EC-Council

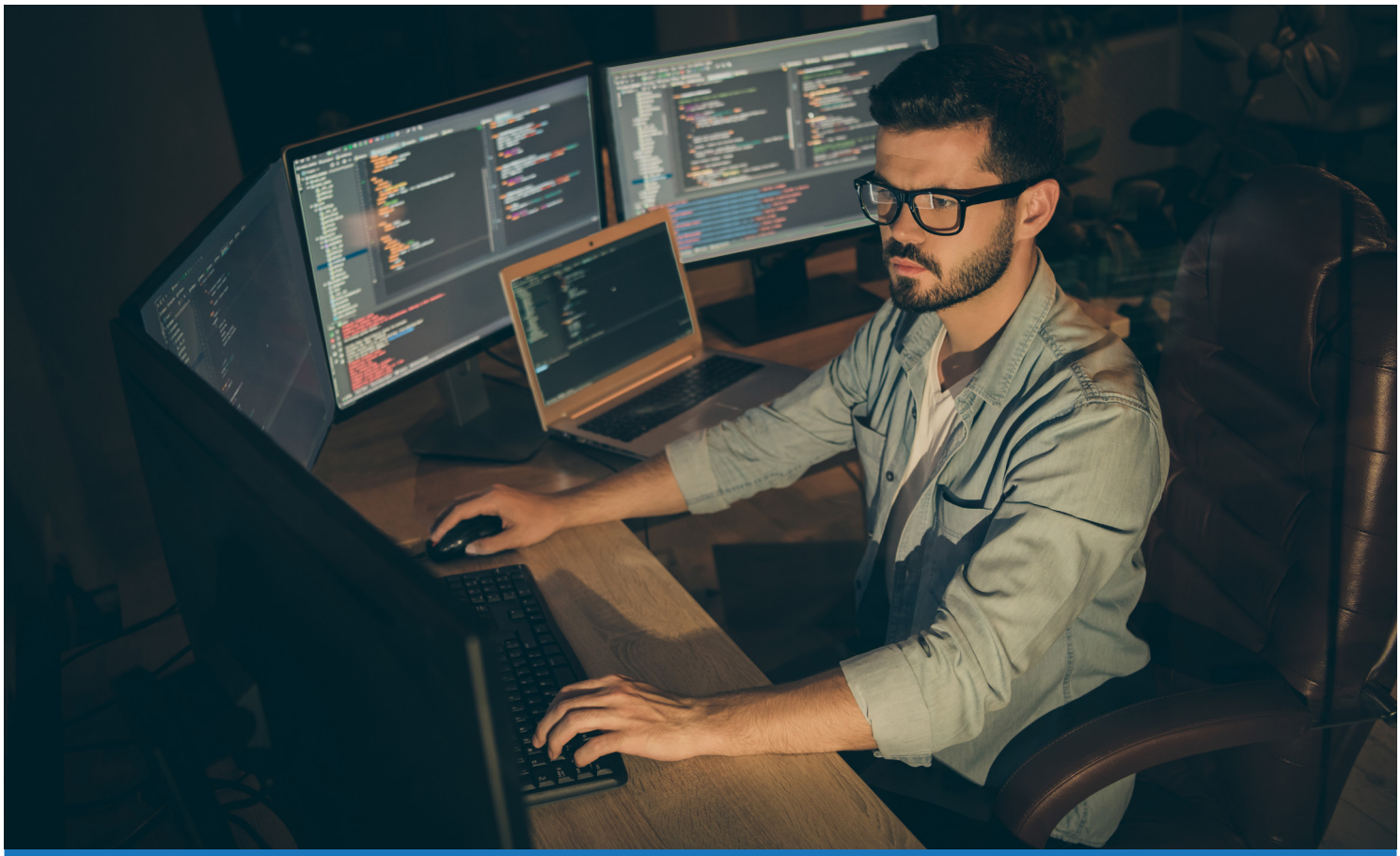
EC-Council
Certified SOC Analyst

El único entrenamiento desarrollado específicamente para Analistas de SOC

Descripción del curso

El programa Certified SOC Analyst (CSA) es el primer paso para unirse a un centro de operaciones de seguridad (SOC). Está diseñado para los actuales y aspirantes Analistas de SOC de Nivel I y Nivel II para lograr competencia en la realización de operaciones de nivel básico e intermedio.

