ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 24 horas

Seguridad / Certified SOC Analyst (C|SA)

El programa EC-Council Certified Incident Handler (E|CIH) capacita a los estudiantes con los conocimientos, habilidades y capacidades necesarias para prepararse, gestionar y erradicar amenazas y actores maliciosos durante un incidente de seguridad. El curso cubre el proceso completo de manejo y respuesta a incidentes, combinando contenido teórico con laboratorios prácticos diseñados para enseñar procedimientos y técnicas tácticas que permiten planificar, registrar, clasificar, notificar y contener incidentes de manera efectiva. Los participantes aprenden a manejar distintos tipos de incidentes, aplicar metodologías de evaluación de riesgos y comprender las leyes y políticas relevantes relacionadas con la gestión de incidentes. Además, el programa incluye actividades posteriores al incidente, como contención, erradicación, recopilación de evidencias y análisis forense, orientadas a acciones legales, mitigación y prevención de futuros incidentes. E|CIH adopta un enfoque metodológico integral que abarca desde la preparación y planificación del proceso de gestión de incidentes hasta la recuperación de activos organizacionales afectados.

Con más de 95 laboratorios avanzados, 800 herramientas y escenarios prácticos en distintos sistemas operativos, el programa ofrece una formación completa y realista que transforma a los estudiantes en profesionales capaces de manejar incidentes en entornos organizacionales complejos, consolidándose como una de las certificaciones más completas del mercado en manejo y respuesta a incidentes.

Perfil de la audiencia

El curso está dirigido a personas que aspiran a incorporarse o avanzar dentro de un Centro de Operaciones de Seguridad (SOC), enfocándose en sus funciones, desarrollo y gestión. El programa prepara a los participantes para desempeñar roles reales en operaciones de seguridad, incluyendo actividades de monitoreo, detección, investigación y respuesta a incidentes.

Además, la certificación C|SA está alineada con funciones laborales que se desempeñan dentro de un SOC, tales como:

- Junior SOC Security Analyst
- SOC Analyst
- Security Incident Response Analyst
- SOC Threat Analyst
- SOC Analysts (Niveles L1, L2 y L3)
- Info Security Analyst 3

Prerrequisitos

Aunque el programa Certified SOC Analyst (C|SA) puede ser tomado por principiantes y está diseñado para formar tanto a aspirantes como a analistas SOC de niveles Tier I, Tier II y Tier III, se recomienda contar con conocimientos básicos de ciberseguridad y de redes. Estos fundamentos facilitan la comprensión de los conceptos, técnicas y herramientas utilizadas durante el entrenamiento, permitiendo que el participante aproveche mejor las actividades prácticas y los escenarios de operación dentro de un SOC.

Módulos

Módulo 01Operaciones y Gestión de Seguridad

Aprende cómo un SOC mejora la gestión de seguridad de una organización para mantener una postura de seguridad sólida, enfocándose en los roles críticos de las personas, la tecnología y los procesos en sus operaciones.

Módulo 02 Comprensión de las Amenazas Cibernéticas, IoCs y Metodología de Ataque

Aprende varios ciberataques, sus IoCs y las tácticas, técnicas y procedimientos (TTPs) que utilizan los cibercriminales.

Módulo 03 Gestión de Registros (Log Management)

Aprende la gestión de registros en SIEM, incluyendo cómo se generan, almacenan, recopilan de manera centralizada, normalizan y correlacionan los registros en los sistemas.

Módulo 04 Detección y Triage de Incidentes

Aprende los fundamentos de SIEM, incluidas sus capacidades, estrategias de despliegue, desarrollo de casos de uso y cómo ayuda a los analistas del SOC a detectar anomalías, clasificar alertas y reportar incidentes.

Módulo 05 Detección Proactiva de Amenazas

Aprende la importancia de la inteligencia de amenazas y del threat hunting para los analistas SOC, y cómo su integración con SIEM ayuda a reducir falsos positivos y permite un triage de alertas más rápido y preciso.

Módulo 06 Respuesta a Incidentes

Aprende las etapas de la respuesta a incidentes y cómo el IRT colabora con el SOC para manejar y responder a incidentes escalados.

Módulo 07 Investigación Forense y Análisis de Malware

Aprende la importancia de la investigación forense y el análisis de malware en las operaciones del SOC para comprender los métodos de ataque, identificar IoCs y mejorar las defensas futuras.

Módulo 08 SOC para Entornos en la Nube

Aprende los procesos del SOC en entornos en la nube, cubriendo monitoreo, detección de incidentes, respuesta automatizada y seguridad en AWS, Azure y GCP utilizando herramientas nativas de la nube.

Examen de Conocimientos – EC-Council SOC Analyst (CSA)

El examen de Certified SOC Analyst evalúa los conocimientos y habilidades adquiridos durante el programa, midiendo la capacidad del candidato para desempeñarse eficazmente dentro de un Centro de Operaciones de Seguridad. Este examen oficial está diseñado para validar competencias en detección de amenazas, gestión de incidentes, análisis forense, uso de SIEM y operación general del SOC.

- Código del examen:
  - 312-39
- Duración:
  - 3 horas
- Disponibilidad:
  - EC-Council Exam Portal
- Formato del examen:
  - Opción múltiple