PROGRAMA OFICIAL ISA / CIBERSEGURIDAD INDUSTRIAL

IC33

IC33 / EVALUACIÓN

Evaluación de la ciberseguridad de sistemas IACS nuevos o existentes

CURSO	DURACIÓN	CEU	VERSIÓN
IC33	3 días	2.1	4.10

Evaluación de la ciberseguridad de sistemas IACS nuevos o existentes (IC33) proporcionará a los participantes la información y las habilidades necesarias para evaluar la ciberseguridad de un sistema de automatización y control industrial (IACS) nuevo o existente, y para desarrollar una especificación de requisitos de ciberseguridad (CRS) que pueda utilizarse para documentar los requisitos de ciberseguridad del proyecto.

IC33 comienza con la primera fase del ciclo de vida de la ciberseguridad de los IACS, tal como se define en la norma ISA/IEC-62443-1-1. Los participantes aprenderán a identificar y documentar los activos de los IACS y a realizar una evaluación de vulnerabilidades y riesgos de ciberseguridad para identificar y comprender las vulnerabilidades de alto riesgo que requieren mitigación. De acuerdo con ISA/IEC-62443-2-1, estas evaluaciones deben realizarse tanto en aplicaciones nuevas (greenfield) como existentes (brownfield).

Parte del proceso de evaluación implica desarrollar un modelo de zonas y conductos del sistema, identificar los niveles de seguridad objetivo y documentar los requisitos de ciberseguridad en una CRS.

Programa de certificación

IC33 es el segundo curso del Programa de Certificación de Ciberseguridad ISA/IEC-62443. Al aprobar el examen se obtiene el certificado de Especialista en Evaluación de Riesgos de Ciberseguridad ISA/IEC-62443 . La inscripción al curso incluye una tarifa de examen.

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

Requisitos previos obligatorios

La finalización exitosa de Uso de los estándares ISA/IEC-62443 para proteger sus sistemas de control (IC32) y la aprobación del examen de certificado de Especialista en Fundamentos de Ciberseguridad ISA/IEC-62443 son requisitos previos obligatorios para este curso.

Audiencia y objetivos

¿Quiénes deben tomar el IC33?

- 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 de aprendizaje

- Identificar y documentar el alcance del IACS bajo evaluación
- Especificar, recopilar o generar la información de ciberseguridad necesaria para realizar la evaluación
- Identificar o descubrir vulnerabilidades de ciberseguridad inherentes a los productos o al diseño del sistema IACS
- Interpretar los resultados de un análisis de peligros del proceso (PHA)
- Organizar y facilitar una evaluación de riesgos de ciberseguridad para un IACS
- Identificar y evaluar escenarios de amenazas realistas
- Identificar y evaluar la eficacia de las contramedidas existentes
- Identificar brechas en las políticas, procedimientos y estándares existentes
- Evaluar el costo, la complejidad y la eficacia de las nuevas contramedidas para hacer recomendaciones significativas
- Establecer y documentar zonas y conductos de seguridad
- Desarrollar una especificación de requisitos de ciberseguridad (CRS)

01 Preparación para una evaluación

- Ciclo de vida de la seguridad
- Alcance
- Diagramas de arquitectura del sistema
- Diagramas de red
- Inventario de activos
- Evaluación de la criticidad cibernética

02 Evaluación de vulnerabilidades de ciberseguridad

- Riesgo
- Tipos de evaluaciones de vulnerabilidad de ciberseguridad
- Evaluaciones de alto nivel
- Evaluaciones pasivas y activas
- Pruebas de penetración
- Realización de evaluaciones de alto nivel
- Herramientas de evaluación
- Herramienta de evaluación de seguridad cibernética (CSET)

03 Realización de evaluaciones de vulnerabilidad

- Proceso de vulnerabilidad
- Evaluación previa
- Normas
- Investigación
- Reunión de inicio y recorrido de inspección
- Recopilación pasiva de datos
- Recopilación activa de datos
- Pruebas de penetración

04 Evaluaciones de riesgos cibernéticos

- Comprender el riesgo
- Identificación, clasificación y evaluación de riesgos
- ISA/IEC 62443-2-1
- Sistema en consideración (SuC)
- Realizar una evaluación de riesgos de alto nivel
- Escala de consecuencias
- Establecer zonas y conductos
- Planos y documentación de zonas y conductos
- Documentar los requisitos de ciberseguridad

05 Realización de evaluaciones de riesgos cibernéticos

- Proceso detallado de evaluación de riesgos cibernéticos
- Amenazas
- Vulnerabilidades
- Consecuencias
- Probabilidad
- Calcular el riesgo
- Niveles de seguridad
- Contramedidas
- Riesgo residual
- Documentación

06 Revisión crítica de los diagramas de arquitectura del sistema

- Inventario de activos
- Evaluación de brechas
- Evaluación de vulnerabilidades de Windows
- Captura de tráfico Ethernet
- Escaneo de puertos
- Uso de herramientas de análisis de vulnerabilidades
- Realizar una evaluación de riesgos de alto nivel
- Creación de un diagrama de zona y conducto
- Realizar una evaluación detallada del riesgo cibernético
- Revisión crítica de una especificación de requisitos de ciberseguridad

07 Documentación e informes

- Documento que se debe mantener
- Informes requeridos
- Diagramas de zonas y conductos
- Especificación de requisitos de ciberseguridad (CRS)

Laboratorios y formación

Ejercicios de laboratorio

- Inventario de activos
- Realizar una evaluación de riesgos de ciberseguridad de alto nivel
- Evaluación de riesgos de alto nivel mediante CSET
- Escaneo de vulnerabilidades
- Pruebas de penetración en Windows XP con Kali Linux
- Creación de un diagrama de zonas y conductos
- Evaluación detallada de riesgos
- Opcional: análisis básico de seguridad (GFI Languard)

Acceso al laboratorio

- Los estudiantes utilizarán el laboratorio de ciberseguridad de la sede de ISA para completar los ejercicios de laboratorio.
- Acceso a un laboratorio virtual únicamente durante la clase.
- Aproximadamente 10 horas de actividades de laboratorio.

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. La traducción independiente de las normas no está aprobada ni autorizada por el Comité ISA99.

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.

Recursos recomendados

Normas relacionadas

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

ISA-62443-2-1 (99.02.01)-2009
Seguridad para sistemas de control y automatización industrial - Parte 2-1: Establecimiento de un programa de seguridad de sistemas de control y automatización industrial.

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

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

Libros y lecturas recomendados

- Biblioteca de ciberseguridad.
- Principios de seguridad de sistemas de control y automatización industrial, segunda edición, por Ronald L. Krutz, PhD, PE.

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.

Orientación para elegir el curso

¿No estás seguro de que este curso sea el adecuado para ti? Contáctanos y nuestros expertos te orientarán para desarrollar tu carrera profesional de acuerdo con tus propios objetivos y las necesidades de tu organización.

Consulta los detalles del curso IC33

WiseCourses.com/courses/2133ven400/