PROGRAMA OFICIAL ISA / CIBERSEGURIDAD INDUSTRIAL

IC32

2132 / FUNDAMENTALS

Empleando el estándar ISA/IEC-62443 para proteger a los Sistemas de Control.

CURSO	DURACIÓN[1]	CEU	VERSIÓN
IC32V	16 horas	1.4	6.20

Uso de los estándares ISA/IEC 62443 para proteger sus sistemas de control (IC32V) es una clase virtual dirigida por un instructor que proporciona una visión detallada de cómo se puede utilizar el marco de estándares ISA/IEC 62443 para proteger los sistemas de control críticos. También explora las diferencias técnicas y de procedimiento entre las soluciones de seguridad apropiadas para entornos de TI tradicionales y las apropiadas para entornos SCADA o de planta.

Con el paso al uso de estándares abiertos, como Ethernet, Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) y tecnologías web, en el control de supervisión y adquisición de datos (SCADA) y las redes de control de procesos (PCN), los sistemas están expuestos a los mismos ciberataques a los que se enfrentan los sistemas de información corporativos, proteger los sistemas de control es más importante que nunca.

Programa de certificación

Esta es una clase preparatoria para el Programa de Certificación de Ciberseguridad ISA/IEC 62443. La inscripción al curso incluye la tarifa de un examen.

Se proporcionará un certificado de finalización que indica el número total de CEU obtenidas al completar con éxito los cursos.

¿Quién debe tomar IC32?

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

[1] Se conserva la duración de 16 horas indicada en la ficha original. La página web indica 2 días y, en sus prerrequisitos, describe una clase intensiva de 14 horas.

Objetivos de aprendizaje

Objetivos de la ficha original

- Discutir los principios detrás de la creación de una seguridad de programa efectiva a largo plazo
- Interpretar el marco de seguridad industrial ISA/IEC 62443 y aplicarlo a su operación
- Definir los fundamentos de las metodologías de análisis de riesgos y vulnerabilidades
- Describir los principios del desarrollo de políticas de seguridad
- Explicar los conceptos de defensa en profundidad y los modelos de seguridad de zona/conducto
- Analizar las tendencias actuales en incidentes de seguridad industrial y los métodos que utilizan los piratas informáticos para atacar un sistema
- Defina los principios detrás de las técnicas clave de mitigación de riesgos, incluida la administración de antivirus y parches, firewalls y redes privadas virtuales
- Describir cómo las estrategias de desarrollo de software seguras pueden hacer que los sistemas sean intrínsecamente más seguros.
- Explicar cómo se verifica la seguridad de los sistemas.

Objetivos publicados en la página del curso

- Describir la importancia de la seguridad de los sistemas de control.
- Describir la estructura y el contenido de la serie de documentos ISA/IEC-62443.
- Explicar la importancia de la concientización como contramedida efectiva.
- Definir los principios detrás de la creación de un programa de seguridad efectivo a largo plazo.
- Analizar los fundamentos del análisis de riesgos, las redes industriales y la seguridad de redes.
- Analizar los conceptos que constituyen la base de las normas ISA/IEC-62443: defensa en profundidad, zonas y conductos.
- Describir cómo aplicar técnicas clave de mitigación de riesgos, como antivirus, gestión de parches y firewalls.
- Explicar cómo las estrategias de desarrollo de software seguro hacen que los sistemas sean intrínsecamente más seguros.
- Describir cómo validar o verificar la seguridad de los sistemas.
- Describir cómo se pueden utilizar los perfiles de seguridad de ISA/IEC-62443.

Temario completo

Todos los temas de la ficha original, en su orden de publicación.

- Comprender el entorno actual de seguridad industrial
- ¿Qué es la seguridad electrónica para sistemas de control y automatización industrial (IACS)?
- En qué se diferencian la TI y la planta y en qué se parecen
- Cómo ocurren los ciberataques
- Comprender las fuentes de amenazas
- Pasos para ataques cibernéticos exitosos
- Creación de un programa de seguridad
- Factores críticos para el éxito
- Comprensión de la 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
- Análisis del riesgo
- Justificación del negocio
- Identificación de riesgos
- Clasificación
- Evaluación
- Abordar el riesgo con la política, la organización y la conciencia de seguridad
- Alcance del sistema de gestión de la ciberseguridad
- Seguridad organizacional
- Capacitación del personal y conciencia de seguridad
- Abordar el riesgo con contramedidas de seguridad seleccionadas
- Seguridad del personal
- Seguridad física y ambiental
- Segmentación de red
- Control de acceso
- Abordar el riesgo con medidas de implementación
- Gestión e implementación de riesgos
- Desarrollo y mantenimiento de sistemas
- Gestión de información y documentos
- Seguimiento y mejora del CSMS
- Cumplimiento y revisión
- Mejorar y mantener el sistema de gestión de seguridad cibernética (CSMS)
- Validación o verificación de la seguridad de los sistemas
- ¿Qué se está haciendo?
- Desarrollo de productos y sistemas seguros.

Temario publicado en la web

Listado completo traducido al español, conservando cada tema por separado.

- Introducción a la seguridad de los sistemas de control
- Concientización sobre ciberseguridad
- Serie de normas ISA/IEC-62443
- Modelos y niveles de seguridad ISA/IEC-62443
- Ciclo de vida de la ciberseguridad de los IACS
- Requisitos del programa de seguridad para los propietarios de activos IACS
- Evolución de las normas, prácticas y regulaciones de seguridad
- Fundamentos de seguridad de redes
- Protocolos industriales
- Introducción a la gestión de parches en el entorno IACS
- Introducción a la evaluación de riesgos de seguridad para el diseño de sistemas
- Requisitos del programa de seguridad para los proveedores de servicios IACS
- Desarrollo de productos y sistemas seguros
- Perfiles de seguridad para ISA/IEC-62443
- Esquema de protección de seguridad de los IACS

Ejercicio

Análisis de capturas PCAP en vivo.

Prerrequisitos recomendados

- No hay prerrequisitos obligatorios para tomar este curso; sin embargo, se recomienda encarecidamente que los participantes tengan entre uno y tres años de experiencia en el campo de la ciberseguridad, con cierta experiencia en un entorno industrial. IC32 es una clase intensiva de 14 horas y no hay mucho tiempo para enseñar comandos básicos y fundamentos de ciberseguridad.
- Sería beneficioso haber realizado los cursos ISA TS07 y TS12, o contar con conocimientos o experiencia equivalentes.
- Nota del instructor: uno de los desafíos al impartir IC32 ha sido la asistencia de estudiantes sin conocimientos, o con conocimientos limitados, de los cursos ISA TS07, TS12 o de los principios generales de ciberseguridad.

Recursos y condiciones del curso

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 recomendados

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

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.

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.

Desde WiseCourses estamos inspirados por la innovación en educación para crear procesos de capacitación que sean representativos del mundo en el que vivimos actualmente. Crear y soportar nuevos sistemas potenciando a los educadores y profesionales que adquieren la experiencia.

Consulta los detalles del curso IC32

WiseCourses.com/courses/2132ven620/