ICS612: ICS Cybersecurity In-Depth

ICS-AWARE MALWARE AND ATTACKS ON CRITICAL INFRASTRUCTURE ARE INCREASING IN FREQUENCY AND SOPHISTICATION. YOU NEED TO IDENTIFY THREATS AND VULNERABILITIES AND METHODS TO SECURE YOUR ICS ENVIRONMENT. LET US SHOW YOU HOW!

The ICS612: ICS Cybersecurity In-Depth course will help you:

• Learn active and passive methods to safely gather information about an ICS environment
• Identify vulnerabilities in ICS environments
• Determine how attackers can maliciously interrupt and control processes and how to build defenses
• Implement proactive measures to prevent, detect, slow down, or stop attacks
• Understand ICS operations and what “normal” looks like
• Build choke points into an architecture and determine how they can be used to detect and respond to security incidents
• Manage complex ICS environments and develop the capability to detect and respond to ICS security events

The course concepts and learning objectives are primarily driven by the hands-on focused labs. The in-classroom lab setup was developed to simulate a real-world environment where a controller is monitoring/controlling devices deployed in the field along with a field-mounted touchscreen Human Machine Interface (HMI) available for local personnel to make needed process changes. Utilizing operator workstations in a remotely located control center, system operators use a SCADA system to monitor and control the field equipment. Representative of a real ICS environment, the classroom setup includes a connection to the enterprise, allowing for data transfer (i.e., Historian), remote access, and other typical corporate functions.

The labs move students through a variety of exercises that demonstrate how an attacker can attack a poorly architected ICS (which, sadly, is not uncommon) and how defenders can secure and manage the environment.

“I loved that this course was lab heavy. I feel 100% more comfortable around OT equipment now. That’s saying a lot since my background and experience has been strictly IT.”

—Jim J., Pilot Flying J

“The pods and student kits offered provide a powerful, hands-on learning experience that exceeded expectations far beyond what any software simulation or slide-based lecture could do. Step-by-step instructions are good, but I really enjoyed when we had exercises that didn’t have all the answers and forced the student to think critically about how to solve the problem. That’s where real learning occurred for me.”

—Joseph P., Deloitte & Touche LLP
**Section Descriptions**

**SECTION 1: The Local Process**
Learning objectives:
- Review of Lab Setup
- Introduction to the PLC Platform Application Tools
- Introduction to Programming a PLC
- Service Discovery on PLC
- Introduction to the HMI Platform Application Tools
- Understand HMI to PLC Communication

**TOPICS:** Process familiarization using the Purdue model; Communication flow mapping referencing the Zones and conduit approach; Components of Level 0-2; Local I/O and local HMI communications; Understand operational functions; Understand inherent process weaknesses; Protocol dissection of operational data; Embedded device essentials; Operator Interface (I/O) subsystems and communications; Safety systems: Process time

**SECTION 2: System of Systems**
Learning objectives:
- Introduction to Peer-to-Peer Communications
- Introduction to SCADA Systems
- OPC Communications

**TOPICS:** Learn components of Level 3; Learn peer-to-peer communications between PLCs; Learn SCADA/OPC communications; Learn the use and dependencies of traditional IT services (DNS, AD, DHCP, NTP, etc.); Vendor security models and industrial DMZs; Learn attack vectors and defense techniques from Level 3

**SECTION 3: ICS Network Infrastructure**
Learning objectives:
- Network Architecture and Technology in ICS
- ICS Firewalls
- ICS Perimeter
- Historians
- Remote Access and Jump Host/2FA

**TOPICS:** Understand connected process; Analyze case studies in ICS environments and secure plant design; Identify typical trusted communications flows (Time, File sharing, Remote Access, Historians, AD replication, Reverse Web Proxies, Patch servers)

**SECTION 4: ICS System Management**
Learning objectives:
- ICS System Monitoring and Logging
- ICS Asset Management
- ICS Asset Validation

**TOPICS:** Logging and traffic collection in an ICS environment; Monitoring and alerting in ICS networks; Monitoring and alerting in a serial network; System integrity verification

**SECTION 5: Covfefe Down!**
Learning objective:
- Hands-on environment troubleshooting
- Attack/Defend – ICS NetWars Style Challenge

**TOPICS:** Pivoting and positioning in an ICS target environment; Operational traffic reverse engineering; Protocol-level manipulation; Firmware manipulation; Industrial wireless discovery and attack; Time synchronization manipulation; Data table and scaling modifications

**Who Should Attend**

- ICS410 course alumni – students who have successfully completed ICS410: ICS/SCADA Security Essentials will have the base knowledge considered as a prerequisite for this course.
- Process control engineers
- Systems or safety system engineers
- Active defenders in ICS
- Anyone with significant control system experience interested in understanding processes and methods to secure the ICS environment

“The training starts with theory and quickly progresses into full hands-on interaction with all components. This experience is not easy to find. It is an amazing course.”
— Bassem Hemida, Deloitte