Course Outline: Introduction to ICS/OT Cyber Security A picture containing sky

Description automatically generated

Industrial Control Systems (ICS) and Operational Technology (OT) run the world around us. Power plants, offshore oil rigs, trains and other transportation systems, manufacturing plants – these are just a few examples of the critical infrastructure that society depends on. Each ICS/OT environment is unique and has specialized security requirements.

Protecting critical infrastructure becomes more important each day as the frequency of cyber-attacks and the number of attackers continues to grow. Nation state adversaries are no longer the only ones targeting these specialized environments. Today’s attackers include ransomware groups, hacktivists, cyber mercenaries, and more.

ICS/OT cyber security can seem complicated and even daunting at first, but it does not have to be. This course will help participants understand the fundamentals of how these environments operate and how to secure such specialized networks.

**Requirements**

None. Understanding IT, networking and cyber security basics is helpful but not necessary to learn about ICS/OT cyber security.

**Who Should Take This Course**

Anyone wanting to learn more about ICS/OT environments and the cyber security of their networks including, but not limited to:

* Cyber security professionals
* ICS/OT engineers and other automation professionals
* IT professionals
* Individuals wanting to take the follow up course – “Penetration Testing for ICS/OT Networks”

If you have any questions about the course, please do not hesitate to contact me at michael@utilsec.com or on LinkedIn (linkedin.com/in/mikeholcomb).

**About the Instructor**

Michael Holcomb is the Fellow of Cybersecurity and the ICS/OT Cybersecurity Global Lead for Fluor, one of the world’s largest engineering, procurement, and construction companies. His current role provides him with the opportunity to work in securing some of the world’s largest ICS/OT environments, from power plants and commuter rail to manufacturing facilities and refineries. He is currently completing his Master’s thesis on the attack surface of Programmable Logic Controllers (PLCs) with the SANS Technology Institute. Additionally, he maintains cyber security and ICS/OT certifications such as the CISSP, GRID, GICSP, GCIP, GPEN, GCIH, ISA 62443, and more.

As part of his community efforts, Michael founded and leads the UpstateSC ISSA Chapter and BSides Greenville conference. He also wrote and taught all six cyber security courses for Greenville Technical College's cyber security program which focused on helping educate the cyber security practitioners of tomorrow. In 2023, he was awarded CyberSC’s MG Lester D. Eisner Award for Cyber Excellence in Leadership for the State of South Carolina.

**Unit 0: ICS/OT Cyber Security Overview**

* Introductions
* Why We Are Here
* About the Course
* Goals of the Course
* Course Units
* ICS/OT Certifications
* Other Training and Certifications

**Unit 1: ICS/OT Cyber Security Overview**

* What is ICS/OT Cyber Security?
* We Are Here to Save the World!
* Types of ICS/OT Environments
* The Differences between IT and ICS/OT Cyber Security
* History of ICS/OT Cyber Security
* ICS/OT Specific Malware
* ISA 62443 – The Gold Standard for ICS/OT Cyber Security
* ICS/OT Cyber Security Industry Certifications
* Creating Your Home ICS/OT Lab (Without Having to Pay for Costly Equipment!)
* Introducing AtomICS Linux
* Review Questions

**Unit 2: Main Types of Control Systems & Protocols**

* Let’s Build a Power Plant!
* ISBL vs OSBL
* Control Systems
  + PLC (Programmable Logic Controller)
  + DCS (Distributed Control System)
  + HMI (Human Management Interface)
  + SIS (Safety Instrumented System)
  + EWS (Engineering Workstations)
  + Data Historians
  + Other
* Industrial Control Protocols
  + Modbus
  + S7comm
  + OPC
  + OPC UA
  + Other
* Industrial Control Wireless Protocols
  + 802.11 Wi-Fi
  + ZigBee
  + Wireless HART
  + Other
* Programming Control Systems
  + Ladder Logic
  + Program Mode vs Run Mode
* Review Questions

**Unit 3: Secure Network Architecture**

* A World Without Cyber Security
* Real World Attack Example: TRISIS
* The Purdue Model
* ISA 62443: Zones and Conduits
* IIoT (Industrial Internet of Things)
* Secure Remote Access
* Physical Security
* Review Questions

**Unit 4: Asset Registers and Control Systems Inventory**

* The Important Role of Asset Registers
* Creating an Asset Register
* Walking the Environment
* Mapping ICS/OT Networks
* Change Management
* Monitoring Control System State
* Securing the Asset Register
* Review Questions

**Unit 5: Threat & Vulnerability Management**

* What is Threat & Vulnerability Management?
* Introduction to Industrial Controls Risk
* IT Vulnerability Management Process
* OT Vulnerability Management Process
* Operational Risks of Vulnerability Scanning
* Passively & Actively Identifying Assets & Vulnerabilities
* Patching Systems in ICS/OT Environments
* Leveraging Threat Intelligence
* Review Questions

**Unit 6: OSINT for Industrial Controls**

* Finding Industrial Control Systems with Shodan
  + Industrial Control Protocols
  + ICS Tags
  + Image Searches
  + Honeypots
* Google Searches
* WHOIS & DNS
* Digital Certificates
* Social Media
* Other
* Review Questions

**Unit 7: Incident Detection**

* Incident Detection in ICS/OT Networks
* Threat Hunting
* SEIM, SIEM, SIM, SEM
* Deploying ICS/OT Honeypots for High Fidelity Alerts
* Review Questions

**Unit 8: Incident Response**

* The Incident Response Process
* Developing an Industrial Incident Response Program
* Incident Response Planning
* IR Tabletop Exercises
* Backdoors & Breaches
* Review Questions

**Unit 9: Risk Assessments, Governance & Compliance**

* ISA 62443 Deep Dive
* Conducting Risk Assessments
* Threat Modeling
* Cyber Security Policies, Standards and Guidelines
* FERC (Federal Energy Regulatory Commission)
* NERC (North American Energy Regulatory Commission)
* NERC CIP (Critical Infrastructure Protection)
* Other Cyber Security Frameworks
* Measuring Compliance
* Review Questions

**Unit 10: Penetration Testing in ICS/OT**

* Traditional IT Attacks
* Pivoting from IT to OT
* The ICS Cyber Kill Chain
* MITRE ATT&CK for ICS
* ICS/OT-Specific Attacks
* Differences in IT and OT Penetration Testing
* ICS Cyber Kill Chain
* Rules of Engagement
* Attacker Methodologies in Detail
* Pivoting Through the Purdue Model
* Exploitation of Control Systems
* Exploiting Industrial Control Protocols
* Living Off the Land in ICS/OT Environments
* Review Questions