vitc Vester Industrial training center

CERTIFIED WORKSHOPS FOR INDUSTRIAL ENGINEERING

CYBERSECURITY FOR INDUSTRIAL ENVIRONMENTS AND CRITICAL INFRASTRUCTURES

Online based theoretical Workshop with real practices.

Organized by Vester Industrial Training Center
Paula Garibay
Ph: (+34) 935 721 007 | Mobile: (+34) 660 997 665
Email: p.garibay@vestersl.com
www.vestertraining.com

CYBERSECURITY for INDUSTRIAL ENVIRONMENTS and CRITICAL INFRASTRUCTURES

Cybersecurity training and consulting aimed to all levels of the organization: awareness, analysis, implementation, evaluation and actions monitoring.

Learn the basics notions, attacks types, anti-intrusion systems application and IT security control and diode firewalls.

GENERAL DESCRIPTION

Three-day workshop designed with the aim of learning the general concepts of **Cybersecurity at Industrial Environments and Critical Infrastructures**, as well as its most important aspects and the basic protection against attacks.
The workshop includes a theoretical part, followed by a practical part. At the end of the training, the student will be provided with free software with all the test tools used during the three days training.

At the end of the course, the student will have the theoretical and practical knowledge to:

- Evaluate threats and audit their monitoring and control systems.
- Obtain a list of critical points and their direct relationship with the applied countermeasures.
- Protect the most critical points of your installation and know what to do with the least critical ones.
- Install and / or configure protection equipment with physical access.

AIMED AT:

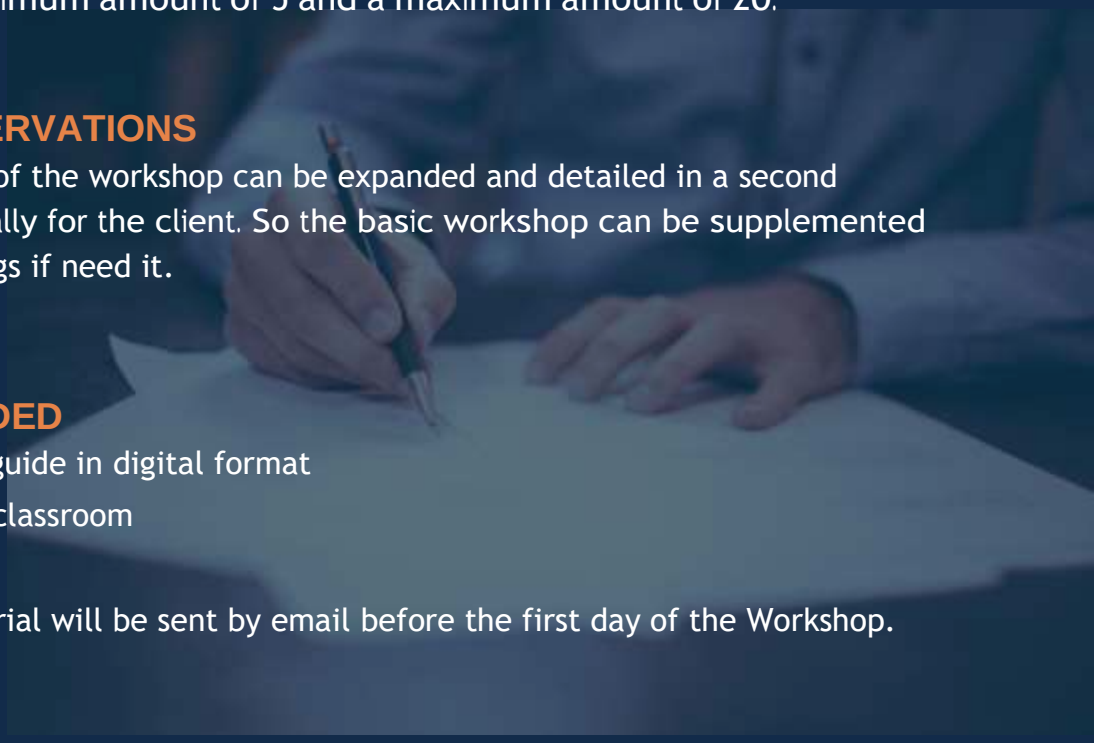
This workshop is designed to train technicians and engineers involved in the protection of critical industrial systems and the security measures implementation for PLC / SCADA / MES environments.
It is mainly aimed at technical personnel involved in the design of architectures, installation, configuration, maintenance and supervision projects commissioning and / or remote control systems automation.

GENERAL OBJECTIVE

- Anti-intrusion systems application, computer security control and equipment firewall.
- Provide a general overview of the most important concepts associated with industrial cybersecurity.
- Analyze the main vulnerabilities and threats that may be experienced at industrial environments.
- Know the different types of hacker attacks that can be carried out on an OT network or a critical infrastructure.
- Describe the main countermeasures that can be included to fortify industrial networks and protocols.
- Provide recommendations and practical advice to strengthen the company's industrial systems and networks.
- Introduce the main standards and/or the current and future laws regarding the implementation of said countermeasures.

WORKSHOP CHARACTERISTICS:

- Mode: Online with supervised practices as complement to the theory.
- Methodology: Keynote lectures and practical workshops.
- Participants: A minimum amount of 5 and a maximum amount of 20.



WORKSHOP OBSERVATIONS

Any topic or sub-topic of the workshop can be expanded and detailed in a second session tailored specially for the client. So the basic workshop can be supplemented with successive trainings if need it.

MATERIAL INCLUDED

- Manual and exercise guide in digital format
- Access to the virtual classroom
- Digital certificate

All the necessary material will be sent by email before the first day of the Workshop.

WORKSHOP SCHEDULLE

Day 1	Day 2	Day 3
Introduction to computer security: - What is hacking? - Information security properties: confidentiality, integrity / non-repudiation and availability	**Attack stages III:** - Maintain Access - Cover the tracks * Practice	**Countermeasures and protection I:** - Defense and protection technologies. -Perimeter defense architecture
- Authentication and authorization - Risk,Threat, Vulnerability (+ CVSS), Exploit and Zero Day - Main differences between IT Security and Cybersecurity in Industrial Environments * Practice	**Safety Audits I:** - Types: White Box, Gray Box and Black Box - Limitations: time, scope, allowed tests and knowledge - Reporting - Auditing from the Internet -Auditing from the internal network	**Countermeasures and protection II:** - Management and protection Decalogue. Physical security Firewalls, IDS, IPS and SIEMs
Attacks and Malware: Types of attacks: - According to the actions of the attacker: assets and liabilities - According to the location of the attacker: internal and external * Practice	**Safety Audits II:** - Work on equipment - Interviews with the organization members * Practice	**Cryptography I:** - Symmetric: DES, AES, RC4 - Asymmetric: RSA, GPG, IKE, SSL
Attack stages I: - Recognition - Information gathering **Attack stages II:** - Scanning - Exploitation	**Industrial networks safety I:** - Security in wired networks: - Wired networks basic concepts - Sniffers: TCPDump, WireShark - Physical security: Port Security **Industrial networks safety II:** - DHCP Security: DHCP Snooping - RSTP Security: BPDU Guard, Root Guard - MiTM: IP Source Guard - VPNs	**Cryptography II:** - Hashes: MD5, SH - Password cracking: brute force, hash tables and rainbow tables