



EC-Council

CSA
Certified SOC Analyst

ANALISTA DE CENTRO DE OPERACIONES DE SEGURIDAD CERTIFICADO (CSA)

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 analistas de SOC de Nivel I y Nivel II actuales y aspirantes, para lograr la competencia en la realización de operaciones de nivel de entrada e intermedio.

CSA es un programa de capacitación y certificación que ayuda al candidato a adquirir habilidades técnicas en tendencia y demanda a través de la instrucción de algunos de los entrenadores más experimentados de la industria. El programa se enfoca en crear nuevas oportunidades de carrera a través de un conocimiento extenso y meticuloso con capacidades mejoradas para contribuir dinámicamente a un equipo de SOC. Siendo un programa intensivo de 3 días, cubre a fondo los fundamentos de las operaciones de SOC, antes de transmitir el conocimiento de gestión y correlación de registros, implementación de SIEM, detección avanzada de incidentes y respuesta a incidentes. Además, el candidato aprenderá a gestionar varios procesos de SOC y a colaborar con CSIRT en momentos de necesidad.



La Asociación Nacional de Directores de Tecnología de la Información de los Estados (NASCIO), que representa a las Oficinas de Información del Jefe de los Estados, reveló en una encuesta de más de un año (julio de 2016 a diciembre de 2017), que "desde la creación del Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés), la división de seguridad ha experimentado una disminución general del 64 por ciento en el tiempo de respuesta a incidentes".

“ Casi 6 de cada 10 proveedores de servicios financieros tienen un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés). ”

– Encuesta Global de Seguridad de la Información de EY 2018–19.

A medida que el panorama de seguridad se expande, un equipo de Centro de Operaciones de Seguridad (SOC) ofrece servicios de alta calidad en seguridad informática para detectar activamente posibles amenazas/ataques cibernéticos y responder rápidamente a incidentes de seguridad. Las organizaciones necesitan analistas de SOC capacitados que puedan servir como defensores de primera línea, advirtiendo a otros profesionales sobre las amenazas cibernéticas emergentes y presentes.

El programa CSA, intensivo en laboratorio, enfatiza el enfoque holístico para brindar conocimientos elementales y avanzados sobre cómo identificar y validar intentos de intrusión. A través de esto, el candidato aprenderá a utilizar soluciones de SIEM y capacidades predictivas utilizando inteligencia de amenazas. El programa también introduce el aspecto práctico del SIEM utilizando herramientas avanzadas y las más utilizadas con frecuencia. El candidato aprenderá a realizar una detección avanzada de amenazas utilizando las capacidades predictivas de Inteligencia de Amenazas.

En los últimos años, se ha presenciado la evolución de los riesgos cibernéticos, creando un entorno inseguro para los jugadores de diversos sectores. Para enfrentar estas amenazas sofisticadas, las empresas necesitan soluciones avanzadas de ciberseguridad junto con métodos tradicionales de defensa. Practicar una buena higiene de ciberseguridad, implementar una línea de defensa adecuada e incorporar un Centro de Operaciones de Seguridad (SOC) se ha convertido en soluciones razonables. El equipo busca una cobertura de veinticuatro horas y "seguir el sol" para llevar a cabo la monitorización de seguridad, la gestión de incidentes de seguridad, la gestión de vulnerabilidades, la gestión de dispositivos de seguridad y la monitorización del flujo de red. Un analista de SOC monitorea y detecta continuamente posibles amenazas, clasifica las alertas y las escalas adecuadamente. Sin un analista de SOC, los procesos de monitorización, detección, análisis y clasificación perderán su efectividad, lo que afectará negativamente a la organización.



Público Objetivo

- *Analistas de SOC (Nivel I y Nivel II)*
- *Administradores de Red y Seguridad, Ingenieros de Red y Seguridad, Analistas de Defensa de Red, Técnicos de Defensa de Red, Especialistas en Seguridad de Red, Operadores de Seguridad de Red y cualquier profesional de seguridad que maneje operaciones de seguridad de red*
- *Analistas de Ciberseguridad*
- *Profesionales de ciberseguridad de nivel inicial*
- *Cualquier persona que desee convertirse en Analista de SOC.*



Duración Sugerida

- 3 días (9 am – 5 pm)
- Mínimo de 24 horas

Certificación

Después de completar el entrenamiento CSA, los candidatos estarán listos para realizar el examen Certified SOC Analyst. Al completar con éxito el examen, con una puntuación de al menos el 70%, el candidato obtendrá el certificado CSA y los privilegios de membresía. Se espera que los miembros cumplan con los requisitos de recertificación a través de los Requisitos de Educación Continua de EC-Council.



Detalles del examen

El examen CSA está diseñado para evaluar y validar la comprensión integral del candidato de las tareas laborales requeridas como analista de SOC, validando así su comprensión completa de un flujo de trabajo completo de SOC.

