Course Overview

Industrial security should be ingrained in your company's culture, equivalent to safety. Cyber incident preparedness begins with people. This class starts from a strategic perspective, helping students "get their head around" the big picture. It introduces beginner to intermediate topics such as OT/ICS vulnerabilities, "hacker" methodologies, and security controls at a comfortable and easy to follow pace. These topics are then exercised and reinforced using ThreatGEN® Red vs. Blue cybersecurity training game and other hands-on simulations.

This course will help students gain an understanding of the overall cyber risk management program and strategy, as well as OT/ICS vulnerabilities, basic adversary methods, and the security controls and strategies to defend against them.

What will you get out of this course?

- ✓ Gain a comprehensive, "big picture" understanding of how all the cybersecurity pieces work together.
- ✓ An introductory overview of the concepts, function, and components of industrial control systems, equipment, and technology
- ✓ Learn vulnerabilities and attack vectors specific to ICS.
- ✓ Learn about the methods and strategies hackers use to attack industrial control systems as well as traditional IT systems *(Introductory level. This is not a technical hands-on, "hacking" course)*
- ✓ Learn and apply practical industrial cybersecurity and risk management concepts.
- ✓ Learn how to deploy efficient and cost-effective mitigation strategies and security controls
- ✓ Learn how to build a complete ICS cyber security program.
- ✓ Apply what you've learned against a live adversary using the cutting-edge, turn-based computer training simulation/game, *ThreatGEN Red vs. Blue*
- ✓ Learn how to respond to, adapt, and defend against active attacks *(Introductory level, this is not an incident response or threat hunting class)*
- ✓ Participate as the blue team and the red team, regardless of experience or technical skill level.
- ✓ Taught by world-renown ICS cybersecurity experts with years of real-world experience.

Intended Audience

- Anyone interested in gaining beginner to intermediate knowledge of ICS/OT cybersecurity
- Anyone interested in or tasked with ICS/OT risk assessment and management.
- Anyone interested in gaining a better understanding over the overall cybersecurity "big picture."
- Cybersecurity managers
- Upper management concerned with IT/OT cybersecurity
- Plant managers and asset owners
- IT cybersecurity staff tasked with ICS/OT cybersecurity
- Engineers tasked with ICS/OT cybersecurity
- End users looking for a more effective (and entertaining) cybersecurity awareness training.

Course Syllabus

1. What is OT Cybersecurity
2. ICS/OT Primer
3. OT Threat Landscape
4. OT Cybersecurity/Risk Management Programs
5. OT Cybersecurity/Risk Management Strategies
6. The Risk Assessment Process
7. Vulnerabilities Primer
8. ICS Specific Vulnerabilities
9. OT Attack Surface
10. Cybersecurity Basics: "Blocking and Tackling"
11. OT Cybersecurity Architecture
12. Introduction to OT Threat Monitoring
13. Introduction to OT Cyber Incident Response