Centro de Ciberseguridad Industrial

Sección Española

Centro de
Ciberseguridad Industrial

C/ Maiquez, 18 · 28009 MADRID
Tel.: +34 910 910 751
e-mail: info@cci-es.org
www.cci-es.org
Blog: blog.cci-es.org
Twitter: @info_cci

Contratación

Para formalizar la contratación del curso es imprescindible que se ponga en contacto con nosotros a través del envío de un email a la dirección
info@cci-es.org
indicando su deseo de contratar este curso, fechas, asistentes y datos de facturación.

El CCI se pondrá en contacto con usted para hacerle llegar el contrato del curso con toda la información.

Precio del curso : 1.050 € + IVA

Curso Responsable de Ciberseguridad en IACS (Sistemas de Automatización y Control Industrial)

9 y 10 de mayo de 2018. Hotel Meliá Avd. de América

Resumen

Actualmente las organizaciones e infraestructuras industriales, sobre todo las que soportan servicios esenciales, están muy sensibilizadas por los recientes y graves incidentes de ciberseguridad que se han producido en algunos procesos críticos, cuya interrupción o destrucción podría tener un impacto en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas.

Analizar y comprender el riesgo asociado a estas infraestructuras y su relación básica con los Sistemas de Control Industrial es necesario para cualquier profesional de la seguridad involucrado o relacionado con áreas como la energía, industria química y nuclear, alimentación o transporte, entre otros.

Curso práctico para implantar un sistema de Gestión de Ciberseguridad en un entorno IACS, basado tanto en un análisis de riesgos, como en un diagnóstico de ciberseguridad.

Se utilizará de forma práctica la guía para la construcción de un SGCI https://www.cci-es.org/sgci en la que se han aplicado directrices específicas de los estándares ISO27001 e IEC62443 para un tratamiento eficaz y continuado de los riesgos sobre la disponibilidad, la integridad y la confidencialidad de las operaciones y de la información gestionadas por los sistemas de automatización y control industrial.

Después de completar este curso de 2 días, el asistente podrá:

1. Identificar y definir los conceptos de Ciberseguridad en Sistemas de Control Industrial, analizando los riesgos e impacto en el negocio y en nuestras vidas, desde las distintas perspectivas, tecnológicas y de seguridad.
2. Descubrir y analizar el estado del arte de la Protección de IACS (Sistemas de Automatización y control industrial.)
3. Detectar y analizar la situación actual de la Seguridad en el entorno Industrial y las amenazas y vulnerabilidades de los Sistemas de Control Industrial reconociendo su riesgo asociado en un informe.
4. Discutir aspectos organizacionales y de gestión importantes: Director de TI vs. Director de Seguridad vs. Director de Planta vs. Director de Producción/Fabricación. Diseñar y proponer un marco de gestión adecuado en las Infraestructuras de automatización y control industrial.
5. Gestionar la seguridad digital en un entorno de tecnologías de operación. Establecer, implementar y adoptar un Programa de Seguridad de los Sistemas de Automatización y Control Industrial.

Agenda

Día 1
CONSECUENCIAS DE LOS RIESGOS OT Y SU DIAGNÓSTICO

- Bienvenida, presentaciones individuales...
- Contexto. Automatización industrial
- Consecuencias de los riesgos tecnológicos en IACS
- Diagnóstico de ciberseguridad en entornos industriales
- **Descanso/café**
- Relación entre Protección de Infraestructuras Críticas y Ciberseguridad Entornos Industriales
- Ambitos de aplicación de un sistema de gestión de ciberseguridad industrial
- **Comida**
- Dominio 1: Definición de una estrategia
- Dominio 2: Gestión de los riesgos de ciberseguridad industrial

Día 2
SISTEMA DE GESTIÓN DE CIBERSEGURIDAD INDUSTRIAL

- Bienvenida, y resumen del día anterior
- Dominio 3: Cultura en ciberseguridad
- Dominio 4: Medidas de protección en IACS
- **Descanso/café**
- Dominio 5: Garantía de resiliencia y continuidad
- Modelos de madurez. Ciberseguridad
- **Comida**
- Revisión de Herramienta de evaluación de madurez
- Uso práctico de la herramienta de evaluación de madurez
- Benchmarking práctico. 27 objetivos
- Clausura del curso

Dirigido

Este curso está dirigido fundamentalmente a los responsables de gestionar los riesgos de ciberseguridad en organizaciones industriales, así como a consultores y auditores de sistemas de gestión de riesgos. Dirigido también a profesionales de automatización industrial que necesitan comprender como gestionar los riesgos OT

Formadores

Miguel García-Menéndez

Es responsable de Gobierno Corporativo y Estrategia en el Centro de Ciberseguridad Industrial. Ingeniero de Informática por la Universidad de Oviedo (España), inició la referida trayectoria entre sinópticos (HMI) de instalaciones de tratamiento de acero y algoritmos de control (MES) para la industria siderúrgica española y latinoamericana, al frente del área de Informática de Procesos de una ingeniería ubicada en el norte de España, donde también fue CIO.

Los últimos quince años ha desarrollado una frenética actividad como consultor, auditor, docente y divulgador en diversas firmas de consultoría de dirección y universidades, desde las que ha tenido ocasión de ayudar a otros CIOs (y CISOs) a cumplir con sus obligaciones y a ganar visibilidad dentro de sus organizaciones. Miguel ha formado parte de la lista de expertos externos de la European Network and Information Security Agency (ENISA) y ha sido, y es, miembro de los órganos de gobierno de diversas entidades profesionales y/o sectoriales, ligadas al ámbito tecnológico. Cuenta con múltiples cualificaciones relacionadas con la ciberseguridad como Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA), Certified in the Governance of Enterprise IT (CGEIT), COBIT Foundation Certificate, COBIT Implementation Certificate, COBIT Assessor Certificate, COBIT Foundation Trainer, COBIT Implementation Trainer y COBIT Assessor Trainer, otorgadas por ISACA, entidad de la que ha sido Director de Análisis, en su delegación de Madrid, durante seis años.

José Valiente

Diplomado en Informática de Gestión por la Universidad Pontificia de Comillas, es Especialista en Consultoría Tecnológica y de Seguridad. Con más de 20 años de experiencia trabajando en Consultoras como Davinci Consulting y Tecnocom en proyectos de Seguridad y TI para Gran Cuenta y Administración Pública. Cuenta con múltiples certificaciones de soluciones de fabricantes de seguridad y TI (Cisco CCNA y CCDA, System Security Mcafee, Security Specialist Juniper, Websense Certified Enginer, F5 Bigip Specialist y Radware certified security Specialist) y certificación CISM de ISACA.

Actualmente es responsable de coordinación y comunicación en el Centro de Ciberseguridad Industrial y experto en la dirección de proyectos para gran cuenta y administración pública. Ha dirigido proyectos de implantación de SGSIs en compañías del IBEX 35 y administración pública, con equipos de trabajo de alta capacitación en seguridad y cuenta con amplios conocimientos en ITIL y PMI, impartiendo formación a empresas del sector industrial, financiero y administración pública.

Tipo de curso

Duración: 2 días

Formato: Taller multidisciplinar de trabajo con prácticas en grupo e individuales.

Requisitos/Conocimiento: Será necesario disponer de conocimientos básicos de networking para entender los apartados técnicos y poder realizar adecuadamente las prácticas de laboratorio.