CyManII OT Cybersecurity Bootcamp

Table of Contents

Course Structure/Content Outline

Module 1: Fundamentals of OT

- **Terminal Learning Objective (TLO)**: At the end of this module, the participant will be able to discuss foundational concepts for both Operational Technology (OT) and Information Technology (IT). The goal for this module is to level set OT and IT professionals working in the OT environment.

Topic 1.1. OT Environment Introduction

- **TLO**: Establish a clear framing of the OT world describing what is really happening on the production floor and how cyber is integrated into the processes.
- **Enabling Learning Objectives (ELO)**: At the end of this topic area, participants will be able to:
    - Summarize OT/IT convergence
    - Discuss the impacts to the organization from a cyber incident
    - Discuss potential cascading impacts from the loss of services and/or products
    - Summarize ICS processes, roles and responsibilities
    - Describe common OT assets
    - Describe common IT assets used in an OT environment
    - Describe the differences of OT and IT
    - Explain Industrial Control System (ICS) components and architecture
    - Summarize strategies for securing the OT environment
- Lesson 1.1.1: Introduction to Operational Technology
- Lesson 1.1.2: Overview of Industrial Control Systems
- Lesson 1.1.3: IT Devices in the OT environment
- Lesson 1.1.4: IT/OT Convergence
- Lesson 1.1.5: IoT and IT/OT Convergence
- Lesson 1.1.6: IT-OT Convergence and New Technologies Increase Risk
- Lesson 1.1.7: Impacts of a Cyber Incident
- Lesson 1.1.8: Strategies for Securing the OT Environment

Topic 1.2. ICS Processes, Roles, and Responsibilities

- **TLO**: Explain ICS processes, and distinguish roles and responsibilities needed for OT environments.
- **ELO**: At the end of this topic area, participants will be able to:
    - Identify components of ICS
    - Recognize the three main layers of industrial process control systems
    - Summarize the function of high-level ICS processes
    - Explain the roles and responsibilities of ICS processes
    - Recognize process control system integration challenges
    - Summarize ICS job roles and responsibilities.

        - Distinguish between job roles and job titles for the learners as every company will break these up differently.
- Lesson 1.2.1: Overview of ICS Processes
- Lesson 1.2.2: Introduction to ICS Roles and Responsibilities
- Lesson 1.2.3 Challenges Faced by Process Control System Integrators
- Lesson 1.2.4: ICS Job Roles and Responsibilities

Topic 1.3. ICS Components & Architecture

- **TLO**: Define, describe and provide examples of cyber physical systems, IT architectures used in the OT environment and their associated vulnerabilities
- **ELO**: At the end of this topic area, participants will be able to:
    - Describe common OT systems and controllers
    - Summarize how OT systems and controllers are used
    - Summarize ICS components, purposes, deployments, significant drivers and constraints
    - Describe vulnerabilities associated with OT systems and controllers
    - Describe common IT networking systems and devices and provide examples of how they are used
    - Summarize the different wireless communication technologies used in ICS
    - Describe IT structures, protocols and communications used in ICS
    - Describe vulnerabilities associated with IT architectures
    - Discuss how the OT network is situated within the context of the broader IT infrastructure and connected to it
    - Distinguish the difference between OT/ICS and IT
    - Discuss the importance of CIA in cybersecurity and the order of precedence in the ICS environment
    - Categorize assets that comprise Purdue Reference Architecture levels zero through three
    - Summarize the use of levels and zones in defining a secure ICS architecture as well as the devices deployed at each level and zone
- Lesson 1.3.1: IT Systems and Their Impact on OT Security
- Lesson 1.3.2: Cyber-Physical Systems, IT Architectures Used in the OT Environment, and Their Associated Vulnerabilities
- Lesson 1.3.3: Distinguish the Difference Between OT/ICS and IT
- Lesson 1.3.4: Zones, Devices, and Security in PERA Levels 0–3

Topic 1.4. Securing OT

- **TLO**: Discuss strategies, devices and processes for securing an operational technology environment
- **ELO**: At the end of this topic area, participants will be able to:
    - Summarize the OT threat environment
    - Describe vulnerabilities, attack methods and exploits in OT/ICS network design
    - Describe how cybersecurity frameworks can reduce cybersecurity risk

    - Recognize the basic principles of Risk Management
    - Describe how risk is measured and how it can be used to inform disaster recovery and incident response activities
    - Determine the threat landscape using high-level concepts of threat modeling
    - Describe physical security considerations for the OT environment
    - Describe the importance of endpoint security software
    - Summarize how communications can be compromised within ICS and describe protection techniques that can be used including cryptography.
    - Discuss wireless communication technologies and techniques to protect
    - them.
    - Summarize the benefits of information sharing and how information sharing and analysis organizations can reduce risk for critical infrastructure
    - Summarize the steps and best practices used in building a security program for an ICS
    - Differentiate plans needed for response, recovery, and continuity
    - Recognize OT cybersecurity resources

- Lesson 1.4.1: OT Threat and Vulnerability Landscape
- Lesson 1.4.2: Attack Methods and Exploits
- Lesson 1.4.3: Understand Cybersecurity Frameworks
- Lesson 1.4.4: Intelligence Gathering and Threat Modeling
- Lesson 1.4.5: Physical Security
- Lesson 1.4.6: Hardening and Protecting Endpoints
- Lesson 1.4.7: Securing Communications
- Lesson 1.4.8: Securing Wireless Technologies
- Lesson 1.4.9: Cybersecurity Information Sharing

Module 2: Risk Management

- **TLO:** At the end of this module, participants will be able to summarize risk management processes, components, and strategies to minimize internal and external risks that could negatively impact OT environments. The goal for this module is to assist participants in identifying potential problems before they occur and have a plan for addressing them.

Topic 2.1. Defining Cyber Risk and Mitigation

- **TLO:** Outline key risk concepts, factors, and mitigation strategies in OT environments.
- **ELO:** At the end of this topic area, participants will be able to:
    - Summarize the fundamental concepts of cyber risk, including its impact on organizations and critical infrastructure.
    - Define key risk concepts from NIST SP 800-30 R1, such as threat, vulnerability, impact, and likelihood
    - Differentiate between cyber risks in IT and OT environments.
    - Discuss the importance of cyber risk mitigation strategies

- Lesson 2.1.1: Cyber Risk and Impacts on Organization
- Lesson 2.1.2: Key Risk Concepts
- Lesson 2.1.3: Cyber Risk Mitigation Strategies

Topic 2.2: Mapping Vulnerabilities and Threats

- **TLO:** Apply effective management strategies to vulnerabilities and threats in OT systems.
- **ELO:** At the end of this topic area, participants will be able to:
    - Identify common vulnerabilities in devices, networks, remote access, supply chains within OT systems.
    - Recognize vulnerabilities related to people and processes in OT environments.
    - Correlate the MITRE ATT&CK knowledge base, including the ICS ATT&CK Matrix, to common ICS/OT cyber threats.
    - Analyze real-world examples of insider threats and attack campaigns and their impact on OT systems and security.
- Lesson 2.2.1: Vulnerabilities in Devices, Networks, Remote Access, and Supply Chains Within OT Systems
- Lesson 2.2.2: Vulnerabilities Related to People and Processes in OT Environments
- Lesson 2.2.3: Correlating Threat Vectors to Vulnerabilities in the ICS/OT Environment
- Lesson 2.2.4: Analyzing Real-World Examples of Insider Threats and Attack Campaigns and Their Impact on OT Systems and Security.

Topic 2.3: Planning a Cyber Risk Management Program

- **TLO:** Develop a high-level risk management and mitigation plan for an OT Environment
- **ELO:** At the end of this topic area, participants will be able to:
    - Compare risk-based approaches to cyber risk mitigation with CSF (Cybersecurity Framework)-based approaches.
    - Illustrate how risk-based approaches align with corporate risk mitigation strategies.
    - Summarize the core contents of NIST SP 800-37r2 (Risk Management Framework) as relevant to cyber risk management
- Lesson 2.3.1: Risk Based Approaches to Cyber Risk Mitigation
- Lesson 2.3.2: Risk Based Approaches and Risk Mitigation Strategies
- Lesson 2.3.3: Introduction to NIST SP 800-37r2
- Lesson 2.3.4: Implementing a Cyber Risk Management Program

Topic 2.4: Implementing Cyber Risk Mitigation

- **TLO:** Assess risk management strategies in practical deployment and configuration scenarios.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Evaluate different security strategies and architectures, including Defense in Depth (DiD) and Zero Trust (ZT)
    - Explain the benefits and challenges of combining DiD and ZT approaches.

    - Describe Hybrid models
    - Outline the tasks involved in detailed design and integration during deployment.
    - Apply NIST 800-82 R3 and NIST CSWP-28 guidelines to a practical deployment and configuration scenario.
- Lesson 2.4.1: Security Strategies and Architectures
- Lesson 2.4.2: Deployment Design and Integration
- Lesson 2.4.3: NIST Guidelines for Deployment

Module 3: Supply Chain Security

- **TLO:** At the end of this module, participants will be able to summarize strategies to identify, evaluate and mitigate risks associated with external vendors, suppliers, transportation, and logistics.

Topic 3.1. Supply Chain Security Overview

- **TLO:** Summarize the key stages and strategies for efficient and effective production flow
- **ELO:** At the end of this topic area, the participant will be able to:
    - Describe the major components of the supply chain lifecycle
    - Explain the use of third-party vendors
    - Differentiate Bill of Materials (BoMs) vs Software Bill of Materials (SBoMs)
    - Summarize third-party risks
    - Explain components of third-party risk analysis
    - Recognize strategies for OT supply chain management
- Lesson 3.1.1: Supply Chain Lifecycle
- Lesson 3.1.2: Strategies for OT Supply Chain Risk Management

Topic 3.2. Real World Examples

- **TLO:** Summarize the possible negative impacts that can be realized through cybersecurity risk in the supply chain.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Give examples of supply chain cybersecurity attacks
    - Summarize various cybersecurity supply chain issues
- Lesson 3.2.1: Supply Chain Attacks
- Lesson 3.2.2: Other OT Cybersecurity Issues in the Supply Chain

Topic 3.3. Supply Chain Risks

- **TLO:** At the end of this section, the participant will be able to explain strategies to evaluate and manage the risks associated with third-party vendors and service providers.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Explain supply chain risk analysis
    - Describe the process for threat and vulnerability identification and risk prioritization
    - Describe the difference of known vulnerabilities and unknown vulnerabilities
    - Summarize the purpose of Supply Chain Risk Assessments
- Lesson 3.3.1: Supply Chain Cybersecurity Risks in OT Environments

- Lesson 3.3.2: OT Supply Chain Risk Analysis Steps
- Lesson 3.3.3: Vulnerability Identification and Risk Prioritization in OT Environments
- Lesson 3.3.4: Supply Chain Risk Assessment Using NIST 800-161 Framework

Topic 3.4. BOMS, SBOMS, and HOMS

- **TLO:** At the end of this section, the participant will be able to describe strategies to safeguard their operations and enhance trust with their vendors and partners.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Summarize key components of a secure supply chain strategy
    - Describe how information sharing can reduce cybersecurity risks
    - Explain how SBOMs can help mitigate risk
- Lesson 3.4.1: BOM, SBOM, and HBOM
- Lesson 3.4.2: Using SBOMs to Mitigate Third Party Risks in an OT Environment

Module 4: New & Emerging Operational Technology (Smart Automation/Manufacturing Capabilities)

- **TLO:** At the end of this module, the participant will be able to understand and apply emerging technologies, including Artificial Intelligence (AI), Blockchain, and Robotics, in OT environments, addressing the implementation challenges, ethical considerations, and real-world applications to enhance system efficiency, security, and adaptability.

