ICS410: **ICS/SCADA Security Essentials**

GICSP
Industrial Cyber Security Professional
giac.org/gicsp

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model.
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense to detect host and network-based intrusions via intrusion detection technologies
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, the Center for Internet Security Critical Security Controls, and COBIT 5

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. 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 (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS 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

Author Statement

This course provides students with the essentials for conducting cybersecurity work in industrial control system environments. After spending years working with industry, we believe there is a gap in the skill sets of industrial control system personnel, whether it be cybersecurity skills for engineers or engineering principles for cybersecurity experts. In addition, both information technology and operational technology roles have converged in today's industrial control system environments, so there is a greater need than ever for a common understanding between the various groups who support or rely on these systems. Students in ICS410 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

– Justin Searle

Section Descriptions

SECTION 1: ICS Overview

Students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

TOPICS: Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Purdue Levels 0 and 1; Purdue Levels 2 and 3; IT & ICS Differences; Physical and Cybersecurity

SECTION 2: Architectures and Field Devices

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During Section 2, students will develop a better understanding of where these specific attack vectors exist and more defensible architectures for OT/ICS. Students will look at different technologies and communications used in Perdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from the PLCs they programmed in Section 1 and look at what other fieldbus protocols used in the industry.

TOPICS: ICS Attack Surface; Secure ICS Network Architectures; Purdue Level 0 and 1

SECTION 3: Communications and Protocols

Section 3 will take students through the communication protocols often found throughout control networks. Students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol. Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each.

TOPICS: Ethernet and TCP/IP; Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses

SECTION 4: Supervisory Systems

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. After a hand-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Perdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks. In the afternoon, students will learn about how to create baselines and secure Windows-based workstation and servers.

TOPICS: Supervisory Servers; User Interfaces; Defending Microsoft Windows; Patching ICS Systems

SECTION 5: ICS Security Governance

Section 5 will further explore baselines and hardening, but his time on Linux-based workstations and servers. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Finally, students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments.

TOPICS: Defending Unix and Linux; Endpoint Protection and SIEMS; Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Measuring Cybersecurity Risk; Incident Response; Final Thoughts and Next Steps

SECTION 6: Capstone Exercise

Students will work through a group-based, table-top exercise (TTX) that includes hands-on components. 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/OCS network. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

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

"A mix of hands-on and theoretical class, being driven by a highly skilled instructor, makes this the best training in ICS security."

— Rafael Issa, **Technip**