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: 1.350 € + IVA

Centro de Ciberseguridad Industrial

Curso multidisciplinar de Seguridad Digital en la Industria [4.0] y Protección de servicios esenciales

13, 14 y 15 de noviembre 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 las TIC, energía, industria química y nuclear, sistemas financieros y tributarios, alimentación o transporte, entre otros.

Este curso llevará a los participantes a través del estudio del estado del arte de la Protección de los servicios esenciales y la Ciberseguridad Industrial en todo el mundo, tanto en lo que a legislación y normativa se refiere, como a los estándares, iniciativas, marcos de gestión y tecnologías aplicables, consiguiendo así una visión global de la gestión de la seguridad en este tipo de organizaciones que permita al final del curso establecer claramente los siguientes pasos a seguir para asegurar una correcta supervisión, gestión e implantación de las medidas necesarias adecuadas.

Después de completar este curso de 3 días, el asistente podrá:

1. Identificar y definir los conceptos de Ciberseguridad en Sistemas de Control Industrial y Protección de Servicios Esenciales, sus definiciones y relaciones, analizando los riesgos e impacto en el negocio y en nuestras vidas, desde las distintas perspectivas de cumplimiento, tecnológicas y de seguridad.
2. Descubrir y analizar el estado del arte de la Protección de Infraestructuras Críticas a nivel internacional (USA y Canadá, Latinoamérica, Europa) en cuanto a regulaciones, iniciativas, estándares, sectores, organizaciones, metodologías, etc.
3. Detectar y analizar la situación actual de la Seguridad en el Sector Industrial y las amenazas y vulnerabilidades de los Sistemas de Control Industrial reconociendo su riesgo asociado.
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 Críticas y Entornos Industriales
5. Identificar, describir y adoptar marcos y estándares aplicables en estos entornos: IEC 62443, ISO 27001, BS 25999, NIST SP 800-82, Framework NIST...
6. Establecer, implementar y adoptar un Programa de Seguridad de los Sistemas de Control Industrial y Diseñar un Plan de Seguridad y Protección de la Infraestructura Crítica.
7. Mediante el taller práctico HOL “Hands On Lab” se logrará comprender y aplicar el diseño de redes seguras, así como aplicar estrategias y técnicas de defensa experimentando las dos caras de la Ciberseguridad de los sistemas de control.

Agenda

Día 1
Conceptos y estado del arte

- Bienvenida, presentaciones individuales...
- Introducción
- Términos y Conceptos Generales
- Estado del Arte Internacional
- Descanso/café
- Relación entre Protección de Infraestructuras Críticas y Ciberseguridad Entornos Industriales
- Trabajo en Grupo/Discusión: Aplicación Stuxnet otros entornos (uno por sector)
- Aproximación a los Sistemas de Control Industrial
- Trabajo en Grupo: Identificación Sistemas Control Industrial
- Comida
- Vulnerabilidades y Amenazas de los Sistemas de Control Industrial
- Trabajo en Grupo: Análisis de un Caso Práctico (identificación vulnerabilidades, contramedidas...)
- Situación Actual de la Ciberseguridad Industrial

Día 2
Diagnóstico, estandares y recomendaciones

- Bienvenida y resumen día anterior
- Aspectos Organizacionales y de Gestión
- Diagnóstico de la Ciberseguridad Industrial
- Trabajo en Grupo: Discusión sobre el Diagnóstico Presentado
- Descanso/café
- Estándares Aplicables
- Recomendaciones y Siguientes Pasos: Estableciendo un Programa de Ciberseguridad
- Comida
- Trabajo en Grupo: Caso Práctico y Desarrollo y Presentación por Equipo del Esquema Plan de Seguridad
- Café y Preparación Presentaciones
- Presentación por equipos (10 minutos por equipo) del Programa de Ciberseguridad o Protección y Discusión pública
- Presentación Hands-On Lab (a desarrollar al día siguiente)

Día 3
Taller práctico

- Bienvenida y Presentación Taller Práctico HOL (Hands On Lab)
- Taller y Actividades Prácticas
- Conclusiones

Formadores

Silvia Villanueva

Con más de 15 años de experiencia en gestión de riesgos tecnológicos, y con un perfil multidisciplinar que combina áreas de seguridad tanto técnicas como estratégicas, Silvia ha centrado su carrera en gestionar y realizar múltiples proyectos en el ámbito de la Seguridad y Protección de la Información.

Pionera en España en Seguridad Industrial, especializada en Bastionado de Servidores y Revisiones de Seguridad, Análisis y Diseño de Arquitectura de Red y Seguridad en Redes SCADA/ICS/DCS. Adicionalmente dispone de las certificaciones CISSP y CSSLP de ISC2, CISM y CISA de ISACA, CEH de EC-COUNCIL, CSSA de IA Certification y GISCP (Industrial Cyber Security Ceritification) de GIAC, estando esta última focalizada en Ciberseguridad Industrial.

Agustín Valencia

Ingeniero Industrial por ICAI, con formación adicional en distintos ámbitos como Gestión de Mantenimiento, Tecnología Nuclear BWR y más recientemente Director de Seguridad y Master de Seguridad Informática. Con más de 15 años de experiencia, ha cubierto todos los ámbitos del mundo de la energía, desde Ingeniería a Operación y Mantenimiento en centrales de ciclo combinado y nuclear.

Desde 2011, responsable de ciberseguridad en sector nuclear. Liderando desarrollo de planes y análisis de riesgos de ciberseguridad en infraestructuras críticas de acuerdo con Ley PIC. También como Jefe de Ingeniería de proyectos de instrumentación y control y ciberseguridad, modernizando plataformas de control distribuido e introduciendo ciberseguridad desde el diseño o rediseñando arquitecturas de redes y sistemas de control enfocado a bastionado, segmentación de redes, whitelisting y SIEM-IDS sobre sistemas de los principales fabricantes (GE, Honeywell, Schneider-Electric, etc).

Actualmente Responsable de OT en el área de Ciberseguridad Global de Iberdrola, coordinando estrategias OT entre los distintos negocios de su corporación (Generación, Renovables, Redes, Smartgrids) y colaborador con ISA 99/62443 para dispositivos de campo y con ISA84/61511 para integración con 62443.

José Valiente

José Valiente es Director y Responsable de Coordinación y Comunicación del Centro de Ciberseguridad Industrial. Especialista en consultoría Tecnológica y de Seguridad. Cuenta con más de 20 años de experiencia trabajando en grandes consultoras, en las que ha desarrollado su carrera profesional tanto en el ámbito de tecnologías de la información, como en el sector de la automatización industrial.

Ha participado en más de una docena de publicaciones sobre ciberseguridad industrial, así como en múltiples congresos, eventos y cursos especializados en ciberseguridad. Actualmente dispone de múltiples certificaciones en soluciones de fabricantes de seguridad y TI, así como las certificaciones profesionales CISM de ISACA y Global Industrial Cyber Security Professional (GICSP) de GIAC.

Tipo de curso

Duración: 3 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.

Requisitos/Material: El tercer día, los asistentes deberán llevar ordenador personal con capacidad de arranque desde USB.