Topic 4.1: Artificial Intelligence in OT

- **TLO**: Upon completion of this module, learners will be able to evaluate and implement AI applications, techniques, and solutions in OT environments, addressing key challenges such as data quality, security risks, and ethical considerations, to optimize, improve, and enhance system security.
- **ELO**: At the end of this topic area, the participant will be able to:
    - Summarize the various applications of AI in OT environments, including predictive maintenance, process optimization, automated management processes, anomaly detection, and quality control, to enhance operational efficiency, security, and product quality.
    - Explore and differentiate among key AI techniques and algorithms, including machine learning and natural language processing, to understand their applications and impact within OT systems.
    - Implement AI solutions in OT environments by mastering data acquisition, model development, and the integration of AI models with OT systems.
    - Address the key challenges and considerations in AI adoption within OT environments, including data quality, security risks, and ethical governance, to ensure responsible and secure AI implementation.
- Lesson 4.1.1: Artificial Intelligence in OT
- Lesson 4.1.2: AI Techniques and Algorithms
- Lesson 4.1.3: Implementing AI Solutions in OT Environments

- Lesson 4.1.4: Addressing Challenges and Considerations in AI Adoption

Topic 4.2: Blockchain in OT

- **TLO:** Demonstrate a comprehensive understanding of blockchain technology and its applications in Operational Technology (OT) environments by summarizing key concepts, exploring practical applications, implementing blockchain solutions, and addressing the challenges and considerations associated with blockchain adoption in OT systems.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Summarize the fundamental concepts of blockchain technology
    - Understand blockchain applications in OT environments
    - Implement at a high level, blockchain in OT systems
    - Summarize the challenges and considerations in blockchain adoption
- Lesson 4.2.1: Summarize the Fundamental Concepts of Blockchain Technology
- Lesson 4.2.2: Explore Blockchain Applications in OT Environments
- Lesson 4.2.3: Address Challenges and Considerations in Blockchain Adoption

Topic 4.3: Robotics in OT

- **TLO:** Evaluate and implement AI-powered robotics in OT environments by understanding their applications, exploring key AI techniques, and addressing integration, safety, and ethical challenges to enhance operational efficiency.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Summarize the role and benefits of AI-powered robotics in OT environments, including their applications in manufacturing, logistics, and utilities, to enhance operational flexibility and efficiency.
    - Explore AI techniques for robotic control and perception, including machine learning, computer vision, natural language processing, and sensor fusion, to enhance robotic capabilities in OT environments.
    - Implement AI robotic solutions in OT environments, focusing on system integration, safety, edge computing, and continuous learning to optimize operations and human-robot collaboration.
    - Address challenges in AI robotics adoption, including security, ethics, change management, and scalability, to ensure successful deployment in OT environments.
- Lesson 4.3.1: Summarize the Role of AI in Industrial Robotics for OT Environments
- Lesson 4.3.2: Explore AI Techniques and Algorithms for Robotic Control and Perception
- Lesson 4.3.3: Implement AI Robotic Solutions in OT Environments
- Lesson 4.3.4: Address Challenges and Considerations in AI Robotics Adoption

Module 5: Design and Upgrades of Smart Manufacturing Systems and Processes

- **TLO:** At the end of this module, the participant will be able to understand and apply strategies to modernize legacy Operational Technology (OT) systems by integrating Industrial Internet of Things (IIoT) technologies, while addressing the challenges of compatibility, security, and operational continuity.

Topic 5.1: Modernizing Legacy Systems in OT Environments

- **TLO:** Describe the architecture and components of legacy OT systems and IIoT. Describe typical use cases for IIoT and trends in smart manufacturing. Describe the opportunities and challenges in modernizing legacy OT systems with IIoT. Understand the typical best practices in operating a manufacturing environment.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Understand the architecture and key components of legacy OT systems, including supervisory control and data acquisition (SCADA), distributed control systems (DCS), human-machine interface (HMI), remote terminal units (RTU), and the communication protocols (e.g., Modbus, Profibus, RS-232) which connect them.
    - Familiarize with the Industry IoT Consortium's Industrial Internet Reference Architecture (IIRA) publication.
    - Describe the three-tier IIoT system architecture (Edge, Platform, and Enterprise tiers), five functional domains, the different networks, components, and protocols used, including edge computing, wireless sensor networks, and commercial IIoT platforms.
    - Identify and evaluate strategies for modernizing legacy OT systems by incorporating IIoT technologies, such as edge and cloud computing, and integrating modern monitoring, analytics, and security tools.
    - Discuss key trends and considerations in smart OT systems, focusing on the convergence of IT and OT networks, secure-by-design principles, and the impact of regulatory and policy developments.
    - Identify the challenges of integrating legacy and modern OT systems, including resource limitations, compatibility issues, and the complexity of integration projects, and discuss strategies to address these challenges.
    - Review best practices for maintaining OT environments, including implementing redundancy, network segmentation, preventive maintenance, and secure remote access to ensure system reliability and security.
- Lesson 5.1.1: Identify the Architecture and Components of Legacy OT Systems
- Lesson 5.1.2: Identify the Architecture and Components of IIoT Systems
- Lesson 5.1.3: Describe Opportunities to Modernize Legacy Systems with IIoT
- Lesson 5.1.4: Discuss Important Trends and Considerations in Smart OT Systems
- Lesson 5.1.5: Discuss Challenges in Integrating Legacy and Modern Systems in OT Environments