Título del Examen	Certified SOC Analyst
Código del Examen	312-39
Número de Preguntas	100
Duración	3 horas
Disponibilidad	Portal de Exámenes de EC-Council (por favor visite https://www.ecexam.com)
Formato del Examen	Opción Múltiple
Puntaje de Aprobación	70%

El requisito de elegibilidad para el examen

El programa CSA requiere que el candidato tenga al menos 1 año de experiencia laboral en el dominio de Administración de Redes/Seguridad y pueda proporcionar pruebas de ello validadas a través del proceso de solicitud, a menos que el candidato asista a una capacitación oficial.

Los "8 Componentes Críticos de CSA"

1. Cumplimiento del 100% con el Marco NICE 2.0:

CSA se ajusta al 100% al Marco Nacional de Iniciativas para la Educación en Ciberseguridad (NICE) en la categoría de "Proteger y Defender (PR)" para el rol de Análisis de Defensa Cibernética (CDA). Está diseñado según los roles y responsabilidades en tiempo real de un analista de SOC. El curso de CSA capacita al candidato para utilizar diversas medidas defensivas y datos recolectados de múltiples fuentes para identificar, analizar e informar eventos que puedan ocurrir o que ya estén presentes en la red, con el objetivo de proteger datos, sistemas y redes de amenazas.

2. Enfatiza en el flujo de trabajo completo del SOC:

CSA ofrece una comprensión completa del flujo de trabajo del SOC, incluyendo todos los procedimientos, tecnologías y procesos utilizados para recolectar, clasificar, informar, responder y documentar incidentes.

3. Aprendizaje de detección de incidentes con SIEM:

Capacitación en diversos casos de uso de soluciones SIEM (Gestión de Información y Eventos de Seguridad) para detectar incidentes mediante tecnologías de detección basadas en firmas y anomalías. Los candidatos aprenderán a detectar incidentes en diferentes niveles: nivel de aplicación, nivel interno, nivel de red y nivel de host.

4. Mejora en la detección de incidentes con Inteligencia de Amenazas:

CSA incluye un módulo dedicado a la detección rápida de incidentes con Inteligencia de Amenazas. Este módulo también proporciona conocimientos sobre cómo integrar feeds de Inteligencia de Amenazas en SIEM para mejorar la detección de amenazas.

5. Comprensión detallada de la implementación de SIEM:

CSA cubre 45 casos de uso detallados que son ampliamente utilizados en todas las implementaciones de SIEM.

6. Promueve el aprendizaje práctico:

CSA es un programa práctico que ofrece experiencia práctica en la monitorización, detección, clasificación y análisis de incidentes de seguridad. También abarca la contención, erradicación, recuperación e informe de incidentes de seguridad. Para ello, se incluyen 80 herramientas en la capacitación.

7. Entorno de laboratorio que simula un entorno en tiempo real:

El programa CSA cuenta con 22 laboratorios en total, que demuestran procesos alineados con el flujo de trabajo del SOC. Estos incluyen, pero no se limitan a, actividades como:

- Modus operandi de diferentes tipos de ataques a nivel de aplicación, red y host para comprender sus indicadores de compromiso (IOCs).
- Funcionamiento de los conceptos de registro local y centralizado que demuestra cómo se extraen los registros de los diferentes dispositivos en la red para facilitar la monitorización, detección y análisis de incidentes.
- Ejemplos de desarrollo de casos de uso de SIEM para detectar incidentes a nivel de aplicación, red y host utilizando varias herramientas de SIEM.
- Clasificación rápida de alertas para proporcionar detección y respuesta rápida a incidentes.
- Priorización y escalado de incidentes mediante la generación de tickets de incidentes.
- Contención de incidentes
- La erradicación de incidentes.
- La recuperación de los incidentes.
- Creación de informes de los incidentes

8. Aprender más con Material de Referencia Adicional:

El programa CSA incluye material de referencia adicional, que incluye una lista de 291 casos de uso comunes y específicos para implementaciones de SIEM de ArcSight, Qradar, LogRhythm y Splunk.

Esquema del Curso

Módulo 1

Operaciones y Gestión de Seguridad

Módulo 2

Comprender las Amenazas Cibernéticas, Indicadores de Compromiso (IoCs) y Metodología de Ataque

Módulo 3

Incidentes, Eventos y Registros

Módulo 4

Detección de Incidentes con Gestión de Información y Eventos de Seguridad (SIEM)

