vitc Vester Industrial training center

WORKSHOPS & CURSOS ESPECIALIZADOS EN INGENIERÍA INDUSTRIAL

Ciberseguridad en entornos Industriales e Infraestructuras críticas

www.vestertraining.com

Ciberseguridad en entornos Industriales e Infraestructuras críticas

Formación y asesoramiento en materia de ciberseguridad en todos los niveles de la organización: concienciación, análisis, implantación, evaluación y seguimiento de las acciones.

Aprende los conceptos básicos, tipos de ciberataques, aplicación de sistemas anti-intrusión, control de seguridad informática y firewalls de diodo.

Descripción general

Curso de tres días que tiene como objetivo que el alumno conozca de forma genérica la Ciberseguridad en Entornos Industriales e Infraestructuras Críticas, los aspectos más importantes de la misma y las formas básicas de protegerse ante ciberataques.

El curso consta de una parte teórica, seguida de una parte práctica. Al término del curso, el alumno dispondrá de un repositorio de software libre con todas las herramientas de test utilizadas durante los tres días.

Al finalizar el curso, el alumno tendrá los conocimientos teóricos y prácticos para:

- Evaluar las amenazas y realizar una auditoría de sus sistemas de control y supervisión.
- Obtener la lista de puntos críticos y su relación directa con las contramedidas a aplicar.
- Proteger los puntos más críticos de su instalación y saber qué hacer con los menos críticos.
- Instalar y/o configurar un equipo de protección de acceso físico.

Objetivo general

- Aplicación de sistemas anti-intrusión, control de seguridad informática y firewall de equipos.
- Proporcionar una visión general acerca de los conceptos más importantes asociados al área de la ciberseguridad industrial.
- Analizar las principales vulnerabilidades y amenazas que se pueden sufrir en entornos industriales.
- Conocer los diferentes tipos de ciberataques que pueden realizarse a una red OT o una infraestructura crítica.
- Describir las principales contramedidas que pueden incluirse para fortificar las redes y protocolos industriales.
- Facilitar recomendaciones y consejos prácticos que permitan fortificar los sistemas y redes vinculados al ámbito industrial de las organizaciones.
- Dar a conocer las principales normas y/o leyes actuales y futuras, en la aplicación de las contra medidas.

¿A quién va dirigido?

Este curso está diseñado para formar a técnicos e ingenieros involucrados en la protección de sistemas críticos industriales y la aplicación de medidas de seguridad en entornos PLC / SCADA / MES.

Se dirige principalmente al personal técnico que participa en el diseño de arquitecturas, instalación, configuración, mantenimiento y puesta en marcha de proyectos de supervisión y/o automatización de sistemas de telecontrol.

Características del curso

- **Modalidades:** Presencial o virtual online en vivo con desarrollo de prácticas supervisadas que complementarán las explicaciones dadas.
- **Metodología:** Charlas magistrales y talleres de práctica.
- **Participantes:** Una cantidad mínima de 5 y una cantidad máxima de 12.