Topic 5.2: Secure by Design

- **TLO:** Describe the principles secure by design and apply it to the various components of a system, its architecture, and its operation.
- **ELO**: At the end of this topic area, the participant will be able to:
    - Understand how to conduct a risk assessment
    - Understand principles of secure by design from a network perspective
    - Understand foundations of secure communication
    - Understand access control models techniques
    - Understand principles of secure by design from a software development practice
    - Understand importance of implementing continuous monitoring and incidence response capabilities as part of secure by design.
    - Understand principles of secure by design from a user aspect.
    - Understand principles of secure by design from a supply chain perspective
    - Understand standards that need to be followed for designing security into systems and operations.
    - Understand importance of continuous improvement in security operation and practice via regular reviews and feedback.

- Lesson 5.2.1: Vulnerable by Design
- Lesson 5.2.2: Secure by Design
- Lesson 5.2.3: Secure by Default
- Lesson 5.2.4: Software Product Security Principles
- Lesson 5.2.5: Secure by Design Tactics
- Lesson 5.2.6: Secure by Default Tactics
- Lesson 5.2.7: Customer Recommendations
- Lesson 5.2.8: Secure by Design vs. Cyber-Informed Engineering

Topic 5.3: Cyber-Informed Engineering

- **TLO:** Outline considerations and locate resources for application of cyber-informed engineering (CIE) principles and methods into the conception, design, development, upgrade, and operation of smart manufacturing systems, to mitigate or even eliminate avenues for cyber-enabled attacks.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Summarize the fundamental concepts of cyber-informed engineering (CIE)
    - Differentiate between CIE and Secure-by-Design strategies
    - Define the worst potential consequences from cyberattacks to their system
    - Develop examples of the application of CIE principles to mitigate or eliminate the possibility of those consequences to their system
- Lesson 5.3.1 What is Engineering?
- Lesson 5.3.2 What is Cyber-Informed Engineering?
- Lesson 5.3.3 Is CIE Just for Computer Engineers?
- Lesson 5.3.4 Is CIE Another Required Course?

- Lesson 5.3.5 How Do We Apply CIE?
- Lesson 5.3.6 How Do I Find Out More?

Module 6: Defending OT Systems

- **TLO:** At the end of this module, the participant will be able to identify security vulnerabilities in OT networks, software programs, and hardware systems. The participant will also be able to develop a risk assessment plan to help mitigate risks. The goal for this module is to equip the participant with the skills needed to protect OT networks from traditional and non-traditional attack vectors by evaluating the entire ICS security stack (IT/OT communication protocols, software, hardware, and physical access controls).

Topic 6.1. Defending OT Systems Primer

- **TLO:** Describe legacy and modern software and network technologies and risk assessment measures and then develop a defense-in-depth plan based on these tools and techniques.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Review the use of legacy software and network technologies in ICS/OT environments
    - Summarize the use of modern software and network technologies in ICS/OT environments
    - Identify measures to harden ICS/OT systems based on risk assessments
    - Demonstrate tools and techniques designed to help defend against ICS attacks
    - Develop a defense-in-depth plan
- Lesson 6.1.1: Review the Use of Legacy Software and Network Technologies in ICS/OT Environments
- Lesson 6.1.2: Summarize the Use of Modern Software and Network Technologies in ICS/OT Environments
- Lesson 6.1.3: Identify Measures to Harden ICS/OT Systems Based on Risk Assessments
- Lesson 6.1.4: Demonstrate Tools and Techniques Designed to Help Defend Against ICS Attacks

Topic 6.2: Physical Security Systems

- **TLO:** Assess and defend physical control systems in OT environments in accordance with North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC) standards.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Describe standard control schemes and designs in physical security systems.
    - Apply NERC and FERC standards to assess a physical security system.
    - Identify techniques to physically secure removable and peripheral devices.
    - Implement access control mechanisms in a physical security system.
    - Evaluate devices used for surveillance and monitoring physical systems.

    - Design protective measures that can mitigate environmental threats to physical security systems.
    - Outline the various levels of security in site plans (Red, Yellow, Green, Grey)
    - Develop a physical security site plan based on a given scenario.
- Lesson 6.2.1: Outline Standard Control Schemes and Designs in Physical Security Systems
- Lesson 6.2.2: Apply NERC and FERC Standards to Assess a Physical Security System
- Lesson 6.2.3: Identify Techniques to Physically Secure Removable and Peripheral Devices
- Lesson 6.2.4: Implement Access Control Mechanisms in a Physical Security System
- Lesson 6.2.5: Evaluate Devices Used for Surveillance and Monitoring Physical Systems
- Lesson 6.2.6: Design Proactive Measures That Can Mitigate Environment Threats to Physical Security Systems
- Lesson 6.2.7: Develop a Physical Security Site Plan Based on a Given Scenario

Topic 6.3: Network Security

- **TLO:** Implement secure networking best practices to reduce the risk of malicious action on the OT/ICS network.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Apply network security layering to mitigate vulnerabilities.
    - Configure network interfaces, ports, communication channels, and software packages securely and reliably.
    - Deploy instruction detection/prevention systems and firewalls for IT and OT networks
    - Utilize network monitoring tools, including wireless communication devices.
    - Detect and mitigate known attacks using IDS/IPS, firewalls, and other tools
    - Detect and mitigate unknown attacks using ML/DL-based anomaly detection techniques
- Lesson 6.3.1: Review of Network Stack Based on TCP/IP and OSI Models and Major IT/OT Network Protocols
- Lesson 6.3.2: Network attacks and Commonly Exploited Protocol Features
- Lesson 6.3.3: Identifying Network Vulnerabilities Using Network Mapping, Active and Passive Scanning, OT-Focused Penetration Testing, and Configuration Reviews
- Lesson 6.3.4: Network Design and Configuration for Performance, Security, and Management: Network Segmentation, IDS/IPS Deployment, Firewall Configuration, and Review of Network Logs
- Lesson 6.3.5: Monitoring and Analyzing Network Traffic Using Wireshark and Other Tools
- Lesson 6.3.6: Detection and Mitigation of Known Attacks on IT and OT Networks
- Lesson 6.3.7: Using Machine Learning (ML)/Deep Learning (DL) Models to Detect Unknown or Zero-Day Attacks and Developing Mitigation Strategies

Topic 6.4: Hardware security

- **TLO:** Identify vulnerabilities and security risks associated with hardware systems commonly used in ICS/OT. Develop an understanding of printed circuit boards, digital electronics, how to interpret data sheets, and how to assess vulnerabilities in PLC (Programmable Logic Controller) architectures.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Explore printed circuit board designs and common programmable logic controller architectures.
    - Learn to identify and understand basic functions associated with digital electronics components, including capacitors, transistors, bus routes, sensors, and logic gates.
    - Use the information contained in data sheets to develop an understanding of a particular hardware system and to help identify potential security vulnerabilities.
    - Learn to identify and access debug ports found on printed circuit boards and programmable logic controllers.
    - Understand how hardware vulnerabilities can be introduced during the supply chain lifecycle.
    - Understand how ICS hardware devices fit into the Purdue Model Framework for Industrial Control Systems.
    - Using a data sheet, known CVEs, and a virtual simulation of a programmable logic controller (PLC), identify any hardware vulnerabilities in the associated PLC.
- Lesson 6.4.1: Exposure to PCB and PLCs
- Lesson 6.4.2: Introduction to Digital Electronics
- Lesson 6.4.3: Learn to Analyze and/or Interpret Data sheets
- Lesson 6.4.4: Debug Ports
- Lesson 6.4.5: Supply Chain
- Lesson 6.4.6: Purdue Model Security Measures

