# ICS410: ICS/SCADA Security Essentials

## Course Overview

Threat hunting and incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident or contain propagating ransomware. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions. This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and ransomware operators.ate their moves and build better defenses.

ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

## Job Roles

| |
|---|
| IT (includes operational technology support) |
| IT security (includes operational technology security) |
| Engineering |
| Corporate, industry, and professional standards |

## NICE Framework Work Roles

- Process Control Engineer / Instrument & Control Engineer (ZZ-ICS-001)
- ICS/SCADA Security Engineer (ZZ-ICS-002)
- ICS/OT Systems Engineer (ZZ-ICS-003)
- OT SOC Operator (ZZ-ICS-004)

## Prerequisites

Course participants need to have a basic understanding of networking and system administration, TCP/IP, networking design/architecture, vulnerability assessment, and risk methodologies. ICS410 covers many of the core areas of security and assumes a basic understanding of technology, networks, and security. For those who are brand new to the field and have no background knowledge, SEC301: Intro to Information Security would be the recommended starting point. While SEC301 is not a prerequisite, it provides introductory knowledge that will help maximize a student's experience with ICS410.

## Duration

6 Days

## Certifications

Global Industrial Cyber Security Professional (GICSP)

## Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

## Connect with us

APPLIED TECHNOLOGY ACADEMY

## Sign Up Today!

AppliedTechnologyAcademy.com

# ICS410: ICS/SCADA Security Essentials

## Course Outline

### SECTION 1: ICS Overview
**TOPICS:** ICS Overview, Global Industrial Cybersecurity Professional (GICSP) Overview, Secure ICS Network Architectures, Physical and Cyber Security

### SECTION 2: Architectures and Processes
**TOPICS:** Field Devices and Controllers, ICS Attack Surface, Safety Instrumented Systems (SIS), Secure ICS Network Architectures, Purdue Level 0 and 1

### SECTION 3: Communications and Protocols
**TOPICS:** Supervisory Systems, Ethernet and TCP/IP, Wireless Attacks and Defenses, Enforcement Zone Devices

### SECTION 4: Supervisory Systems
**TOPICS:** Workstations and Servers, Supervisory Servers, User Interfaces, Defending Microsoft Windows, Patching ICS Systems, Understanding Basic Cryptography, Wireless Technologies, Wireless Attacks and Defenses

### SECTION 5: ICS Security Governance
**TOPICS:** ICS Security Governance, Defending Unix and Linux, Endpoint Protection and SIEMS, Building an ICS Cyber Security Program, Creating ICS Cyber Security Policy, Measuring Cyber Security Risk, Incident Response, Final Thoughts and Next Steps

### SECTION 6: Capstone CTF
Students will work through a capture-the-flag (CTF) game based on an incident response exercise. Students must use the knowledge they gained throughout the week to identify indicators of compromise (IoCs), determine actions that should be taken to limit the attacker's ability to compromise additional assets and react to changes in the attacker's tactics, techniques, and procedures (TTPs) as they progress deeper into the OT/ICS network.

## Course Objectives

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints.
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals.

## Global Industrial Cyber Security Professional (GICSP)

The Global Industrial Cyber Security Professional (GICSP) certification is a vendor-neutral, practitioner focused certification that bridges IT, engineering, and cyber security to achieve security throughout the industrial control systems lifecycle. The GICSP assesses a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

- Industrial control system components, purposes, deployments, significant drivers, and constraints
- Control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals