Cybersecurity

Los candidatos a este examen se están preparando para un trabajo como técnico de ciberseguridad de nivel básico o analista junior. Este examen evalúa su comprensión de los principios, marcos y mentalidades clave de seguridad. Los candidatos seleccionados tendrán una gran conciencia de cómo las vulnerabilidades exponen a una empresa a incidentes de seguridad y de cómo el cumplimiento de los principios de seguridad y la implementación de puntos de referencia pueden ayudar a mitigar el riesgo de ataque. Están desarrollando las habilidades de investigación e interpretación necesarias para tener éxito en el campo y tienen aptitud y deseo de aprender más. Están familiarizados con el conjunto de herramientas utilizado para monitorear un dispositivo terminal y una red en busca de indicaciones de un incidente y pueden analizar registros para determinar si debe ocurrir una escalada. Los candidatos deben tener al menos 150 horas.

de instrucción o experiencia práctica con ciberseguridad.

Antes de comenzar a estudiar para este examen, los candidatos deben tener experiencia en el uso de una computadora de escritorio, una computadora todo en uno o una computadora portátil como usuario final. Deben tener conocimientos generales de al menos un sistema operativo, estar familiarizados con la conexión a una red inalámbrica y con la configuración de una red doméstica sencilla. Deben tener buenas habilidades de pensamiento crítico y resolución de problemas, al menos un nivel de lectura de octavo grado y haber completado Álgebra I.

• Habilidades de lectura, escritura y comunicación de octavo grado • Álgebra 1
• Habilidades de
pensamiento crítico y resolución de problemas • Conocimiento
general del sistema operativo (Windows, MacOS, Linux) • Familiaridad con la conexión a una
red inalámbrica con programas comerciales comunes
componentes •
Familiaridad con la configuración de una red doméstica sencilla

1. Principios de seguridad

1.1 Explicar los principios de seguridad comunes.

- Endurecimiento; defensa en profundidad; confidencialidad, integridad y disponibilidad (CIA); código ético; Seguridad de confianza cero; privacidad (incluidos los casos de uso de IA); políticas de clasificación y retención de datos; gobernanza de la seguridad

1.2 Explicar los marcos de ciberseguridad y los mejores aceptados por la industria. practicas

- Marco de ciberseguridad del NIST, ISO/IEC 2700, seguridad crítica del CIS Control S

1.3 Explicar vulnerabilidades, amenazas y ataques comunes

- Vulnerabilidades, amenazas, exploits y riesgos; tipos de atacantes; razones para ataques; vectores de ataque
- Tipos de ataques: malware, fuerza bruta, ataques a sitios web y aplicaciones (inyección de SQL y desbordamiento de búfer), escalada de privilegios, ransomware, denegación de servicio/DDoS, botnets, ataques físicos, hombre en el medio, vulnerabilidades de IoT, amenazas internas, amenaza persistente avanzada (APT), suplantación de identidad

1.4 Reconocer ataques de ingeniería social

- Tailgating y suplantación de identidad •

Spear phishing, phishing, vishing, smishing, caza de ballenas, abrevaderos, pharming, etc.

- Redirección maliciosa (códigos QR, URL acortadas y sitios web falsos) • Mayor sofisticación

de los ataques debido al uso de IA y bots

1.5 Explicar los principios y procedimientos de gestión de acceso.

- Autenticación, autorización y contabilidad (AAA); RADIO; métodos de autenticación multifactor (MFA); políticas de contraseñas; autenticación biométrica; intercambio de recursos basado en la nube

1.6 Explicar cómo el cifrado protege la confidencialidad y la integridad. de datos

- Cifrado asimétrico y simétrico, hash; certificados; infraestructura de clave pública (PKI); algoritmos de cifrado fuertes versus débiles; cifrado utilizado para datos en tránsito, datos en reposo y datos en uso

2. Asegurar la red

2.1 Identificar vulnerabilidades asociadas con protocolos de uso común

- TCP, ARP, ICMP, DHCP, DNS, SMTP, ND, CDP/LLDP, SNMP, syslog • HTTP/HTTPS,

FTP/SFTP, Telnet/SSH

2.2 Describir el papel del direccionamiento en la seguridad de la red.

- Segmentación de red (DMZ, VLAN), • NAT; redes

públicas versus privadas; Redes internas, externas y confiables.

2.3 Describir el propósito y la función de las tecnologías de seguridad de red.

- Honeypot, servidor proxy, IDS, IPS, portal cautivo, tipos de firewalls (con estado, sin estado), ACL

- VPN, NAC, herramientas de escritorio remoto
- Infraestructura de seguridad en la nube (VPC y grupos de seguridad)

2.4 Validar la seguridad de las redes inalámbricas

- filtrado de direcciones MAC; estándares y protocolos de cifrado inalámbrico, SSID

2.5 Examinar los registros de seguridad de la red para identificar anomalías

- registros de firewall, registros IDS/IPS

3. Protección de dispositivos terminales

3.1 Aplicar configuraciones de seguridad para reforzar los sistemas operativos

- Sistemas operativos: Windows, macOS y Linux • Windows

Defender, permisos de archivos y directorios, escalada de privilegios, archivos y cifrado de unidades, utilizando puntos de referencia CIS

3.2 Utilice herramientas de punto final para recopilar información de evaluación de seguridad

- netstat, nslookup, nmap, zenmap, ss

3.3 Utilice utilidades de captura de paquetes para identificar anomalías

- Wireshark, tcpdump

3.4 Demostrar familiaridad con las políticas de seguridad de endpoints y estándares

- Cumplimiento normativo (PCI DSS, HIPAA, GDPR), BYOD, dispositivo administración (verificar el estado de las actualizaciones de Windows, actualizaciones de aplicaciones, controladores de dispositivos, firmware y parches), administración de configuración

3.5 Interpretar los registros del sistema para identificar anomalías

- Visor de eventos, consola, registros de auditoría, registros del sistema y de aplicaciones, syslog
- Dispositivos de servidor y de usuario final

3.6 Realizar eliminación de malware

- Escaneo de sistemas, revisión de registros de escaneo, eliminación de malware, comprensión de que el malware puede infectar puntos de restauración y copias de seguridad, respuesta a incidentes de malware (contención, cuarentena, tratamiento e inoculación)

4. Evaluación de vulnerabilidad y gestión de riesgos

4.1 Utilice fuentes de inteligencia sobre amenazas para identificar posibles vulnerabilidades de la red

- Usos y limitaciones de las bases de datos de vulnerabilidades; 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

4.2 Explicar la gestión de riesgos

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

4.3 Explicar el proceso de prueba de penetración.

- Identificación de vulnerabilidades, presentación de informes de resultados a las partes interesadas y toma de decisiones. recomendaciones de mitigación; reconocimiento activo y pasivo; pruebas (escaneo de puertos y automatización);

5. Manejo de incidentes

5.1 Supervisar los eventos de seguridad para determinar si se requiere una escalada

- Papel de SIEM y SOAR, identificando eventos sospechosos a medida que ocurren, diferenciar entre un verdadero o falso positivo, diferenciar entre un verdadero o falso negativo

5.2 Explicar el proceso de análisis forense digital y los marcos de ataque.

- Fuentes de evidencia (artefactos); Manejo de evidencia (preservación de datos digitales). evidencia, cadena de custodia)
- Cyber Kill Chain, matriz MITRE ATT&CK, modelo Diamond; Táctica, Técnicas y Procedimientos (TTP); Pirámide del dolor

5.3 Explicar 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)
- Impacto de los marcos de cumplimiento (GDPR, HIPAA, PCI-DSS, FERPA, FISMA) sobre los requisitos de notificación y presentación de informes

5.4 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), todo tipo de copias de seguridad de datos, repuestos en caliente y en frío, controles de recuperación ante desastres (detectivos, preventivos y correctivos)

5.5 Ayudar a los usuarios a restaurar datos después de un incidente

- Puntos de restauración, restauración desde almacenamiento en la nube

INFORMATION TECHNOLOGY SPECIALIST

pue | academy