Topic 6.5: Software security

- **TLO:** Illustrate how to prevent, detect, respond, and mitigate software security vulnerabilities in the kernel, firmware, malware, and Web interface with common tools and techniques.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Outline methods to recognize malware designed to target and affect ICS.
    - Describe static and dynamic analysis techniques.
    - Explore common dynamic analysis toolsets for ICS/OT.
    - Explain firmware and security issues associated with firmware-based attacks.
    - Examine the issue of unprivileged remote access and remote access trojans (RATs).
    - Summarize common security risks associated with web interfaces with the OWASP TOP 10.
    - Demonstrate how common software testing tools are used in software security defense.

    - Identify malware in an ICS environment and security risks in a web application.
- Lesson 6.5.1: Outline Methods to Recognize Malware Designed to Target and Affect ICS
- Lesson 6.5.2: Describe Static and Dynamic Analysis Techniques
- Lesson 6.5.3: Explore Common Dynamic Analysis Toolsets for ICS/OT
- Lesson 6.5.4: Outline Security Issues Associated with Firmware-Based Attacks
- Lesson 6.5.5: Describe PLC Ladder Logic Programming and Its Vulnerabilities
- Lesson 6.5.6: Examine the Issue of Unprivileged Remote Access and RATs
- Lesson 6.5.7: Summarize Common Security Risks Associated with Web Interfaces with the OWASP TOP 10

Module 7: Forensics & Recovery

- **TLO:** At the end of this module, the participant will be able to conduct basic online and offline forensic examinations of OT and IT systems and restore systems, when applicable, to an operational state. The goal for this module is to equip the participant with the skills needed to obtain forensic artifacts from compromised OT devices, without altering data, and preserving the chain of custody for criminal prosecution and civil litigation.

Topic 7.1: Intrusion Detection

- **TLO:** Detect and evaluate events, incidents, and indicators of compromise in ICS/OT systems, and develop detection rules used to generate alerts.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Learn to implement intrusion detection systems (heuristic, behavioral, signature, and anomaly-based systems) for ICS, capture and evaluate .pcap files, and write detection rules in Suricata and Elastic Security.
    - Learn how to collect, store, and interpret logs from various IT and OT sources to help identify potential incidents.
    - Develop the skills necessary to identify suspicious processes (e.g. malware), active connections, and user-generated activities in IT and OT systems to help identify potential incidents.
    - Participate in a structured lab environment that reinforces the techniques learned in this module
    - The participant will demonstrate proper detection, identification, and classification of events in a simulated environment by implementing appropriate detection rules with an intrusion detection system.
- Lesson 7.1.1: Intrusion Detection
- Lesson 7.1.2: Intrusion Detection Laboratory Using Splunk's Boss of the SOC
- Lesson 7.1.3: Identifying Suspicious Processes and User Activity

Topic 7.2: Responding to Breaches

- **TLO:** Develop and implement comprehensive incident response plans tailored to ICS environments, conduct thorough incident investigations to identify the root cause, scope,

and impact of security incidents, and implement effective containment measures to mitigate the impact of security incidents and prevent further damage.

- **ELO:** At the end of this topic area, the participant will be able to:
  - Explore common types of incidents in ICS environments.
  - Understand the unique characteristics and challenges of incident response in manufacturing and ICS environments.
  - Develop a comprehensive incident response plan, including roles, responsibilities, and procedures.
  - Conduct tabletop exercises and simulations to test the incident response plan.
  - Gather and analyze evidence from various sources, including logs (i.e. SIEMs), network traffic, and system artifacts.
  - Practice analyzing logs and system artifacts in a simulated incident.
  - Use tools to identify the root cause of the incident and determine its scope and impact.
  - Implement containment strategies to isolate the affected systems and prevent further spread of the incident.
- Lesson 7.2.1: Incident Response Introduction
- Lesson 7.2.2: Creating a Comprehensive Incident Response Plan
- Lesson 7.2.3: Root Cause Identification Plan
- Lesson 7.2.4: Containment Strategies in ICS Environments
- Lesson 7.2.5: SIEMs and Log Analysis

