Faysal Aziz

OT Security

For ICS/SCADA - one day

FA-0539 · one day

Cybersecurity

Introduction

Welcome to our one-day training on Operational Technology (OT) Security for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

The materials for this course were gathered to address an increasingly vital aspect of industrial operations—ensuring the security and integrity of critical infrastructures that sustain our daily lives and the economy. In a world where cyber threats are evolving rapidly, understanding how to protect the technological backbones of industrial environments is not just beneficial; it's essential.

This training is designed to equip you with the knowledge and skills needed to navigate, analyze, and fortify the cybersecurity defenses of ICS and SCADA systems.

Learning outcomes

By the end of this training, you will:

- Have a deep understanding of the architecture and functionality of ICS/SCADA systems.
- Be able to identify key vulnerabilities and potential threat vectors in these systems.
- Learn the best practices and strategic approaches to mitigate risks and enhance system security.
- Develop capabilities in incident response management tailored for the unique challenges of OT environments.

Prerequisites

Participants are expected to have:

- A basic understanding of networking and system security concepts.
- Some familiarity with operational technology or industrial control environments.

- An interest in advancing cybersecurity measures within industrial settings.

Training outline

1. Overview of ICS/SCADA Systems

1. Introduction to the components and architecture of ICS/SCADA.
2. Role of these systems in critical infrastructure and industrial automation.

2. Understanding OT Security

1. Distinctions between IT and OT security.
2. Specific security challenges in OT environments.

3. Common Vulnerabilities in ICS/SCADA Systems

1. Analysis of common security weaknesses and historical attack vectors.
2. Review of notable cybersecurity incidents affecting ICS/SCADA systems.

4. Security Best Practices and Frameworks

1. Introduction to industry standards and best practices for securing ICS/SCADA systems.
2. Detailed discussion on implementing ISA/IEC 62443 and NIST SP 800-82.

5. Risk Assessment and Management in ICS/SCADA

1. Methodologies for risk assessment specific to operational technology.
2. Tools and practices for ongoing risk management.

6. Security Monitoring and Incident Handling

1. Setup and operation of monitoring tools designed for ICS environments.
2. Strategies for developing and implementing an effective incident response plan.

7. Future Trends and Advanced Topics

1. Exploration of emerging technologies impacting ICS security.
2. Discussion on the future of cybersecurity in operational technology.

© 2026 Faysal Aziz · Kuala Lumpur