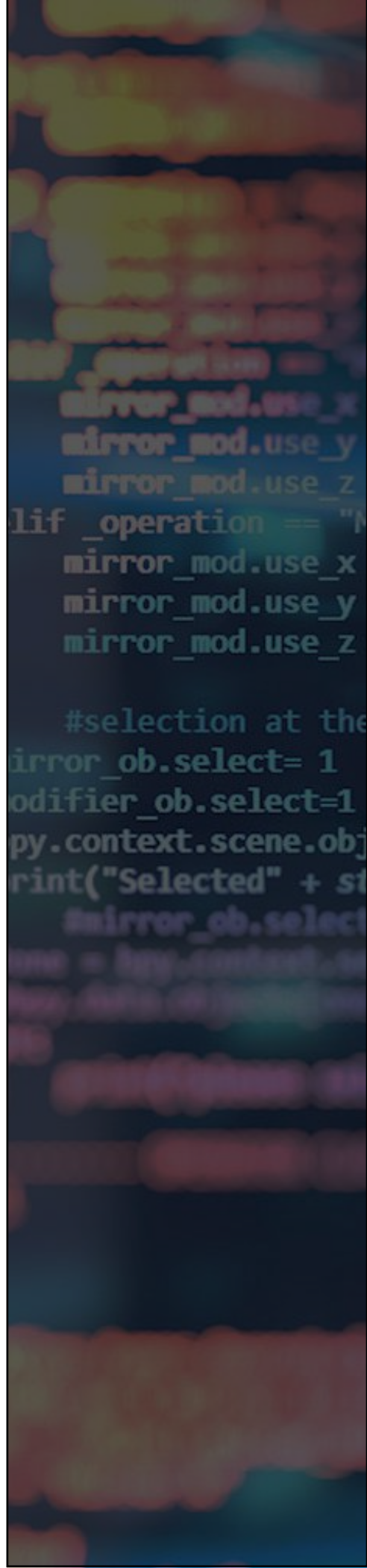
Observaciones del curso

Cualquier módulo o sub-módulo del curso podrá ser ampliado y detallado en una segunda sesión ideada a medida del cliente. De esta forma, se ofrece un primer "briefing" del curso básico pudiendo complementarse en sucesivos cursos.

Material inlcuido

- Manual de formación.
- Acceso a la clase virtual (formato online).
- Documento digital de certificación otorgado por VITC.

*Todo el material necesario será enviado por email unos días antes del curso.



Temario del curso

Día 1

Introducción a la seguridad Informática:

¿Qué es el hacking?
Propiedades de la seguridad de la información: confidencialidad, integridad / 'non-repudiation' y disponibilidad.

Networking Basics

¿Cómo funciona un switch?
¿En qué protocolos se basan las redes industriales?
¿Por qué Ethernet es vulnerable?

Autenticación y autorización:

Riesgo, amenaza, vulnerabilidad (+CVSS), Exploit y Zero Day.
Principales diferencias entre Seguridad IT y Ciberseguridad en entornos industriales.
* Práctica.

Ataques y Malware:

Tipos de ataques:
Según acciones del atacante: activos y pasivos.
Según la localización del atacante: internos y externos.
*Práctica.

Fases de un ataque I:

Reconocimiento.
Recopilación de información.

Fases de un ataque II:

Escaneo.
Explotación.

Temario del curso

Día 2

Fases de un ataque III:
Mantener acceso.
Cubrir las huellas.
*Práctica.

Auditorias de seguridad I:
Tipos: White Box, Gray Box y Black Box.
Limitaciones: tiempo, alcance, test permitidos y conocimientos.
Reporting.
Auditoría desde Internet.
Auditoría desde la red interna.

Auditorias de seguridad II:
Trabajo sobre los equipos.
Ejecución de entrevistas de los miembros de la organización.
*Práctica.

Seguridad redes industriales I:
Seguridad en redes cableadas:
Conceptos básicos de las redes cableadas.
Sniffers: TCPDump, WireShark.
Seguridad física: Port Security.

Seguridad redes industriales II:
Seguridad DHCP: DHCP Snooping.
Seguridad RSTP: BPDU Guard, Root Guard.
MiTM: IP Source Guard.
VPNs.

Temario del curso

Día 3

Contramedidas y protección I:
Tecnologías de defensa y protección.
Arquitectura perimetral de defensa.

Contramedidas y protección II:
Decálogo de gestión y protección.
Seguridad física.
Firewalls, IDS, IPS y SIEMs.
Disaster Recovery Plan.

Criptografía I:
Simétrica: DES, AES, RC4.
Asimétrica: RSA, GPG, IKE, SSL.

Criptografía II:
Hashes: MD5, SH.
Password cracking: fuerza bruta, hash tables y rainbow tables.

Información del curso

Duración del curso:

3 días

Modalidades:

Online

Presencial

Privado

Idiomas disponibles:

Español

Inglés

Contacto:

Paula Garibay

Email:

p.garibay@vestersl.com

Teléfono:

(+34) 935 721 007 / (+34) 660 997 665

Organizado por
Vester Industrial Training Center

info@vitrainingcenter.com
www.vestertraining.com

España y Portugal
(+34) 935 686 178
(+34) 650 199 175

Costa Rica
(+506) 2225-2344

México
(+52) 55 46282593