CSA es un programa de capacitación y acreditación que ayuda al candidato adquirir habilidades técnicas de tendencia y demanda a través de la instrucción por algunos de los entrenadores más experimentados de la industria. El programa se enfoca en crear nuevas oportunidades profesionales a través de conocimiento meticuloso con capacidades de nivel mejoradas para
contribuyendo dinámicamente a un equipo SOC. Siendo un intenso día 3 programa, cubre a fondo los fundamentos de las operaciones SOC, antes de transmitir el conocimiento de la gestión de registros y correlación, despliegue SIEM, detección avanzada de incidentes, y respuesta a incidentes. Además, el candidato aprender a gestionar varios procesos SOC y colaborar con CSIRT en el momento de necesidad.



¿Quién debería asistir?

- 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 básico
- Cualquiera que quiera convertirse en analista de SOC

Agenda del curso

Duración: 24 horas

Día 1

- Gestión y Operaciones de Seguridad
- Entendiendo la Ciber Amenazas, Indicadores de Compromiso, y Metodologías de Ataque

Día 2

- Eventos, Incidentes y Registro
- Detección de Incidentes con Gestión de Eventos e Incidentes de Seguridad (SIEM)

Día 3

- Mejora a la Detección de Incidentes con la Inteligencia de Amenazas
- Respuesta a Incidentes

SAVANT CONSULTORES

EC-Council

809-363-1162 | cursos@savant.com.do | www.savant.com.do

Security information and event management

Objetivos de aprendizaje

- Obtenga conocimiento de los procesos, procedimientos, tecnologías y flujos de trabajo de SOC.
- Obtenga una comprensión básica y un conocimiento profundo de amenazas de seguridad, ataques,
- Vulnerabilidades, comportamientos del atacante, cadena de asesinato cibernético, etc.
- Capaz de reconocer las herramientas, tácticas y procedimientos del atacante para identificar indicadores de
- Compromiso (IOC) que se puede utilizar durante 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).
- Adquirir conocimientos sobre el proceso de gestión centralizada de registros (CLM).
- Capaz de realizar eventos de seguridad y recopilación, monitoreo y análisis de registros.
- Adquiera experiencia y amplio conocimiento de información y eventos de seguridad
- Administración.
- Obtenga conocimiento sobre la administración de soluciones SIEM (Splunk / AlienVault / OSSIM / ELK).
- Comprender la arquitectura, implementación y ajuste de las soluciones SIEM (Splunk /
- AlienVault / OSSIM / ELK).
- Obtenga experiencia práctica en el proceso de desarrollo de casos de uso de SIEM.
- Capaz de desarrollar casos de amenazas (reglas de correlación), crear informes, etc.
- Conozca los casos de uso ampliamente utilizados en la implementación de SIEM.
- Planifique, organice y realice monitoreo y análisis de amenazas en la empresa.
- Capaz de monitorear patrones de amenazas emergentes y realizar análisis de amenazas de seguridad.
- Obtenga experiencia práctica en el proceso de selección de alertas.
- Capaz de escalar incidentes a los equipos apropiados para obtener asistencia adicional.
- Capaz de utilizar un sistema de tickets de la mesa de servicio.
- Capaz de preparar informes e informes de metodología de análisis y resultados.
- Obtenga conocimiento sobre la integración de inteligencia de amenazas en SIEM para mejorar el incidente
- Detección y respuesta.
- Capaz de utilizar información de amenazas variada, dispareja y en constante cambio.
- Obtener conocimiento del proceso de respuesta a incidentes.
- Obtenga conocimiento de la colaboración entre SOC e IRT para una mejor respuesta a incidentes.

SAVANT CONSULTORES

EC-Council

Examen

Duración: 3 horas

Nombre del examen: Certified SOC Analyst
Código del examen: 312-39
Cantidad de preguntas: 100
Formato: Selección múltiple
Disponibilidad: EC-Council Exam Portal
Puntuación para pasar: 70%

Certificación

El examen **CSA** puede ser tomado después de finalizar la aistencia al curso oficial completo de **CSA**.
Los candidatos que pasan con éxito el examen recibirá su certificado **CSA** y los privilegios de membresía.
Se espera que los miembros se adhieran a los requisitos de recertificación a través de los requisitos de Educación Continua.

Información general

- El costo del curso oficial incluye el voucher para tomar el examen
- Courseware digital con más de 600 páginas repletas de contenido organizado metodológicamente
- Acceso al portal Aspen.eccouncil.org donde puede acceder miles de herramientas
- Subscripción por seis meses a los laboratorios virtuales para mayor comodidad con más de 50 laboratorios

EC-Council Accredited Training Center

C|SA Certified SOC Analyst

C|EI Certified EC-Council Instructor

SAVANT CONSULTORES

EC-Council

809-363-1162 | cursos@savant.com.do | www.savant.com.do