EC-Council Certified SOC Analyst (C|CSA) + Exam voucher

Duración: 3 Días Código del Curso: EC-CSA Version: 1.0

Temario:

El programa de Certified SOC Analyst (CSA) es el primer paso para poder formar parte de un centro de operaciones de seguridad (SOC). Está diseñado para que los actuales y futuros analistas SOC de nivel I y II alcancen la competencia para realizar operaciones de nivel básico e intermedio.
El CSA es un programa de formación y certificación que ayuda al candidato a adquirir habilidades técnicas altamente demandadas a través de la formación. El programa se centra en la creación de nuevas oportunidades de carrera a través de un conocimiento extenso y meticuloso con capacidades de nivel mejoradas para contribuir de forma dinámica a un equipo SOC. Siendo un programa intenso de 3 días, cubre a fondo los fundamentos de las operaciones del SOC, además de transmitir los conocimientos de gestión y correlación de registros, despliegue de SIEM, detección avanzada de incidentes y respuesta a incidentes. Además, el candidato aprenderá a gestionar varios procesos SOC y a colaborar con el CSIRT en el momento que lo necesite.
Esta es la formación recomendada para aquellos estudiantes que buscan alcanzar la certificación de analista SOC certificado por el EC-Council

Dirigido a:

Analistas SOC (Tier I y Tier II), Analistas de Ciberseguridad, Profesionales de la ciberseguridad de nivel básico. Administradores de redes y seguridad

Objetivos:

- **Tras este curso, los profesionales podrán:**
- Articular los procesos, procedimientos, tecnologías y flujos de trabajo del SOC.
- Entender y las amenazas de seguridad, ataques, vulnerabilidades, comportamientos de los atacantes, cadena de muerte cibernética, etc.
- Reconocer las herramientas, tácticas y procedimientos de los atacantes para identificar los indicadores de compromiso (SOC) que pueden ser utilizados durante las investigaciones activas y futuras.
- Supervisar y analizar registros y alertas de una variedad de tecnologías diferentes a través de múltiples plataformas (IDS/IPS, protección de puntos finales, servidores y estaciones de trabajo).
- Aplicar procesos de gestión centralizada de registros (CLM).
- Realizar eventos de seguridad y recolección, monitoreo y análisis de registros.
- Comprender la información de seguridad y la gestión de eventos.
- Administrar soluciones SIEM (Splunk/AlienVault/OSSIM/ELK).
- Entender la arquitectura, implementación y ajuste fino de las soluciones SIEM (Splunk/ AlienVault/OSSIM/ELK).
- Obtener experiencia práctica en el proceso de desarrollo de casos de uso de SIEM.
- Desarrollar casos de amenaza (reglas de correlación), crear
- Reconocer los casos de uso que se utilizan ampliamente en todo el despliegue del SIEM.
- Planificar, organizar y llevar a cabo la supervisión y el análisis de las amenazas en la empresa.
- Monitorear los patrones de amenazas emergentes y realizar análisis de amenazas a la seguridad.
- Obtener experiencia práctica en el proceso de triaje de alertas.
- Escalar los incidentes a los equipos apropiados para obtener asistencia adicional.
- Usar un sistema de tickets del Service Desk.
- Preparar sesiones informativas e informes de la metodología de análisis y los resultados.
- Integrar la inteligencia de amenazas en el SIEM para mejorar la detección de incidentes y la respuesta.
- Hacer uso de información sobre amenazas variada, dispareja y en constante cambio.
- Articular el conocimiento del proceso de respuesta a incidentes.
- Comprender la colaboración entre el SOC y la TRI para una mejor respuesta a los incidentes

informes, etc.

Prerequisitos:

Para este curso, es recomendable tener conocimiento en:

- Administración de redes o seguridad de dominios

Exámenes y certificación

312-39 - Certified SOC Analyst

El programa CSA requiere que el candidato tenga un año de experiencia laboral en el dominio de la administración de redes/seguridad y debe poder aportar pruebas de la misma validadas a través del proceso de solicitud, a menos que el candidato asista a una formación oficial.

Contenido:

SOC: conceptos esenciales

- Gestión de la seguridad
- Operaciones de seguridad
- Centro de Operaciones de Seguridad (SOC)
- Necesidad de SOC
- Capacidades del SOC
- Operaciones del SOC
- Flujo de trabajo del SOC
- Componentes de SOC: Personas, procesos y tecnología
- Gente
- Tecnología
- Procesos
- Tipos de modelos SOC
- Modelos de madurez SOC
- Generaciones SOC
- Implementación del SOC
- Indicadores clave de rendimiento del SOC
- Desafíos en la aplicación del SOC
- Mejores prácticas para el funcionamiento del SOC
- SOC vs NOC
- Comprensión de las amenazas cibernéticas, los IO y la metodología de ataque

Amenazas Cibernéticas

- Intención-Motivo-Goal
- Táctica-Técnica-Procedimientos (TTP)
- Oportunidad-Vulnerabilidad-Debilidad
- Ataques a nivel de red
- Ataques a nivel de anfitrión
- Ataques a nivel de aplicación
- Amenazas a la seguridad del correo electrónico
- Comprensión de los indicadores de compromiso
- Entendiendo la metodología de ataque del atacante
- Incidentes, eventos y registro

Incidente

- Evento
- Bitácora
- Fuentes de registro típicas
- Necesidad de registro
- Requisitos de registro
- Formato de registro típico
- Registro de enfoques
- La tala de árboles local
- Registro centralizado
- Detección de Incidentes con Información de Seguridad y Gestión de Eventos (SIEM)

Información de Seguridad y Gestión de Eventos (SIEM)

- Análisis de seguridad
- Necesidad del SIEM
- Capacidades típicas del SIEM
- La arquitectura del SIEM y sus

Paso 1: Preparación para la respuesta al incidente

Paso 2: Registro y asignación de incidentes

Paso 3: Triaje de incidentes

Paso 4: Notificación

Paso 5: Contención

Paso 6: Recopilación de pruebas y análisis forense

Paso 7: Erradicación

Paso 8: Recuperación

Paso 9: Actividades posteriores al incidente

- Respuesta a los incidentes de seguridad de la red
- Respuesta a los incidentes de seguridad de las aplicaciones
- Responder a los incidentes de seguridad del correo electrónico
- Respuesta a los incidentes con información privilegiada
- Respuesta a los incidentes de malware

componentes
- Soluciones SIEM
- Despliegue del SIEM
- Detección de incidentes con el SIEM
- Ejemplos de casos de uso común en todos los despliegues del SIEM
- Manejo del rastreo y análisis de alertas
- Detección de incidentes mejorada con inteligencia de amenazas
- Entendiendo la inteligencia de la amenaza cibernética
- ¿Por qué amenazar el SOC impulsado por la inteligencia?

Respuesta a incidentes

- Equipo de respuesta a incidentes (IRT)
- ¿Dónde encaja la TRI en la organización
- Colaboración del SOC y el IRT
- Resumen del proceso de respuesta a incidentes (IR)

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid