

Industrial Cybersecurity Essentials

Scope and Sequence

Version 1.0

Contents

Target Audience	3
Prerequisites	3
Course Description	3
Equipment Requirements	4
Course Outline	4
Next Courses Recommended	6
How you can use this course	6

Target Audience

The Cisco Networking Academy "Industrial Cybersecurity Essentials" course is designed for students in secondary and post-secondary educational institutions, as well as any learner interested in understanding the fundamental principles and practices of cybersecurity within modern industrial network infrastructures.

Prerequisites

Learners should have completed the Industrial Networking Essentials course and either the Industrial IoT and Control Systems in Energy or Industrial IoT and Control Systems in Manufacturing courses or possess equivalent knowledge.

Course Description

Industrial Cybersecurity Essentials offers a comprehensive introduction to the critical aspects of securing industrial infrastructures against cyber threats. The course emphasizes the unique challenges and requirements of cybersecurity in Operational Technology (OT) environments, particularly in the context of IIoT and IACS. It explores the integration of Information Technology (IT) and OT security principles.

A key feature of this course is the practical application of industrial cybersecurity skills through various labs using a pre-built Kali Linux Virtual Machine (VM) and Cisco Packet Tracer. Learners will have the opportunity to analyze cyberattacks, assess vulnerabilities, configuring an industrial firewall, implement access control and secure remote access, implement device hardening and monitor industrial network scenarios in virtual environments.

The course design includes:

- 9 modules focusing on essential cybersecurity concepts tailored to industrial contexts.
- Emphasis on applied skills with approximately 10 labs and 7 Cisco Packet Tracer activities to simulate real-world industrial cybersecurity scenarios.
- Videos and quizzes to enhance learning experiences and knowledge retention.
- A final exam that, upon successful completion, awards a Digital Badge.

The estimated time commitment for the course is 25 hours, offering flexibility to accommodate different learning paces and schedules.

Course Objectives

The course aims to develop a foundational understanding of cybersecurity within the context of industrial settings. Key objectives include:

- Explain the importance of cybersecurity in Industrial and Operational Technologies.
- Explain how cyber-attacks occur.
- Explain why it is important to comply with security standards and compliance frameworks such as IEC 62443 and NIST SP 800-82r3.
- Explain the impacts of exploitation of common ICS vulnerabilities and strategies for mitigation.

- Evaluate security in an ICS system using risk assessment tools.
- Use tools to secure an industrial network.
- Implement local and remote access control to secure industrial networks.
- Explain techniques for hardening the industrial network infrastructure.
- Explain emerging trends in industrial cybersecurity.

Equipment Requirements

Hands-on labs require computers capable of running Cisco Packet Tracer and virtualization software (VirtualBox or UTM) with at least 4GB of RAM and 20GB of free disk space. Other learning experiences require focused internet-based research.

Software:

- Cisco Packet Tracer 9.0.0 or higher
- Oracle VirtualBox or UTM
- Ethical Hacker Kali Linux OVA file

Course Outline

The "Industrial Cybersecurity Essentials" course is structured into 9 modules that cover specific competencies.

The table below details the modules and their associated competencies. Each module is an integrated unit of learning that consists of content, activities, and assessments that target a specific set of competencies. The size of the module depends on the depth of knowledge and skill needed to master competency.

Module Title and Objective

Module Title/Topic Title	Objective
Module 1: Introduction to Industrial Cybersecurity	Explain the importance of cybersecurity in the Industrial IoT
1.1: Cyberattack of the IACS	Explain the need for a synthesis of the Information Technologies and Operational Technologies functions in the Industrial Internet of Things.
1.2: Cybersecurity Basics	Explain the features of IIoT implementations.
1.3: IIoT Security Requirements	Explain security requirements for IIoT networks.
1.4: The McCumber Cube Security Model	Explain the meaning of the McCumber Cube security model.
1.5: IT, OT, and IoT Security Requirements	Explain approaches to OT security.
Module 2: Attack Concepts and Techniques	Explain how cyber-attacks occur.
2.1: Industrial Cyber Attacks	Explain how industrial control systems are vulnerable to cyber-attacks.
2.2: Threat Actors	Describe who threat actors are and what they want.
2.3: Methods of Attack	Describe the different methods of infiltration and disruption.
2.4: Analyzing Attacks	Explain how the MITRE ATT&CK framework is used to analyze cyberattacks.

Module Title/Topic Title	Objective
2.5: Cyberwarfare	Explain what cyberwarfare is and why nations and governments need cybersecurity professionals to help protect their citizens and infrastructure.
Module 3: Industrial Cybersecurity Frameworks and Regulations	Explain why it is important to comply with security standards and compliance frameworks such as IEC 62443 and NIST SP 800-82r3.
3.1: Standards and Frameworks	Explain the origins and importance of security standards and compliance frameworks for IACS.
3.2: The IEC 62443 Family of Standards	Explain the major features of the IEC 62443 family of specifications.
3.3: NIST SP 800-82 and the Cybersecurity Framework	Explain the major features of the NIST SP 800-82 specifications.
3.4: Other Standards	Explain the major features of special purpose standards such as IEC 61850-90 and NERC CIP and ISO27001.
3.5: Legal and Ethical Issues	Explain the legal considerations and compliance issues related to cybersecurity in an industrial context.
Module 4: Vulnerabilities	Explain the impacts of exploitation of common ICS vulnerabilities and strategies for mitigation.
4.1: Common ICS Vulnerabilities	Explain common ICS vulnerabilities, threats, and their mitigation.
4.2: Vulnerability Testing Types and Tools	Explain how tools and services are used to assess vulnerabilities in ICS systems.
Module 5: Risk Assessment	Evaluate security in an ICS system using risk assessment tools.
5.1: Risk Assessment Concepts and Approaches	Explain approaches to security risk assessment.
5.2: Using a Risk Assessment Tool	Use the CVSS to assess risk in a target system.
5.3: Assessing Risk with Threat Modeling	Evaluate risks in an IoT system using assessment tools.
Module 6: Securing Industrial Networks	Use tools to secure an industrial network.
6.1: Designing Secure Industrial Networks	Explain considerations in designing secure industrial networks.
6.2: Secure Network Segmentation	Configure a firewall for network segmentation to enhance network security.
6.3: Risk Assessment	Use tools to monitor a secure industrial network.
Module 7: Authentication and Authorization Controls	Implement local and remote access control to secure industrial networks.
7.1: Access Control Concepts	Explain access control in industrial networks.
7.2: Access Control Models	Implement access control models in an industrial network.
7.3: Secure Remote Access	Implement secure remote access in an industrial network.
Module 8: Hardening the Industrial Network Infrastructure	Explain techniques for hardening the industrial network infrastructure.
8.1: Harden Industrial Networks and Protocols	Explain best practices for hardening the industrial networks and protocols.
8.2: Industrial Network Infrastructure Security	Explain how to harden the industrial network infrastructure.
Module 9: Frontiers in Industrial Cybersecurity	Explain emerging trends in industrial cybersecurity.
9.1: The Emerging Threat Landscape	Explain how the industrial cybersecurity threat landscape is evolving.
9.2: Zero Trust Architecture in Industrial Environments	Explain how Zero Trust Architecture strengthens industrial cybersecurity by replacing traditional perimeter-based defenses with identity-driven, context-aware access controls.
9.3: The Network as a Sensor	Explain how network telemetry and behavioral analytics convert the industrial network itself into a sensor that reveals anomalies and operational technology (OT)-specific threats.

Next Courses Recommended

After completing the "Industrial Cybersecurity Essentials" course, learners interested in further developing their cybersecurity skills, particularly in offensive security, may consider enrolling in the Cisco Networking Academy Ethical Hacker course. While not specifically focused on industrial scenarios, this course provides a solid foundation in offensive security techniques and methodologies, which can be highly valuable for understanding and defending against cyber threats in any environment.

How you can use this course

This course can be taken as a standalone learning experience and additionally, it is designed to integrate seamlessly with other Cisco Networking Academy courses to build comprehensive learning pathways. When combined with the "Industrial Networking Essentials" course and either the "Industrial IoT and Control Systems in Energy" or "Industrial IoT and Control Systems in Manufacturing" courses, it forms two distinct career-focused learning pathways.

Each of these paths offers a total estimated duration of approximately 75 hours, providing a deep dive into industrial networking, IoT, control systems, and cybersecurity tailored to specific industry verticals:

- Manufacturing: Combines "Industrial Networking Essentials," "Industrial IoT and Control Systems in Manufacturing," and "Industrial Cybersecurity Essentials."
- Power Energy: Combines "Industrial Networking Essentials," "Industrial IoT and Control Systems in Energy," and "Industrial Cybersecurity Essentials."

These structured pathways are ideal for entry-level profiles aiming to contribute to connecting and securing modern industrial infrastructures within these critical sectors.

