LOGITEK
real time solutions

Industrial Cybersecurity
by LOGITEK

Curso Intensivo Ciberseguridad Industrial

Conceptos, ataques, contramedidas y procedimientos para fortificar entornos industriales y proteger infraestructuras críticas.

Este curso intensivo de **dos días** de duración y estructurado en **18 sesiones** permitirá a los **clientes finales y a los operadores críticos** entender el alcance de la ciberseguridad industrial, de los riesgos y amenazas que pueden sufrir en sus operaciones del día a día y ayudarles a poner en práctica las contramedidas y recomendaciones propuestas durante su desarrollo. Por otro lado, **los integradores de sistemas**, podrán adquirir los conocimientos fundamentales para entender las necesidades de los clientes finales y así proporcionarles la mejor solución posible en cada situación.

Industrial Cybersecurity
by LOGITEK

Objetivos del Curso

1. **Proporcionar una visión general** acerca de los conceptos más importantes asociados al área de la ciberseguridad industrial.

2. **Entender las principales diferencias** existentes entre las políticas de seguridad que se llevan a cabo en entornos IT y en entornos OT.

3. **Analizar las principales vulnerabilidades y amenazas** que se pueden sufrir en entornos industriales.

4. **Conocer los diferentes tipos de ataques** hacker que pueden realizarse a una red OT o una infraestructura crítica.

5. **Identificar las principales características** de una APT y sus posibles consecuencias en un entorno industrial.

6. **Introducir los aspectos más importantes** asociados a la protección de infraestructuras críticas y las normativas vigentes.

7. **Describir las principales contramedidas** que pueden incluirse para fortificar las redes y protocolos industriales.

8. **Esbozar las principales normas y estándares** relacionados con este entorno que intentan facilitar el despliegue de políticas de seguridad efectivas.

9. **Facilitar recomendaciones y consejos** prácticos que permitan fortificar los sistemas y redes vinculados al ámbito industrial de las organizaciones.

Precio

El curso se realiza en **modalidad "on-demand"** y tiene un precio de **4.500 € con un máximo de 8 personas por curso**. No se incluyen los gastos de desplazamiento. Para solicitar más información o personalizar la oferta te puedes poner en contacto con nosotros a través de:

- **Correo electrónico**: formacion@logitek.es, indicando los siguientes datos: Empresa, nombre y apellidos, teléfono de contacto.

- **Telefónicamente**, llamando al 902 10 32 83 y preguntando por el Departamento de Formación.

Día 1

Conceptos básicos sobre ciberseguridad industrial y principales tipos de ataques a redes OT e infraestructuras críticas.

08.30-10.30 / Ciberseguridad en entornos OT

Sesión 1

- Conceptos básicos asociados a la informática industrial y a la ciberseguridad en entornos OT. Definiciones y vocabulario.
- Identificación de dominios y capas típicamente utilizados en entornos OT.

Sesión 2

- Principales diferencias entre Seguridad IT vs Ciberseguridad OT.
- Evaluación cuantitativa y análisis del riesgo operativo.
- Sistemas de gestión de la seguridad (soluciones específicas OT).

Sesión 3

- Definición y clasificación de vulnerabilidades.
- Metodología de análisis de vulnerabilidades para entornos OT.
- Laboratorio de vulnerabilidades.

11.00-14.00 / Técnicas Hacker en entornos OT

Sesión 4

- Anatomía de un ataque hacker.
- Técnicas de recogida de información (ingeniería social, phishing, sniffing).

Sesión 5

- Técnicas de construcción (spoofing, poisoning MitM, hijacking, inyecciones, forgeries).

Sesión 6

- Técnicas de anonimato
- Consecuencias típicas de los ataques en entornos OT (escalado de privilegios, DoS y DDoS, backdoor access, robos y modificaciones de datos).

15.00-17.00 / Ciberseguridad en entornos OT

Sesión 7

- Virus, gusanos, troyanos, rootkits..
- Introducción a las APT´s.

Sesión 8

- Recorrido por los principales ataques ocurridos en entornos OT (Stuxnet, Duqu, Flame, Shamoon, Dragonfly, Laziok).

Sesión 9

- Definición de infraestructura crítica y conceptos asociados.
- Objeto y alcance de la Ley PIC (Protección de Infraestructuras Críticas).

Industrial Cybersecurity by LOGITEK

AGENDA

Día 2

Principales contramedidas y procedimientos de seguridad.

Industrial Cybersecurity by LOGITEK

Curso Intensivo Ciberseguridad Industrial

08.30-10.30 / Contramedidas de red-arquitectura.

Sesión 10

- Tipos de firewall. Firewalls industriales DPI.
- Arquitecturas segmentadas en entornos OT.
- Configuración de reglas y mejores prácticas.

Sesión 11

- Utilización de VLAN en entornos OT.
- Vulnerabilidades y ataques específicos sobre VLAN.
- Recomendaciones para el despliegue.

Sesión 12

- Segmentación mediante diodo de datos.
- Otras tecnologías de segmentación.

11.00-14.00 / Caso práctico, contramedidas de red-protocolo y red-sistema.

Sesión 13

- Maqueta ciberseguridad. industrial.
- Herramientas para la elaboración de ataques.
- Caso práctico de utilización de firewalls industriales DPI.

Sesión 14

- Criptografía.
- Esquemas IAAA.
- Protocolos industriales seguros:
  - *Seguridad en OPC UA.*
  - *Secure DNP3.*
- Acceso remoto seguro:
  - *VPN IPSec.*
  - *VPN SSL (OpenVPN).*

Sesión 15

- Sistemas de gestión de cambios.
- Tecnologías para control de versiones y generación automática de backups.

15.00-17.00 / Contramedidas de administrador, estándares y mejores prácticas.

Sesión 16

- Soluciones antimalware en entornos OT y gestión de parcheado y actualizaciones.

Sesión 17

- Introducción a la ISA99 y NERC.
- Mejores prácticas desarrolladas por el ICS-CERT, NIST y NERC.
- Otras mejores prácticas.

Sesión 18

- Ciberseguridad en la Industria 4.0 y recopilación de mejores prácticas.

Caso práctico

LOGITEK

real time solutions

Carretera Sant Cugat, 63, Edificio B 1ª Planta
08191 – Rubí (Barcelona)
Tel.:902 10 32 83
www.logitek.es