CSA: Certified SOC Analyst

El programa CSA Certified SOC Analyst es el primer paso para integrarse a un Centro de Operaciones en Seguridad (SOC). Esta ingeniado para el actual y el futuro aspirante a Analista SOC Tier I y Tier II para obtener las competencias en el desempeño nivel introducción y nivel intermedio de operaciones.

CSA es un programa de entrenamiento y credencialización que ayuda al candidato a adquirir habilidades técnicas en demanda y por tendencia mediante una instrucción por los mejores y más experimentados entrenadores en la industria. El programa se enfoca en crear nuevas oportunidades de carrera a través de un extenso y meticuloso conocimiento con capacidades de nivel avanzado para contribuir dinámicamente a un equipo SOC.

Siendo un programa intenso de tres días, abarca minuciosamente los fundamentos de las operaciones SOC, antes de retransmitir el conocimiento de la gestión de log y correlación, despliegue de SIEM, detección avanzada de incidentes y respuesta incidente. Además, el candidato aprenderá a gestionar varios procesos de SOC y colaborará con el CSIRT en el momento de la necesidad.

1.1 Componentes críticos

- 100% Cumplimiento con el marco tecnológico de NICE 2.0
- Destaca en el extremo-a-extremo del flujo de trabajo del SOC
- Aprenda detectar incidencias con SIEM
- Detección de incidencias mejorada con Threat Intelligence
- Crear el entendimiento del despliegue SIEM
- Promueve el aprendizaje práctico
- El entorno de laboratorio simula un entorno en tiempo real
- Obtenga más información con material de referencia adicional

1.2 Temario

- Módulo 1 - Operaciones y gestión de la seguridad
- Módulo 2 - Comprensión de las amenazas cibernéticas, IoCs y metodología de ataque
- Módulo 3 - Los incidentes, Eventos y registro
- Módulo 4 - Detección de incidentes de seguridad de la información y administración de eventos (SIEM)
- Módulo 5 - Detección de incidencias mejorada con Threat Intelligence
- Módulo 6 - Respuesta a incidentes

1.3 Información del Examen

Detalles de Examen

El examen de la CSA está diseñado para poner a prueba y validar en un candidato la comprensión global de los trabajos y tareas necesarias como analista del SOC. Validando así su comprensión global de un completo flujo de trabajo del SOC.

- Título del examen: Certified SOC Analyst
- Código de examen: 312-39
- Número de preguntas: 100
- Duración: 3 horas
- Disponibilidad: Portal de examen ECC (please visit https://www.eccexam.com)
- Formato de Prueba: Opción múltiple
- Puntuación: 70%

Requerimiento de elegibilidad de examen

El programa CSA requiere un candidato que tenga 1 año de experiencia laboral en la administración de la red / dominio de seguridad y deberá ser capaz de proporcionar pruebas de la misma, validados a través del proceso de solicitud, a menos que el candidato asista a la formación oficial.