CompTIA

Cybersecurity Analyst+ (CySA+)

CompTIA Cybersecurity Analyst (CySA+) es la certificación líder para profesionales de ciberseguridad encargados de la detección, prevención y respuesta a incidentes mediante la monitorización continua de la seguridad. Valida la experiencia de un profesional tecnológico en procesos de respuesta a incidentes y gestión de vulnerabilidades, haciendo hincapié en las habilidades de comunicación esenciales para un análisis de seguridad eficaz y el cumplimiento normativo.

Resumen del curso

Operaciones de seguridad (33%)

- **Arquitectura de sistemas y redes:** explicación de la ingestión de registros, conceptos de sistema operativo (SO), infraestructura, arquitectura de red, gestión de identidad y acceso (IAM), cifrado y protección de datos confidenciales.
- **Indicadores de actividad maliciosa:** análisis de anomalías de la red como picos de ancho de banda y dispositivos fraudulentos, problemas de host como software no autorizado y exfiltración de datos, irregularidades en las aplicaciones como interrupciones inesperadas de la comunicación y el servicio, y amenazas como ataques de ingeniería social.
- **Herramientas y técnicas:** detección de actividad maliciosa mediante herramientas como Wireshark, gestión de eventos e información de seguridad (SIEM) y VirusTotal, junto con técnicas como reconocimiento de patrones y análisis de correo electrónico, respaldadas por lenguajes de scripting como Python y PowerShell.
- **Inteligencia y búsqueda de amenazas:** comparación de actores de amenazas, tácticas, técnicas y procedimientos (TTP); niveles de confianza; métodos de recopilación; intercambio de inteligencia; y técnicas de búsqueda.
- **Mejora de procesos:** estandarizar procesos, agilizar operaciones, integrar herramientas y utilizar un único panel de control.

Gestión de vulnerabilidades (30%)

- **Escaneo de vulnerabilidades:** implementación de descubrimiento de activos, escaneo interno vs. externo, con agente vs. sin agente, con credenciales vs. sin credenciales, pasivo vs. activo, estático vs. dinámico y escaneo de infraestructura crítica.
- **Resultados de la herramienta de evaluación:** análisis de escaneo de red, escáneres de aplicaciones web, escáneres de vulnerabilidad, depuradores, herramientas multipropósito y evaluaciones de infraestructura en la nube.
- **Priorización de vulnerabilidades:** interpretación del sistema común de puntuación de vulnerabilidades (CVSS), validación de hallazgos, evaluación de la explotabilidad y consideración del valor de los activos y las vulnerabilidades de día cero.
- **Controles de mitigación:** recomendación de controles para secuencias de comandos entre sitios (XSS), vulnerabilidades de desbordamiento y envenenamiento de datos.
- **Respuesta a la vulnerabilidad:** explicación de controles de compensación, parches, gestión de configuración, ventanas de mantenimiento, excepciones, gobernanza, objetivos de nivel de servicio (SLO), ciclo de vida de desarrollo de software seguro (SDLC) y modelado de amenazas.

Gestión de respuesta a incidentes (20%)

- **Marcos de metodología de ataque:** explicación de las cadenas de ataque cibernéticas, modelo de diamante de análisis de intrusiones, MITRE ATT&CK, Manual de metodología de pruebas de seguridad de código abierto (OSSTMM) y guía de pruebas OWASP.
- **Actividades de respuesta a incidentes:** realizar detección, análisis, contención, erradicación y recuperación.
- **Ciclo de vida de la gestión de incidentes:** explicación de los planes de respuesta a incidentes, herramientas, manuales, ejercicios de mesa, capacitación, continuidad del negocio (BC), recuperación ante desastres (DR), análisis forense y análisis de causa raíz.

Informes y comunicación (17%)

- **Informes de gestión de vulnerabilidades:** explicación de informes de cumplimiento, planes de acción, inhibidores de la remediación, métricas, indicadores clave de rendimiento (KPI) y comunicación con las partes interesadas.
- **Informes de respuesta a incidentes:** explicación de la declaración de incidentes, la escalada, los informes, la comunicación, el análisis de la causa raíz, las lecciones aprendidas y las métricas y los KPI.

Habilidades que aprenderás

Desarrolle habilidades con la capacitación de CompTIA y valídelas con la certificación CySA+.

- Mejore los procesos de operaciones de seguridad, diferencie la inteligencia de amenazas y la búsqueda de amenazas e identifique la actividad maliciosa utilizando herramientas adecuadas.
- Realizar evaluaciones de vulnerabilidad, priorizar las vulnerabilidades y recomendar estrategias de mitigación efectivas para la gestión de vulnerabilidades.
- Aplicar marcos de metodología de ataque, realizar respuestas a incidentes y comprender el ciclo de vida de la gestión de incidentes para manejar incidentes de seguridad de manera eficaz.
- Utilice las mejores prácticas de comunicación para informar sobre la gestión de vulnerabilidades y la respuesta a incidentes, proporcionando a las partes interesadas planes viables y métricas significativas.