BLACKBIRD FOR TRAINING

Cybersecurity for Industrial Control Systems (ICS)

12 – 16 September 2027
Online



Cybersecurity for Industrial Control Systems (ICS)

Ref: 3255275_336989 **Date:** 12 – 16 September 2027 **Location:** Online **Fees:** 2700 GBP

Introduction

As industrial operations become increasingly automated and interconnected, Industrial Control Systems ICS have emerged as the backbone of modern infrastructure across energy, manufacturing, and utilities sectors. However, this digital transformation has also introduced new cybersecurity challenges. The convergence of operational technology OT and information technology IT has created vulnerabilities that cyber attackers can exploit to disrupt critical processes and cause costly downtime.

The Cybersecurity for Industrial Control Systems ICS course provides participants with the knowledge and skills needed to protect industrial environments against sophisticated cyber threats. It focuses on identifying vulnerabilities, implementing multi-layered defense strategies, and building resilient architectures that ensure operational continuity and safety.

This course equips professionals with a deep understanding of cybersecurity principles tailored specifically to industrial systems — bridging the gap between IT security and OT reliability.

Course Objectives

By the end of this course, participants will be able to:

- Understand the architecture and components of industrial control systems.
- Identify and assess cybersecurity threats specific to ICS environments.
- Apply defense-in-depth strategies to protect critical infrastructure.
- Investigate and respond to cyber incidents in industrial environments.
- Implement monitoring and intrusion detection systems for ICS.
- Align with international standards such as IEC 62443 and NIST 800-82.
- Develop business continuity and disaster recovery plans for control systems.

Course Outlines

Day 1: Introduction to Cybersecurity in Industrial Systems

- Overview of cybersecurity concepts within operational environments.
- Differences between Information Technology IT and Operational Technology OT.
- Components of Industrial Control Systems: SCADA, DCS, and PLC.
- Common vulnerabilities in industrial networks.
- Case studies of major cyber incidents affecting industrial operations.



Day 2: Threats and Vulnerabilities in ICS Environments

- Common types of cyberattacks targeting industrial systems.
- Vulnerabilities in hardware, firmware, and communication protocols.
- Insider threats and social engineering in industrial contexts.
- Identity and access management for industrial networks.
- Network monitoring and anomaly detection techniques.

Day 3: Global Standards and Security Frameworks

- Overview of IEC 62443, NIST 800-82, and other global standards.
- Applying defense-in-depth principles in industrial cybersecurity.
- Implementing security policies for operational networks.
- Risk management and compliance in critical infrastructure.
- Building security governance models for industrial environments.

Day 4: Incident Detection, Response, and Forensics

- Implementing Security Information and Event Management SIEM systems.
- Using Intrusion Detection and Prevention Systems IDS/IPS in OT.
- Developing incident response IR capabilities for industrial systems.
- Conducting digital forensics in ICS environments.
- Leveraging AI and analytics for early threat detection.

Day 5: Secure Design and Business Continuity

- Designing secure ICS networks and architectures.
- Network segmentation and IT/OT isolation practices.
- Implementing disaster recovery and backup strategies.
- Testing and validating cybersecurity resilience through audits.
- Final workshop: building a cybersecurity roadmap for industrial environments.

Why Attend this Course: Wins & Losses!

- Gain a comprehensive understanding of cybersecurity in industrial environments.
- Learn to identify, analyze, and mitigate risks to control systems.
- Apply global standards and best practices for ICS protection.
- Develop effective strategies for proactive cyber defense.
- Enhance your organization’s incident response and recovery capabilities.
- Strengthen operational resilience and reduce downtime risk.
- Build technical and managerial confidence in securing industrial assets.
- Apply real-world insights through case studies and hands-on exercises.



Conclusion

Cybersecurity for Industrial Control Systems ICS is no longer a technical luxury — it is a strategic necessity for organizations that rely on automation and digital infrastructure. As cyber threats become more advanced and targeted, protecting ICS environments is critical to maintaining safety, reliability, and operational continuity.

This course provides participants with the expertise to design, implement, and sustain secure industrial networks. Through a combination of theoretical knowledge and practical application, participants will gain the skills needed to lead cybersecurity initiatives that safeguard both assets and people.

In a rapidly evolving digital landscape, mastering ICS cybersecurity ensures that industrial operations remain protected, resilient, and prepared for the challenges of tomorrow.

