EC-COUNCIL



EC-COUNCIL · PROGRAMA DE CIBERSEGURIDAD INDUSTRIAL

ICS/SCADA Cybersecurity

Proteja los Sistemas de Control Industrial (ICS) y las redes OT frente a ataques que pueden afectar la seguridad física de personas y comunidades

¿Por qué debería asistir?

Por el impacto que un ataque puede tener en la seguridad física de comunidades, empleados y clientes, la seguridad de ICS/SCADA es una prioridad aún mayor que la de los sistemas de TI tradicionales. Los ciberdelincuentes ya han desarrollado amenazas como Triton/TRISIS y Stuxnet, capaces de interrumpir la tecnología operativa (OT) industrial.

Este curso práctico le da las bases de la seguridad y de la defensa de arquitecturas frente a ataques. Con el enfoque de “pensar como un hacker”, aprenderá a analizar el riesgo de la red corporativa y de control, aplicar las mejores prácticas para cruzar la brecha de aire (air gap), seguir un proceso sistemático de análisis de intrusiones y malware, y responder a incidentes con un proceso forense digital.

4 días	8	Práctico	IT + OT	ICS + SCADA
DURACIÓN	MÓDULOS	FORMATO	COBERTURA	ENFOQUE



¿Quién debería participar?

Personal de sistemas SCADA
Profesionales que operan y mantienen sistemas SCADA e ICS en plantas, servicios públicos e industria.

Analistas de sistemas de negocio
Analistas que dan soporte a las interfaces entre los sistemas de negocio y SCADA.

Administración e ingeniería
Administradores de sistemas, ingenieros y profesionales de TI que administran, actualizan y aseguran SCADA y/o ICS.

Consultoría de seguridad
Consultores que realizan evaluaciones de seguridad de entornos SCADA y/o ICS.

Objetivos de aprendizaje

- Comprender las arquitecturas ICS/SCADA y las amenazas específicas de la tecnología operativa (OT)
- Analizar el riesgo de la red corporativa de TI y de la red de control industrial
- Aplicar el enfoque de “pensar como un hacker” para defenderse de los ataques comunes contra redes de petróleo y gas
- Gestionar vulnerabilidades en entornos donde los parches no siempre son posibles
- Aplicar estándares y regulaciones de ciberseguridad para Sistemas de Control Industrial
- Asegurar la red ICS y aplicar las mejores prácticas para cruzar la brecha de aire (air gap)
- Seguir un proceso sistemático de análisis de intrusiones y malware con IDS e IPS
- Aplicar el proceso forense digital y responder a incidentes cuando se detecta una brecha

Áreas de habilidad del programa

Defensa de redes ICS/SCADA | Protocolos TCP/IP | Hacking y técnicas de ataque | Gestión de vulnerabilidades | Estándares y regulaciones | Air gap | IDS e IPS | Respuesta a incidentes

La seguridad de los Sistemas de Control Industrial (ICS), de los sistemas SCADA y de la tecnología operativa (OT) es necesaria porque protege procesos que actúan sobre el mundo físico, a diferencia de la seguridad de TI tradicional, que protege sobre todo datos. Estos sistemas controlan la generación y distribución de energía, el tratamiento de agua, los oleoductos, las plantas químicas, la manufactura y el transporte, así que un incidente puede causar explosiones, derrames, apagones, contaminación o pérdida de vidas, además de pérdidas económicas.

El riesgo ha crecido porque las redes OT, diseñadas durante décadas para estar aisladas, hoy se conectan a la red corporativa, a la nube y al acceso remoto de proveedores para ganar eficiencia, y esa brecha de aire (air gap) ya casi no existe. Muchos equipos industriales, como los PLC, las RTU y las HMI, funcionan durante 15 a 30 años con sistemas operativos obsoletos y protocolos como Modbus o DNP3, creados sin autenticación ni cifrado.

Además, no se pueden parchear ni reiniciar con facilidad sin detener la producción: según TheHackerNews, en 2023 el porcentaje de vulnerabilidades de ICS sin parche subió al 34 %, frente al 13 % del año anterior. Los atacantes ya lo han aprovechado. Stuxnet saboteó centrifugadoras manipulando sus controladores, los ataques a la red eléctrica de Ucrania en 2015 y 2016 dejaron a cientos de miles de personas sin electricidad, y Triton/TRISIS atacó en 2017 los sistemas instrumentados de seguridad de una planta petroquímica, que existen precisamente para evitar desastres.

El ransomware contra Colonial Pipeline en 2021 mostró que basta comprometer el lado de TI para obligar a detener la operación física y desabastecer de combustible a una región entera. Por eso las organizaciones necesitan profesionales que entiendan las dos redes, la corporativa y la de control: que sepan analizar el riesgo, segmentar la red, aplicar normas como IEC 62443 y el NIST SP 800-82, detectar intrusiones y responder a incidentes.

Programa del curso

Duración: 4 días

Módulo	Contenido
Módulos 1–2 Día 1	01 **Introducción a la defensa de redes ICS/SCADA:** conceptos de ICS y SCADA, componentes, arquitecturas y amenazas a la tecnología operativa. 02 **TCP/IP 101:** fundamentos de redes y del modelo TCP/IP aplicados a las redes industriales.
Módulos 3–4 Día 2	03 **Introducción al hacking:** cómo piensa y actúa un atacante, y técnicas comunes contra redes corporativas y de control. 04 **Gestión de vulnerabilidades:** identificación, priorización y tratamiento de vulnerabilidades en entornos ICS.
Módulos 5–6 Día 3	05 **Estándares y regulaciones de ciberseguridad:** marcos, normas y regulaciones aplicables a los Sistemas de Control Industrial. 06 **Aseguramiento de la red ICS:** arquitecturas seguras, segmentación y controles para proteger la red de control.
Módulos 7–8 Día 4	07 **Cómo cruzar la brecha de aire (air gap):** mejores prácticas y recomendaciones para conectar de forma segura las redes de TI y OT. 08 **Introducción a los sistemas de detección (IDS) y prevención (IPS) de intrusiones:** análisis de intrusiones y malware, y respuesta a incidentes.

Examen

Duración: 2 horas

Título	ICS/SCADA Cybersecurity		
N.º de preguntas	75	**Duración**	2 horas
Formato	Opción múltiple (MCQ)	**Aprobación**	70 %

Requisitos recomendados

- **Perfil recomendado:** profesionales de TI que gestionan o dirigen la infraestructura de TI de su organización y son responsables de establecer y mantener políticas, prácticas y procedimientos de seguridad de la información.
- **Enfoque:** Sistemas de Control Industrial (ICS) y Sistemas de Supervisión, Control y Adquisición de Datos (SCADA).

Por qué la seguridad ICS es prioritaria

Un ataque a un Sistema de Control Industrial puede afectar la seguridad física de comunidades, empleados y clientes. Según TheHackerNews (2023), el porcentaje de vulnerabilidades de ICS sin parche subió al 34 %, frente al 13 % del año anterior, y amenazas como Triton/TRISIS y Stuxnet ya han interrumpido operaciones industriales.

Información general

- Formación práctica con el enfoque de “pensar como un hacker”, centrada en las redes corporativas y de control de petróleo y gas
- Cubre el análisis de riesgo de TI y OT, el análisis de intrusiones y malware, y el proceso forense digital ante incidentes



EC-Council Accredited Training Center

ICS|SCADA Cybersecurity

C|E|I Certified EC-Council Instructor