ICS418: **ICS Security Essentials for Leaders™**

2	12	Laptop
Day Course	CPEs	Required

You Will Be Able To

- Articulate the value of ICS security and tie cyber risk to business risk decisions
- Trend current and future technology changes to address business needs
- Measure successes in industrial cyber risk management, complete with metrics for executives and boards
- Use best practices to enable ICS security incident detection and response for their teams
- Leverage external information, including threat intelligence, to guide their ICS security program
- Provide governance, oversight, execution, and support across industrial facilities for ICS security initiatives and projects
- Apply the differences between IT and ICS security for an effective control system cybersecurity program
- Develop their security workforce to address gaps in hiring, training, and retention
- Apply advanced techniques to help shape and shift their organization's culture of security

Prerequisites

- Students with backgrounds in IT, ICS, and/or management will do well with this course.
- Students should also have:
- A strong desire to lead people and manage processes to improve ICS security
- Willingness to apply lab exercises and content to their unique industrial organization
- The ability to stretch outside of their comfort zone

What You Will Receive

- Access to Cyber42: Industrial Edition for management-based skills development with applicable business oriented decision making
- Editable leadership drills designed for students to build new strategy and program elements and continuing their development long after the course ends

ICS security is an ever-changing field requiring practitioners to continually adapt defense strategies to meet new challenges and threats. To compound the issue, any security changes need to be thoroughly tested to maintain the safety and reliability of industrial operations.

Globally, "critical infrastructure" and "operators of essential services" represent hundreds of thousands—if not millions—of industrial organizations. Some of them are the lifelines to our modern society, like water, power, oil and gas, food processing, and critical manufacturing—but every industrial facility owner or operater must know their engineering processes are safe and secure. With increased threats, new technology trends, and evolving workforce demands, it is vital for security leaders in operational technology (OT) to be trained in techniques to defend their facilities and their teams.

The two-day ICS418 fills the identified gap amongst leaders working across critical infrastructure and OT environments. It equips new or existing leaders responsible for OT/ICS, or converged IT/OT cybersecurity. The course provides the experience and tools to address industry pressures to manage industrial cyber risk to prioritize the business, safety and the reliability of operations. ICS leaders will leave the course with a firm understanding of the drivers and constraints that exist in these cyber-physical environments and will obtain a nuanced understanding of how to manage the people, processes, and technologies throughout their organizations.

This Course Will Prepare You To

- Develop ICS-specific cybersecurity programs and measure its impact across the organization
- Use management and leadership skills to communicate your ICS security vision to executives and other leaders
- Build (and keep) your ICS security team, using forecasting, capability modeling, and workforce planning
- Assess the overall effectiveness of your organization's industrial cyber risk management program
- Manage the various constraints across IT, OT, engineering, and physical security to improve your organization's culture

> **"The lessons taught in this class helped me to prepare myself to approach upper management about getting cyber defenses on the OT networks."**
>
> —Vickram R., **Eastern Generating Company**

Section Descriptions

SECTION 1: ICS Security Leader Core Development & Responsibilities

Industrial control systems (ICS) security leaders must be able to create and sustain cybersecurity programs with challenging constraints. These leaders must be able to manage industrial cyber risks, plan for evolving technologies, and incorporate ICS-specific security standards. On the first day, students will learn the differences between traditional information technology (IT) and operational technology (OT) systems, as well as the associated threats, vulnerabilities, and potential impacts from ICS-specific cyber-attacks. Once these elements of industrial cyber risk are established, students will explore using industry best practices, guidelines, and standards to assess and measure ICS security programs.

TOPICS: Overview of ICS and Critical Infrastructure; Attack History and Modern Adversaries; Cybersecurity Risk, Impacts, Goals and Safety; ICS Technology Trends; IT and OT Security Differences; ICS Incident Response Management; Industrial Cyber Risk Management; ICS Policy, Frameworks, Regulations, and Compliance; Strategy Planning and Tactical Priorities

SECTION 2: ICS Security Team Development Focus

The second section of this course builds on the concepts around building an ICS security program and explores the workforce needs to manage the day-to-day tasks, planning, and reporting required to minimize cyber risk. Students will be equipped with a common understanding of the ICS security and safety culture, the skills required to perform various job functions, and both company-wide and team-specific security controls.

TOPICS: Governance, Oversight, Execution, and Support; Dedicated ICS Security Efforts and Measuring Value; Organization Roles and Responsibilities; Key Performance Indicators; Building and Maturing Effective ICS Security Teams; Building and Maturing ICS Cyber Defense Programs; ICS Security Awareness and Safety Culture; Executive Metrics and Communications

Authors Statement

Now, more than ever, it is important to train and equip ICS security leaders with the skills and knowledge they need to protect critical infrastructure—the critical engineering systems that make, more and power our world. This course is the culmination of decades of experience in building and managing OT/ICS security teams—and it is the course we wish was available to us when we started on our ICS security journey. We've drawn across our roles in different industrial sectors and teams—as former company executives, team leads, incident responders, and managers—to create a course empowering leaders facing the greatest challenge of our time: industrial control system cybersecurity.

—Jason D. Christopher & Dean C. Parsons

> **"This course is a must for managers in the ICS space, and I am sure many people out there are probably trying to build an OT security program based on IT standards and guidelines. This course did a great job of pointing out those differences and will benefit anyone that attends in the future."**
>
> —Jason R., **MP Materials**

Who Should Attend

ICS418 is aimed at leaders of staff who are responsible for securing the day-to-day running of operational technology and industrial control system environments across an organization—this includes distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Leaders of these teams often come from a diverse background with either a focus on management skills and minimal understanding of ICS environments, or technical individuals who rise in the ranks to a leader with minimal management skill development.

The course was designed to bridge the gap between those two skill sets, "raising the water level for all ships" when it comes to ICS security leaders, including:

- **Leaders asked to "Step-Over"**
  - Traditional information technology (IT) security manager that must create, lead, or refine an ICS Security program
- **Practitioner to Leader: "Step-Up"**
  - Industrial engineer, operator, or ICS security practitioner promoted to a manager position to create, lead, or refine an ICS security program
- **Leader Development: "In-Place"**
  - An existing ICS security manager that is looking to further develop their leadership skills, specific to industrial security

NICE Framework Work Roles

- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator