CURSO

OPERADOR SOC

Plan de estudio

educación IT

Nuestro propósito

Transformar positivamente la vida de las personas.

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.

Code your future!

Contenido del curso

Investiga alertas, analiza tráfico, detecta amenazas, usa herramientas actuales de Blue Team y aplica procedimientos reales de respuesta a incidentes.

Proyecto Integrador

Investigación de Incidente SOC

Realizarás una investigación completa de un incidente de seguridad en un entorno corporativo simulado, aplicando técnicas y herramientas propias de un Operador SOC nivel L1/L2.

- Analizarás alertas, revisarás logs e interpretarás eventos críticos.
- Extraerás indicadores (IOCs), correlacionarás fuentes de información y elaborarás un informe profesional de incidente siguiendo las mejores prácticas del Blue Team".

¿Qué aprenderás?

- Investigación de alertas SOC L1/L2
- Identificación de IOCs y patrones
- Uso de Sysmon, OSQuery y YARA
- Análisis de PCAPs con Wireshark
- Correlación en SIEM y XDR
- Automatización de flujos en SOAR
- Detección de phishing y fraude
- Preparación de portfolio SOC Jr

Plan de estudios

1 Introducción SOC y BlueTeam

- Roles SOC L1/L2/L3.
- Flujos de trabajo.
- MITRE ATT&CK.
- Tipos de alertas.
- Fuentes de logs.
- Stack Blue Team actual.

2 BlueTeam Toolkit

- Sysinternals Suite.
- Sysmon eventos clave.
- OSQuery consultas.
- System Informer.
- Volatility básico.
- Velociraptor DFIR.

3 Malware y tácticas

- Tipos de malware.
- Cadena de ataque.
- Persistencia común.
- Indicadores e IOCs.
- Comportamientos.

- MITRE aplicado.

4 Análisis de tráfico PCAP

- Filtros Wireshark.
- Patrones comunes.
- PCAPs reales.
- C2 y exfiltración.
- Tráfico y SIEM.
- Anomalías.

5 SIEM. SOAR. XDR

- Casos de uso SIEM.
- Correlación reglas.
- Wazuh/Splunk/Elastic.
- SOAR automatizado.
- EDR/XDR modernos.
- Investigación L1/L2.

6 Investigación Alertas

- Falsos positivos.
- Técnicas L1.
- Análisis L2.
- IOC hunting.
- Priorización.
- Playbooks/Runbooks.



Phishing Correo

- Encabezados full.
- SPF/DKIM/DMARC.
- URLs y sandbox.
- Adjuntos maliciosos.
- OSINT aplicado.
- Casos LATAM.

Modalidad del Curso

Duración
5 semanas / 18 h

Frecuencia semanal
2 encuentros de 2 h

Modalidad
Online en vivo

Grupos reducidos
Promedio 15 personas

Nivel: Avanzado

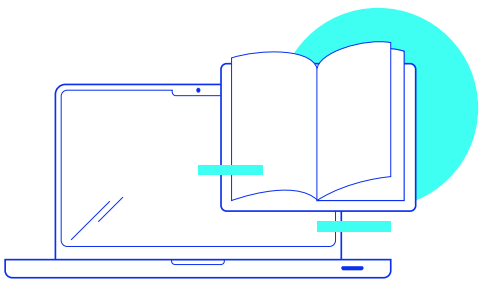


Requisitos

Conocimientos Es recomendable tener una base sobre: **Introducción a redes Introducción a la ciberseguridad**

Dedicación fuera de clase

Además de las horas de clase, recomendamos que inviertas 4 h semanales extras para realizar los desafíos complementarios, estudiar el material de lectura y completar los exámenes del Alumni.



¿Cómo será tu experiencia?



Aprender haciendo

Ejercita y pon en práctica lo estudiado.



Trabajo en equipo

Une esfuerzos y potencia los resultados.



Clases grabadas

Consúltalas las veces que quieras.



Profesores expertos

Aprende de gigantes de la industria.



Asistente académico

Recibe soporte dentro y fuera de clase.



Plataforma Alumni

Encuentra recursos, materiales y clases.

¿Por qué Educación IT?



IT Créditos

Gana puntos al aprobar los exámenes de los cursos. Luego, podrás canjearlos por nuevos cursos sin costo alguno. Los IT Créditos que acumules no vencen ni se devalúan.



Garantía de aprendizaje

Si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, ¡vuelve a tomar el curso sin ningún costo! Puede ser de forma total o parcial.



Comunidad en Discord

Mantente en contacto con la comunidad de EducaciónIT a través de nuestro servidor de Discord. Podrás hablar con tus compañeros, profesores, asistentes académicos y soporte.

Preguntas frecuentes

Si me pierdo una o más clases, ¿puedo recuperarlas?

Todas las clases quedan grabadas de por vida en tu plataforma Alumni. ¡Siempre podrás volver a verlas cada vez que lo necesites!

¿Cómo voy a aprender?

Te enfrentarás a situaciones de trabajo reales, en donde tendrás que aplicar lo aprendido de forma individual y en equipo. Por medio de la prueba y el error, irás superando desafíos y obteniendo nuevas habilidades que luego podrás aplicar en el ámbito laboral.

¿Cómo son las clases online en vivo?

Las clases duran entre 2 y 3 horas de lunes a viernes (sábados 3 o 4 hs) y se desarrollan de forma online en vivo en aulas virtuales, donde vas a poder interactuar con el instructor y tus compañeros. Manejamos cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

Operador SOC

Plan de estudio

Code your future

www.educacionit.com



@educacionit