CCSTC - Cisco Certified Support Technician Cybersecurity

Duración: 70 hrs

Descripción general

Esta formación oficial diseñada por Cisco, *Cisco Certified Support Technician Cybersecurity*, se conforma en base a un recorrido curricular por las áreas clave en la evaluación y el mantenimiento de la seguridad de la información en las organizaciones, incluyendo los sistemas operativos, las aplicaciones y las comunicaciones en red. Partiendo de aspectos fundamentales, se ofrece una perspectiva integral del escenario actual de las amenazas de ciberseguridad; se identifican y categorizan los objetivos, las vulnerabilidades, los autores, y la diversidad de elementos tecnológicos de los que se aprovechan los atacantes.

Así mismo, se caracterizan las diferentes fases que conforman los ciberataques, y los puntos a tener en cuenta para establecer los mejores métodos de contención y defensa. También se tratan los modelos, aproximaciones y tecnologías empleadas en el establecimiento de los mecanismos de seguridad, tanto desde la perspectiva de la comunicación en red, y de los dispositivos que la soportan, como de la seguridad en los puntos finales –clientes y servidores-.

A continuación, se exponen metodologías para la monitorización, evaluación y gestión de la seguridad de la red y de los sistemas operativos y se muestra cómo recabar inteligencia de amenazas para el descubrimiento de vulnerabilidades existentes o potenciales en la organización. A partir del conocimiento de estos elementos, se evidencia la necesidad de aplicar medidas de protección e implementar una serie de buenas prácticas, mediante marcos de gobernanza y cumplimiento, con el objeto de mejorar los niveles de seguridad en las organizaciones, y ser capaz de gestionar y responder ante incidentes de ciberseguridad.

Los contenidos de esta formación están alineados con los objetivos del examen de certificación en Ciberseguridad, CSC-200V: Cybersecurity, cuya superación reconoce, en el marco del programa de referencia en tecnologías de la información, con la certificación oficial Cisco Certified Support Technician Cybersecurity, (CCST- Cybersecurity), que avala la asimilación de los conocimientos y el desempeño en el conjunto de habilidades y competencias básicas requeridas a los profesionales de este ámbito, como técnicos y analistas de ciberseguridad.

Los contenidos oficiales que conforman este recorrido profesional en Ciberseguridad, se ofrecen a través del programa Cisco Networking Academy, proyecto diseñado por la multinacional Cisco Systems,

con el objetivo de acercar a la comunidad IT una formación y certificación oficial en el ámbito tecnológico, especializándose en redes e Internet.

Objetivos

- Explicar cómo los actores de amenazas ejecutan algunos de los tipos más comunes de ciberataques.
- Explicar los principios de seguridad de la red.
- Explicar cómo las vulnerabilidades de TCP/IP permiten los ataques a la red.
- Recomendar medidas para mitigar las amenazas.
- Solucionar problemas en redes inalámbricas.
- Explicar cómo se utilizan los dispositivos y servicios para mejorar la seguridad de la red.
- Utilizar las herramientas administrativas de Windows.
- Implementar la seguridad básica de Linux.
- Evaluar la protección de puntos finales y los impactos del malware.
- Utilizar las mejores prácticas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad.
- Explicar los enfoques para la defensa de la seguridad de la red.
- Implementar algunos de los diversos aspectos del sistema y la defensa de la red.
- Configurar el control de acceso local y basado en servidor.
- Implementar listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red.
- Explicar cómo se implementan los cortafuegos para proporcionar seguridad en la red.
- Implementar un firewall basado en políticas de zona mediante la CLI.
- Recomendar requisitos de seguridad en la nube en función de un escenario de nube determinado.
- Determinar las técnicas criptográficas que se requieren para garantizar la confidencialidad, integridad y autenticidad.
- Explicar cómo las tecnologías de seguridad afectan a la monitorización de seguridad.
- Usar diferentes tipos de registros para almacenar información sobre los hosts y la red.
- Explicar el proceso de evaluación de alertas.
- 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 puntos finales.
- Seleccionar controles de seguridad en función de los resultados de la evaluación de riesgos.
- Utilizar modelos de respuesta a incidentes y técnicas forenses para investigar incidentes de seguridad.

Prerrequisitos del curso

Para un mayor aprovechamiento del curso, es recomendable que el alumno tenga conocimientos básicos de sistemas operativos Windows y/o Linux, conceptos básicos de programación y un nivel de conocimientos previos en redes equivalente a haber realizado CCNA v7.

Dirigido a:

El curso está dirigido de manera específica a profesionales IT (ingenieros de Networking, administradores de redes, etc.) que deseen iniciarse y profundizar en la temática de ciberseguridad y conocer los principales elementos representativos en el contexto de la seguridad, como la importancia de la protección de la información, su clasificación y la de los datos sensibles, así como conocer las aproximaciones de seguridad dirigidas a minimizar la exposición a ciberataques y a la protección de los activos de las organizaciones.

Esquema del curso

Module 1: Cybersecurity Threats, Vulnerabilities, and Attacks.

Module 2: Securing Networks.

Module 3: Attacking the Foundation.

Module 4: Attacking What We Do.

Module 5: Wireless Network Communication.

Module 6: Network Security Infrastructure.

Module 7: The Windows Operating System.

Module 8: Linux Overview.

Module 9: System and Endpoint Protection.

Module 10: Cybersecurity Principles, Practices, and Processes.

Module 11: Understanding Defense.

Module 12: System and Network Defense.

Module 13: Access Control.

Module 14: Access Control Lists.

Module 15: Firewall Technologies.

Module 16: Zone-Based Policy Firewalls.

Module 17: Cloud Security.

Module 18: Cryptography.

Module 19: Technologies and Protocols.

Module 20: Network Security Data.

Module 21: Evaluating Alerts.

Module 22: Governance and Compliance.

Module 23: Network Security Testing.

Module 24: Threat Intelligence.

Module 25: Endpoint Vulnerability Assessment.

Module 26: Risk Management and Security Controls.

Module 27: Digital Forensics and Incident Analysis and Response.