+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 29/11/2023

Sign up

ICS / SCADA Training Industrial Control Systems Security

5 days (35 hours)

PRESENTATION

ICS industrial control systems, commonly known as SCADA systems, control industrial infrastructures. Most critical infrastructures are controlled by ICS/SCADA systems: from power grids to water treatment, from the pharmaceutical, automotive and chemical industries to transportation. This training course addresses the need for engineers and operators of control systems to better understand the important role they play in cybersecurity. This starts with ensuring that a control system is designed with cybersecurity built in, and that cybersecurity has the same level of sensitivity as system reliability throughout the system's lifecycle.

OBJECTIVES

- Understanding the business and its issues
- Control the attack surface of an ICS/SCADA system
- Know and understand standards specific to the industrial world
- Securing your ICS/SCADA systems
- Developing a cybersecurity policy

TARGET AUDIENCE

- Safety managers/experts
- Industrial project managers

Prerequisites

- Good general knowledge of IT and information systems security.
- Basic knowledge of industrial systems and ICS/SCADA control systems

PROGRAMME OF OUR cybersecurity retraining course: DEVSECOPS

Introduction to cybersecurity for ICS/SCADA systems

- ICS attack surface
- Threat sources and reasons for attack
- Leading surface and entrances
- Attack Level 0 and 1
- Control of things platform
- Exercise: Finding passwords in EEPROM dumps
- Purdue Level 0 and 1 Technologies & Communications
- Fieldbus protocol families

ICS/SCADA & Information Systems

- Ethernet and TCP/IP
- Ethernet & TCP/IP Concepts
- ICS protocols over TCP/IP
- Wireshark and ICS
- Attacks on networks: Listing Modbus TCP
- ICS attack surface
- Attacks on HMIs and user interfaces
- Attacks on control servers
- Attacks on network communications
- Attacks on remote devices

Securing ICS/SCADA systems

- Windows & Linux in ICS
- Updates and patching
- Processes and services Configuration hardening
- Endpoint defense
- Automation and auditing
- Log, database and history management

Industrial network organizational security

- SCADA architecture
- Determining zones and pipes
- Architecture security
- Determining ANSSI classification levels

Practical exercises

- PLC programming, HMI
- Secure TCS architecture
- Finding passwords in embedded devices
- Explore Fieldbus protocols
- Forensic attack
- Bypassing Auth with SQL Injection
- Password fuzzing
- Baselining with PowerShell
- Configuring host-based firewalls
- Windows event logs
- Find remote access

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.