Módulo 5

Detección Mejorada de Incidentes con Inteligencia de Amenazas

Módulo 6

Respuesta a Incidentes

Objetivos de aprendizaje del programa CSA

- ▯ Obtener conocimiento sobre los procesos, procedimientos, tecnologías y flujos de trabajo de un SOC.
- ▯ Adquirir una comprensión básica y en profundidad de las amenazas de seguridad, ataques, vulnerabilidades, comportamientos de los atacantes, cadena de ataque cibernético, etc.
- ▯ Ser capaz de reconocer herramientas, tácticas y procedimientos de los atacantes para identificar indicadores de compromiso (IOCs) que puedan utilizarse en investigaciones activas y futuras.
- ▯ Ser capaz de monitorear y analizar registros y alertas de una variedad de tecnologías en múltiples plataformas (IDS/IPS, protección de endpoints, servidores y estaciones de trabajo).
- ▯ Obtener conocimiento del proceso de Gestión Centralizada de Registros (CLM, por sus siglas en inglés).
- ▯ Ser capaz de realizar la recolección, monitoreo y análisis de eventos y registros de seguridad.
- ▯ Adquirir experiencia y amplio conocimiento de la Gestión de Información y Eventos de Seguridad (SIEM, por sus siglas en inglés).
- ▯ Obtener conocimiento sobre la administración de soluciones SIEM (Splunk/AlienVault/OSSIM/ELK).
- ▯ Comprender 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.
- ▯ Ser capaz de desarrollar casos de amenazas (reglas de correlación), crear informes, etc.
- ▯ Aprender casos de uso ampliamente utilizados en la implementación de SIEM.
- ▯ Planificar, organizar y realizar el monitoreo y análisis de amenazas en la empresa.
- ▯ Ser capaz de monitorear patrones emergentes de amenazas y realizar análisis de amenazas de seguridad.
- ▯ Obtener experiencia práctica en el proceso de triaje de alertas.
- ▯ Ser capaz de escalar incidentes a equipos apropiados para obtener asistencia adicional.
- ▯ Ser capaz de utilizar un sistema de gestión de tickets de Servicio de Mesa de Ayuda (Service Desk).
- ▯ Ser capaz de preparar informes y resúmenes de la metodología y resultados de análisis.
- ▯ Obtener conocimiento sobre la integración de inteligencia de amenazas en SIEM para mejorar la detección y respuesta a incidentes.
- ▯ Ser capaz de utilizar información de amenazas variadas, dispares y en constante cambio.
- ▯ Obtener conocimiento del proceso de Respuesta a Incidentes.
- ▯ Obtener comprensión de la colaboración entre SOC e IRT para una mejor respuesta a incidentes.

“

Siento firmemente que este programa proporciona las habilidades necesarias para un rol de Analista de SOC en los niveles L1 y L2. Además, creo que este programa nos ayudará a mejorar las habilidades de nuestro equipo de SOC. Este curso definitivamente beneficia a los Administradores de Seguridad de Red/otros roles de seguridad de red y los dota del conocimiento para convertirse en Analistas de SOC. El programa ofrece una formación exhaustiva en habilidades y herramientas de SOC y también es beneficioso para todos los aspectos del programa de seguridad (GRC, IAM) y para personas en equipos de servicio de ayuda y redes.

”

– Dan Bowden,
CISO de Sentara Healthcare en
Estados Unidos.

“

Considero que este es el primer programa estructurado dedicado a las habilidades requeridas para ser un Analista de SOC, con un enfoque específico en los requisitos del trabajo. Este es un curso bien diseñado y beneficiaría a los profesionales/aspirantes de SOC en adquirir una comprensión general de las habilidades necesarias. Como un subconjunto de las habilidades requeridas en el trabajo de Analista de SOC, este programa también beneficiará a otros roles laborales relacionados con la seguridad de redes.

”

– Prabir Panda,
Arquitecto de Seguridad Empresarial,
Comisión Electoral de India

“

Este programa proporciona la formación académica necesaria y las habilidades requeridas para el rol laboral de Analista de SOC en los niveles L1 y L2. Un entorno virtual con diversos escenarios y ejemplos de playbook y runbooks mejora aún más las habilidades prácticas. El programa beneficiará a nuestro equipo de SOC y servirá como material de referencia valioso. En mi opinión, la principal fortaleza de este programa es la investigación académica realizada para su creación. Los equipos de Forense Digital, Resiliencia, Respuesta a Incidentes e Inteligencia de Amenazas también pueden beneficiarse en gran medida de este programa.

”

– Dawie Wentzel
Jefe de Ciberforenses, Grupo Absa,
Sudáfrica

“

Considero que este programa es un paso lógico que un Analista podría utilizar para progresar hacia una certificación de nivel superior o abrir oportunidades para moverse lateralmente a nuevas certificaciones. Una gran fortaleza que veo en el programa es que cubre todas las áreas/habilidades necesarias en suficiente profundidad para que los individuos operen con éxito como Analistas de SOC y/o utilicen el programa como una plataforma de lanzamiento para desarrollarse como profesionales de seguridad. Estoy seguro de que este programa proporcionará el conjunto de habilidades necesario para los Analistas de SOC en los niveles L1 y L2.

”

– Miki Calero
Fundador
Urbis Global LLC (Ex-Ejército de
Estados Unidos)



EC-Council

Envia un Correo a:
academiacyber@tgk.com.mx
Siguenos en nuestras redes

