Certified SOC Analyst (CSA)

Código: CSA-001

Propuesta de Valor: EC-COUNCIL

Duración: 24 Horas

El programa Certified SOC Analyst (CSA) es el primer paso para unirse a un centro de operaciones de seguridad (SOC). Está diseñado para que los analistas SOC de Nivel I y Nivel II actuales y aspirantes logren la competencia en la realización de operaciones de nivel de entrada e intermedio.
CSA es un programa de capacitación y acreditación que ayuda al candidato a adquirir habilidades técnicas de tendencia y demanda a través de la instrucción de algunos de los capacitadores más experimentados de la industria.

El programa se centra en la creación de nuevas oportunidades profesionales a través de un conocimiento extenso y meticuloso con capacidades de nivel mejoradas para contribuir dinámicamente a un equipo SOC.
Al ser un programa intenso de 3 días, cubre a fondo los fundamentos de las operaciones de SOC, antes de transmitir el conocimiento de la gestión y correlación de registros, la implementación de SIEM, la detección avanzada de incidentes y la respuesta a incidentes. Además, el candidato aprenderá a gestionar varios procesos de SOC y colaborará con CSIRT en el momento de necesidad.

AUDIENCIA

- Analistas de SOC (Nivel I y Nivel II).
- Administradores de redes y seguridad, ingenieros de redes y seguridad, analistas de defensa de redes, técnicos de defensa de redes, especialistas en seguridad de redes, operadores de seguridad de redes y cualquier profesional de seguridad que maneje operaciones de seguridad de redes.
- Analista de ciberseguridad.
- Profesionales de ciberseguridad de nivel de entrada.
- Cualquiera que quiera convertirse en analista de SOC.

PRE REQUISITOS

- Tener conocimiento de redes y seguridad.

OBJETIVOS

- Obtenga conocimiento de los procesos, procedimientos, tecnologías y flujos de trabajo de SOC.
- Obtenga una comprensión básica y un conocimiento profundo de las amenazas de seguridad, ataques, vulnerabilidades, comportamientos de los atacantes, cyber killchain, etc.

- Capaz de reconocer las herramientas, tácticas y procedimientos de los atacantes para identificar indicadores de compromiso (IOC) que se pueden utilizar durante las investigaciones activas y futuras.
- Capaz de monitorear y analizar registros y alertas de una variedad de tecnologías diferentes en múltiples plataformas (IDS / IPS, protección de punto final, servidores y estaciones de trabajo).
- Adquiera conocimientos sobre el proceso de gestión centralizada de registros (CLM).
- Capaz de realizar eventos de seguridad y recopilar, monitorear y analizar registros.
- Adquiera experiencia y amplios conocimientos sobre seguridad de la información y gestión de eventos.
- Obtenga conocimientos sobre la administración de soluciones SIEM (Splunk / AlienVault / OSSIM / ELK).
- Comprender la arquitectura, la implementación y el ajuste de las soluciones SIEM (Splunk / AlienVault / OSSIM / ELK).
- Obtenga experiencia práctica en el proceso de desarrollo de casos de uso de SIEM.

CERTIFICACIÓN DISPONIBLE

- Después de completar la capacitación de CSA, los candidatos estarán listos para realizar el examen 312-39 ANALISTA CERTIFICADO DE SOC (CSA).

CONTENIDO

1. GESTIÓN Y OPERACIONES DE SEGURIDAD

2. COMPRENSIÓN DE LAS AMENAZAS CIBERNÉTICAS, LAS IOC Y LOS ATAQUES METODOLOGÍA

3. INCIDENTES, EVENTOS Y REGISTRO

4. DETECCIÓN DE INCIDENTES CON INFORMACIÓN DE SEGURIDAD Y GESTIÓN DE EVENTOS (SIEM)

5. DETECCIÓN DE INCIDENTES MEJORADA CON AMENAZAS INTELIGENCIA

6. RESPUESTA AL INCIDENTE

BENEFICIOS

- Conocerá Certified SOC Analyst y perfeccionará soluciones avanzadas de ciberseguridad.