PROGRAMA OFICIAL ISA / CIBERSEGURIDAD INDUSTRIAL

IC37

2137 / MANTENIMIENTO

Operación y mantenimiento de ciberseguridad de los IACS

CURSO	DURACIÓN	CEU	VERSIÓN
IC37V	3 días	2.1	3.01

Operación y mantenimiento de ciberseguridad de los IACS (IC37V) se centra en las actividades asociadas con la operación continua y el mantenimiento de la ciberseguridad de los IACS implementada en la fase de diseño e implementación. Esto incluye el diagnóstico y la resolución de problemas de red, el monitoreo de seguridad y la respuesta a incidentes, así como el mantenimiento de las contramedidas de ciberseguridad implementadas. Esta fase también incluye la gestión de cambios en materia de seguridad, los procedimientos de copia de seguridad y recuperación, y las auditorías periódicas de ciberseguridad.

IC37 proporcionará a los participantes la información y las habilidades para detectar y resolver posibles eventos de ciberseguridad, así como para mantener el nivel de seguridad de un sistema en operación durante todo su ciclo de vida, pese a los desafíos de un entorno de amenazas en constante cambio.

Programa de certificación

IC37 es el cuarto curso del Programa de Certificación de Ciberseguridad ISA/IEC 62443. Al aprobar el examen se obtiene el certificado de Especialista en Mantenimiento de Ciberseguridad ISA/IEC 62443. La inscripción al curso incluye la tarifa de un examen.

Al completar el curso con éxito, se proporcionará un certificado de finalización que indica el número total de CEU obtenidas.

Requisitos previos obligatorios

Completar con éxito el curso Uso de las normas ISA/IEC 62443 para proteger sus sistemas de control (IC32) y aprobar el examen del certificado de Especialista en Fundamentos de Ciberseguridad ISA/IEC 62443 son requisitos previos obligatorios para este curso.

¿Quiénes deben tomar IC37?

- Ingenieros y gerentes de sistemas de control
- Integradores de sistemas
- Ingenieros y gerentes de TI en instalaciones industriales
- Gerentes de planta
- Personal de seguridad y gestión de riesgos de la planta

Objetivos y ejercicios

Objetivos de aprendizaje

- Realizar diagnósticos básicos de red y resolver problemas.
- Interpretar los resultados de las alarmas de diagnóstico y los registros de eventos de los dispositivos IACS.
- Implementar procedimientos de copia de seguridad y restauración de los IACS.
- Describir el ciclo de vida y el procedimiento de gestión de parches de los IACS.
- Aplicar un procedimiento de gestión de antivirus.
- Definir los fundamentos de las herramientas de control de aplicaciones y listas de permitidos.
- Definir los fundamentos de la detección de intrusiones en redes y equipos.
- Definir los fundamentos de las herramientas de monitoreo de incidentes y eventos de seguridad.
- Implementar un plan de respuesta a incidentes.
- Implementar un procedimiento de gestión del cambio de los IACS.
- Realizar una auditoría básica de ciberseguridad de los IACS.

Ejercicios

- Construcción del tablero
- Listas de permitidos
- Gestión de parches
- Sistema de detección de intrusiones Snort
- Monitoreo
- Resolución de problemas
- Recuperación tras incidentes
- Gestión de información y eventos de seguridad (SIEM)

Prerrequisitos recomendados: cursos ISA

- Conocimientos y experiencia equivalentes.
- Evaluación de la ciberseguridad de sistemas IACS nuevos o existentes (IC33).
- Diseño e implementación de ciberseguridad de los IACS (IC34).
- Fundamentos de comunicación para sistemas de automatización industrial (TS07).
- Habilidades avanzadas de TI y OT para personal de instrumentación y control (TS12).

Temario completo

01 Introducción al ciclo de vida de la ciberseguridad de los ICS

- Fase de identificación y evaluación
- Fase de diseño e implementación
- Fase de operación y mantenimiento

02 Diagnóstico y resolución de problemas de red

- Interpretación de alarmas y registros de eventos de los dispositivos
- Indicadores tempranos
- Sistemas de detección de intrusiones en la red
- Herramientas de gestión de redes

03 Diagnóstico y resolución de problemas de aplicaciones

- Interpretación de alarmas y registros de eventos del sistema operativo y las aplicaciones
- Indicadores tempranos
- Herramientas de gestión de aplicaciones y listas de permitidos
- Herramientas antivirus y de protección de equipos terminales
- Herramientas de monitoreo de incidentes y eventos de seguridad (SIEM)

04 Procedimientos y herramientas de operación de ciberseguridad de los IACS

- Desarrollo y aplicación de un procedimiento de gestión del cambio de los IACS
- Desarrollo y aplicación de un procedimiento de copia de seguridad de los IACS
- Herramientas de gestión de configuración de los IACS
- Desarrollo y aplicación de un procedimiento de gestión de parches de los IACS
- Herramientas de gestión de parches
- Desarrollo y aplicación de un procedimiento de gestión de antivirus de los IACS
- Herramientas antivirus y de listas de permitidos
- Desarrollo y aplicación de un procedimiento de auditoría de ciberseguridad de los IACS
- Herramientas de auditoría

05 Respuesta a incidentes de los IACS

- Desarrollo y aplicación de un plan de respuesta a incidentes de los IACS
- Investigación de incidentes
- Recuperación del sistema

Recursos y condiciones del curso

Recursos recomendados

ISA-62443-1-1-2007
Seguridad para sistemas de automatización y control industrial - Parte 1-1: Terminología, conceptos y modelos. (Norma)

ANSI/ISA-62443-2-1-2024
Seguridad para sistemas de automatización y control industrial - Parte 2-1: Requisitos del programa de seguridad para los propietarios de activos IACS. (Norma)

ANSI/ISA-62443-3-2-2020
Seguridad para sistemas de automatización y control industrial - Parte 3-2: Evaluación de riesgos de seguridad para el diseño de sistemas. (Norma)

ANSI/ISA-62443-3-3 (99.03.03)-2013
Seguridad para sistemas de automatización y control industrial - Parte 3-3: Requisitos y niveles de seguridad del sistema. (Norma)

Biblioteca de ciberseguridad de ISA. (Publicación)

Idioma de los materiales y de la evaluación

Para la audiencia de habla hispana (y portuguesa) el material de estudio se dispone en idioma inglés. La evaluación de certificación profesional se encuentra disponible únicamente en idioma inglés, al igual que la serie de normas ISA/IEC-62443.

Alcance de la formación ISA

Los principales objetivos de la formación ISA son asegurar que los participantes comprendan e interpreten correctamente los requisitos de la serie de normas ISA/IEC-62443 y lo que debe hacerse. Si bien los ejercicios y los productos utilizados en el laboratorio ayudan a comprender los conceptos, no está entre los objetivos de ISA recomendar una solución específica ni mostrar cómo cumplir los múltiples requisitos.

Instructor

Maximillian G. Kon. Fundador, CEO y director general de WisePlant Group LLC. Ingeniero electrónico especializado en sistemas de control y telecomunicaciones. Consultor especializado en ciberseguridad y seguridad industrial. Instructor oficial de ISA, con más de 20 años de experiencia en sistemas industriales y sistemas críticos en todo tipo de industrias.

Consulta los detalles del curso IC37

WiseCourses.com/courses/2137ven30/