Ciberseguridad Industrial
by LOGITEK

Curso de Introducción a la Ciberseguridad Industrial

Conceptos, ataques, contramedidas y procedimientos:

Logitek Ciberseguridad Industrial basándose en su experiencia de años en el sector y un conocimiento actualizado de las amenazas existentes, proporciona tecnologías y servicios específicos que ayudan a fortificar los entornos industriales y de infraestructuras y a desplegar estrategias de defensa en profundidad. Uno de los aspectos clave de este tipo de estrategias es la formación y la concienciación.

Este curso de dos días de duración, permitirá a los clientes finales 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 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.

Objetivos

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. Distinguir las diferencias entre las contramedidas de sistema, desarrollador, administrador y usuario.
9. Esbozar las principales normas y estándares relacionados con este entorno que intentan facilitar el despliegue de políticas de seguridad efectivas.
10. Facilitar recomendaciones y consejos prácticos que permitan fortificar los sistemas y redes vinculados al ámbito industrial de las organizaciones.

Fechas cursos de Calendario

Centro	JUNIO	OCTUBRE
Madrid	FINALIZADO	2 y 3 de octubre de 2014
Barcelona	16 y 17 de junio de 2014	22 y 23 de octubre de 2014
Bilbao	FINALIZADO	29 y 30 de octubre de 2014

Precios

Modalidad	Importe
Calendario	1.100€ (por persona)
On-Demand	3.200€ (máximo 8 personas)

Inscripción e información

Para solicitar información o realizar la inscripción en alguno de los cursos de calendario o solicitar la realización de un curso On-Demand, puede hacerlo:

- Enviando un correo electrónico a: **formacion@logitek.es**
  Indicando los siguientes datos: Empresa, nombre y apellidos, teléfono de contacto, modalidad del curso y fecha seleccionada.

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

Agenda

Día 1

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

Sesiones 1, 2 y 3: Ciberseguridad en entornos OT (I), (II) y (III)

9:30 a 11:30

- 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.
  - Sistemas de gestión de la seguridad (soluciones específicas OT).
- Sesión 3
  - Definición y clasificación de vulnerabilidades.
  - Metodología de análisis de vulnerabilidades para entornos OT.
  - Medición de impacto de vulnerabilidades.

Sesiones 4, 5, 6 y 7: Técnicas hacker en entornos OT (I), (II) , (III) y (IV)

12:00 a 14:00

- Sesión 4
  - Anatomía de un ataque hacker.
  - Técnicas de recogida de información (ingeniería social, phishing, sniffing).
- Sesión 5
  - Técnicas de construcción (MitM, hijacking, spoofing, poisoning, forgery).
- Sesión 6
  - Técnicas de anonimato (steganography, tunneling, bouncering).
  - Consecuencias típicas de los ataques en entornos OT (escalado de privilegios, DoS, backdoor access, robos y modificaciones de datos).
- Sesión 7
  - Virus, gusanos, troyanos, rootkits y herramientas antimalware.

Sesión 8: Introducción a las APTs

15:30 a 16:10

- Anatomía de un ataque tradicional vs APTs.
- Evolución de las APTs y ejemplos actuales.
- Cibercrimen y ciberguerra.

Sesión 9: Infraestructuras críticas y legislación vigente

16:10 a 16:50

- Definición de infraestructura crítica y conceptos asociados.
- Idiosincrasia del sector agua y sector energía como infraestructuras críticas.
- Panorama nacional e internacional en la gestión PIC.

Sesión 10: Recorrido por los principales ataques ocurridos en entornos OT

16:50 a 17:30

- Descripción.
- Análisis de ejecución y consecuencias.
- Contramedidas que hubieran mitigado el impacto del ataque.

Día 2

Principales contramedidas y procedimientos de seguridad

Sesiones 11, 12 y 13: Contramedidas de red-arquitectura (I), (II) y (III)

9:30 a 11:30

- Sesión 11
  - Segmentación de redes.
  - Tipos de firewall.
  - Reglas típicas de configuración.
- Sesión 12
  - DMZs.
  - Mejores prácticas de configuración.
- Sesión 13
  - Otras tecnologías y formas de segmentación.

Sesión 14: Contramedidas de red-protocolo

12:00 a 12:40

- Criptografía a diferentes niveles.
- Protocolos industriales seguros: OPC versus OPC UA, DNP3 Secure, otros protocolos.
- IPSec y VPN seguras.

Sesión 15: Contramedidas de sistema

12:40 a 13:20

- Políticas de autentificación.
- Sistemas de certificados.

Sesión 16 y 17: Contramedidas de desarrollador, administrador y usuario (I) y (II)

13:20 a 14:00
15:30 a 16:10

- Antimalware y actualizaciones.
- Tecnologías para control de versiones y generación automática de backups.

Sesión 18: Normativas, estándares y mejores prácticas

16:10 a 16:50

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

Sesión 19: Recopilación de mejores prácticas

16:50 a 17:30

- Recopilación