Topic 7.3: Threat Hunting

- **TLO:** Understand threat hunting concepts, develop threat hunting strategies, utilize threat hunting tactics, techniques, and procedures (TTP), and respond to threat intelligence.
- **ELO:** At the end of this topic area, the participant will be able to:
  - Define threat hunting and its importance in ICS environments.
  - Identify common IOCs associated with advanced threats targeting ICS systems.
  - Develop threat hunting strategies based on ICS environments.
  - Identify potential threat actors and their TTPs.
  - Prioritize threat hunting activities based on risk and potential impact.
  - Use a variety of threat hunting tools, including SIEM systems, network traffic analysis tools, and endpoint detection and response solutions.
  - Analyze threat intelligence to identify potential threats and vulnerabilities.
  - Incorporate threat intelligence into threat hunting strategies and activities.
- Lesson 7.3.1: Threat Hunting Introduction
- Lesson 7.3.2: Identifying IOCs in ICS
- Lesson 7.3.3: Developing Threat Hunting Activities
- Lesson 7.3.4: STIX and TAXII

Topic 7.4: Forensics

- **TLO:** Conduct basic digital forensics examinations of IT and OT devices, and learn how to prevent data from being altered, the proper methods for securing forensic data, and how to document your findings if you are called to testify in court.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Learn how to document individuals who have handled and/or processed data seized during a forensics examination and how to properly secure said data as evidence.
    - Understand the importance of testing your forensic tools and ensuring they work correctly and produce the expected results.
    - Understand the importance of ensuring data integrity (e.g. the forensic data is a bit-for-bit copy of the original dataset), in case it needs to be introduced into a court of law.
    - Understand how to use hexadecimal notation to locate forensic data and identify memory addresses. Understand the basic structure of how computers store data, boot into operating systems, and interact with hardware devices and users (I/O).
    - Learn to identify the types of devices in an OT system that can yield forensics artifacts, like programmable logic controllers, human machine interfaces, and data historians.
    - Learn the difference between conducting a live forensics examination (typically to retrieve volatile information) and an offline examination (typically involving a bit-for-bit copy of the target that will not include volatile information or active processes and network connections). The participant will also learn to differentiate between intranet and internet connections.
    - Understand how limited memory and debug/IO ports in OT devices can limit, and sometimes prevent, the collection of forensic artifacts by traditional means.
    - Learn to use common tools forensic examiners use to collect evidence during an examination, especially regarding OT systems.
    - Understand how logs play an important role in forensics examinations and how to determine if the logs have been altered or wiped.
    - Gain experience conducting a real-world forensics examination of a compromised programmable logic controller using live and offline forensics techniques.
- Lesson 7.4.1: Evidence Collection and Chain-of-Custody
- Lesson 7.4.2: Tool Validation
- Lesson 7.4.3: Data Integrity
- Lesson 7.4.4: Computer Architecture and Filesystems
- Lesson 7.4.5: Offline and Live Forensic examinations
- Lesson 7.4.6: OT Devices That Can Yield Forensics Artifacts
- Lesson 7.4.7: Forensic Limitations in ICS
- Lesson 7.4.8: ICS Forensic Investigation Tools

Topic 7.5: Recovery

- **TLO:** Assess the damage done to an OT/ICS environment and follow best practices to return it to working order.
- **ELO:** At the end of this topic area, the participant will be able to:
    - Determine the location and extent of damage caused by an incident.
    - Remove malicious or damaged artifacts and activity from the OT/ICS environment.
    - Restore backups of data and device configurations to return OT/ICS systems to a known state of operation.
    - Determine if it is possible to verify an OT/ICS system offline.
    - Perform offline verification of individual systems to ensure their safety and integrity without reintroducing threats to the OT/ICS environment
- Lesson 7.5.1: Recovery Damage Assessment
- Lesson 7.5.2: Purging Malicious Activity
- Lesson 7.5.3: Wiping and Restoring Systems