Cybersecurity

El candidato seleccionado tiene los conocimientos y las habilidades fundamentales necesarios para demostrar habilidades en ciberseguridad. Esta prueba será un punto de entrada al programa Cisco Certified. La siguiente certificación en este camino es la de **Cisco Certified Cyberops Associate.**

Los candidatos a este examen están comenzando su viaje en el campo de la ciberseguridad. Este examen evalúa su comprensión de los paradigmas, la terminología y la mentalidad de seguridad clave. Los candidatos seleccionados tendrán una gran conciencia de la importancia de la seguridad y las amenazas a una empresa cuando no se siguen los procedimientos de seguridad. Están dispuestos a enseñar a otros sobre cuestiones de seguridad.

Están desarrollando las habilidades de investigación e implementación necesarias para tener éxito en el campo y tienen aptitud y deseo de aprender más. Están familiarizados con el conjunto de herramientas a un nivel fundamental y pueden ayudar en la mitigación de amenazas y la respuesta a incidentes. Los candidatos seleccionados son técnicos calificados en ciberseguridad listos para trabajar con al menos 150 horas de instrucción y experiencia práctica.

Objetivos: CCST Cybersecurity

1. Principios esenciales de seguridad

1.1 Definir principios de seguridad esenciales

- Vulnerabilidades, amenazas, exploits y riesgos; vectores de ataque; endurecimiento; defensa en profundidad; confidencialidad, integridad y disponibilidad (CIA); tipos de atacantes; motivos de los ataques; código ético

1.2 Explicar amenazas y vulnerabilidades comunes

- Malware, ransomware, denegación de servicio, botnets, ataques de ingeniería social (tailgating, phishing, phishing, vishing, smishing, etc.), ataques físicos, intermediarios, vulnerabilidades de IoT, amenazas internas, amenaza persistente avanzada (APT)

1.3 Explicar los principios de gestión de acceso.

- Autenticación, autorización y contabilidad (AAA); RADIO; autenticación multifactor (MFA); políticas de contraseña

1.4 Explicar los métodos y aplicaciones de cifrado.

- Tipos de cifrado, hash, certificados, infraestructura de clave pública (PKI); algoritmos de cifrado fuertes versus débiles; estados de los datos y cifrado adecuado (datos en tránsito, datos en reposo, datos en uso); protocolos que utilizan cifrado

2. Conceptos básicos de seguridad de la red

2.1 Describir las vulnerabilidades del protocolo TCP/IP

- TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS

2.2 Explicar cómo las direcciones de red afectan la seguridad de la red.

- Direcciones IPv4 e IPv6, direcciones MAC, segmentación de red, notación CIDR, NAT, redes públicas versus privadas)

2.3 Describir la infraestructura y las tecnologías de la red.

- Arquitectura de seguridad de red, DMZ, virtualización, nube, honeypot, servidor proxy, IDS, IPS

2.4 Configurar una red SoHo inalámbrica segura

- Filtrado de direcciones MAC, estándares y protocolos de cifrado, SSID

2.5 Implementar tecnologías de acceso seguro

- ACL, cortafuegos, VPN, NAC

3. Conceptos de seguridad de terminales

3.1 Describir los conceptos de seguridad del sistema operativo

- Windows, macOS y Linux; funciones de seguridad, incluidos Windows Defender y firewalls basados en host; CLI y PowerShell; permisos de archivos y directorios; escalada de privilegios

3.2 Demostrar familiaridad con herramientas de punto final apropiadas que recopilan seguridad información de evaluación

- netstat, nslookup, tcpdump

3.3 Verificar que los sistemas de terminales cumplan con las políticas y estándares de seguridad

- Inventario de hardware (gestión de activos), inventario de software, implementación de programas, copias de seguridad de datos, cumplimiento normativo (PCI DSS, HIPAA, GDPR), BYOD (administración de dispositivos, cifrado de datos, distribución de aplicaciones, gestión de configuración)

3.4 Implementar actualizaciones de software y hardware

- Windows Update, actualizaciones de aplicaciones, controladores de dispositivos, firmware, parches

3.5 Interpretar los registros del sistema

- Visor de eventos, registros de auditoría, registros del sistema y de aplicaciones, syslog, identificación de anomalías

3.6 Demostrar familiaridad con la eliminación de malware

- Escaneo de sistemas, revisión de registros de escaneo, eliminación de malware

4. Evaluación de vulnerabilidad y gestión de riesgos

4.1 Explicar la gestión de vulnerabilidades.

- Identificación, gestión y mitigación de vulnerabilidades; reconocimiento activo y pasivo; pruebas (escaneo de puertos, automatización)

4.2 Utilice técnicas de inteligencia de amenazas para identificar redes potenciales vulnerabilidades

- Usos y limitaciones de las bases de datos de vulnerabilidades; herramientas estándar de la industria utilizadas para evaluar vulnerabilidades y hacer recomendaciones, políticas e informes; Vulnerabilidades y exposiciones comunes (CVE), informes de ciberseguridad, noticias de ciberseguridad, servicios de suscripción e inteligencia colectiva; inteligencia sobre amenazas ad hoc y automatizada; la importancia de actualizar la documentación y otras formas de comunicación de manera proactiva antes, durante y después de los incidentes de ciberseguridad; cómo proteger, compartir y actualizar la documentación

4.3 Explicar la gestión de riesgos

- Vulnerabilidad versus riesgo, clasificación de riesgos, enfoques para la gestión de riesgos, estrategias de mitigación de riesgos, niveles de riesgo (bajo, medio, alto, extremadamente alto), riesgos asociados con tipos específicos de datos y clasificaciones de datos, evaluaciones de seguridad de sistemas de TI (información seguridad, gestión de cambios, operaciones informáticas, aseguramiento de la información)

4.4 Explicar la importancia de la recuperación ante desastres y la continuidad del negocio.

planificación

- Desastres naturales y causados por el hombre, características de los planes de recuperación de desastres (DRP) y planes de continuidad del negocio (BCP), respaldo, controles de recuperación ante desastres (detectivos, preventivos y correctivos)

5. Manejo de incidentes

5.1 Monitorear eventos de seguridad y saber cuándo es necesario escalar

- Función de SIEM y SOAR, monitoreo de datos de red para identificar incidentes de seguridad (capturas de paquetes, varias entradas de archivos de registro, etc.), identificando eventos sospechosos a medida que ocurren.

5.2 Explicar la ciencia forense digital y los procesos de atribución de ataques

- Cyber Kill Chain, MITRE ATT&CK Matrix y Diamond Model; Táctica, Técnicas y Procedimientos (TTP); fuentes de evidencia (artefactos); manejo de evidencia (preservación de evidencia digital, cadena de custodia)

5.3 Explicar el impacto de los marcos de cumplimiento en el manejo de incidentes

- Marcos de cumplimiento (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), requisitos de informes y notificaciones.

5.4 Describir los elementos de respuesta a incidentes de ciberseguridad

- Elementos de políticas, planes y procedimientos; Etapas del ciclo de vida de respuesta a incidentes (Publicación especial del NIST 800-61, secciones 2.3, 3.1-3.4)