utilizando un lenguaje de nivel introductorio.
- Las actividades interactivas integradas dividen la lectura de grandes bloques de contenido y refuerzan la comprensión.
- El curso enfatiza las habilidades aplicadas, la experiencia práctica y alienta a los alumnos a considerar educación adicional en TI.

Objetivos del Curso

Administración de Amenazas Cibernéticas presenta importantes conceptos fundamentales en ciberseguridad, como ética y gobernanza, pruebas de seguridad de red, inteligencia de amenazas, evaluación de vulnerabilidades de puntos finales, gestión de riesgos y respuesta posterior a incidentes. Al final del curso, los alumnos estarán preparados para participar en una amplia gama de actividades de gestión de amenazas y respuesta a incidentes como miembros de un equipo de operaciones de ciberseguridad.

El material del curso lo ayudará a desarrollar las habilidades de los alumnos, que incluyen:

- Crear documentos y políticas relacionadas con la gobernanza y el cumplimiento de la ciberseguridad.
- Utilizar herramientas para las pruebas de seguridad de la red.
- Evaluar las fuentes de inteligencia de amenazas.
- Explicar cómo se evalúan y gestionan las vulnerabilidades de los terminales.
- Seleccionar controles de seguridad basados en los resultados de la evaluación de riesgos
- Utilizar modelos de respuesta a incidentes y técnicas forenses para investigar incidentes de seguridad.

Requisitos del equipo

Los laboratorios prácticos de gestión de ciberamenazas requieren equipos que se encuentran en la mayoría de las redes domésticas. Cualquier laboratorio que requiera un entorno de red más complejo utiliza Packet Tracer, la herramienta de simulación de red.

Software

- Oracle Virtualbox
- Archivos OVA de máquina virtual de laboratorio
- Packet Tracer 8.1 o superior

Equipo de laboratorio opcional

- Dispositivo con Microsoft Windows instalado

Esquema del curso

La Tabla 1 detalla los módulos y sus competencias asociadas. Cada módulo es una unidad integrada de aprendizaje que consta de contenido, actividades y evaluaciones que apuntan a un conjunto específico de competencias. El

tamaño del módulo depende de la profundidad del conocimiento y la habilidad necesarios para dominar la competencia.

Tabla 1: Título y objetivo del módulo

Título del módulo/Título del tema	Objetivo
Módulo 1: Gobernanza y Cumplimiento	
1.0 Gobernanza y Cumplimiento	Crear documentos y políticas relacionadas con la gobernanza y el cumplimiento de la ciberseguridad.
1.1 Gobernanza	Crear documentos de política de ciberseguridad.
1.2 La ética de la ciberseguridad	Crear un código personal de conducta ética.
1.3 Marco de gestión de seguridad de TI	Evaluar los controles de seguridad.
Módulo 2: Pruebas de seguridad de red	
2.0 Pruebas de seguridad de red	Utilizar herramientas para las pruebas de seguridad de la red.
2.1 Evaluaciones de seguridad	Usar comandos para recopilar información de red y diagnosticar problemas de conectividad.
2.2 Técnicas de prueba de seguridad de red	Describir las técnicas utilizadas en las pruebas de seguridad de la red.
2.3 Herramientas de prueba de seguridad de red	Describir las herramientas utilizadas en las pruebas de seguridad de la red.
2.4 Pruebas de penetración	Describir cómo una organización utiliza las pruebas de penetración para evaluar la seguridad del sistema.
Módulo 3: Inteligencia de amenazas	
3.0 Inteligencia de amenazas	Evaluar las fuentes de inteligencia de amenazas.
3.1 Fuentes de información	Evaluar las fuentes de información utilizadas para comunicar las amenazas emergentes a la seguridad de la red.
3.2 Servicios de inteligencia de amenazas	Describir varios servicios de inteligencia de amenazas.
Módulo 4: Evaluación de la vulnerabilidad de los endpoints	
Evaluación de vulnerabilidades de endpoints 4.0	Explicar cómo se evalúan y gestionan las vulnerabilidades de los terminales.
4.1 Perfilado de redes y servidores	Explicar el valor de la creación de perfiles de red y servidor.
4.2 Sistema de puntuación de vulnerabilidad común (CVSS)	Explicar cómo se utilizan los informes CVSS para describir las vulnerabilidades de seguridad.

4.3 Gestión segura de dispositivos	Explicar cómo se utilizan las técnicas de gestión segura de dispositivos para proteger los datos y los activos.
Módulo 5: Gestión de Riesgos y Controles de Seguridad	
5.0 Gestión de Riesgos y Controles de Seguridad	Seleccionar los controles de seguridad en función de los resultados de la evaluación de riesgos.
5.1 Gestión de riesgos	Explicar la gestión de riesgos.
5.2 Evaluación de riesgos	Calcular riesgos.
5.3 Controles de seguridad	Evaluar los controles de seguridad según las características de la organización.
Módulo 6: Forense digital y Análisis y respuesta a incidentes	
6.0 Forense digital y Análisis y respuesta a incidentes	Utilizar modelos de respuesta a incidentes y técnicas forenses para investigar incidentes de seguridad.
6.1 Manejo de evidencia y atribución de ataques	Explicar el papel de los procesos forenses digitales.
6.2 La Cadena de Matanzas Cibernéticas	Identificar los pasos en Cyber Kill Chain.
6.3 El modelo de diamante de análisis de intrusión	Utilizar el modelo de diamante de análisis de intrusión para clasificar los eventos de intrusión.
6.4 Respuesta a incidentes	Aplicar los procedimientos de manejo de incidentes NIST 800-61r2 a un escenario de incidente dado.
6.5 Recuperación de desastres	Utilizar comandos para realizar copias de seguridad de archivos y restaurar operaciones de red.