QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1506

Industrial Cybersecurity & OT Security Training Course

INDUSTRIAL AUTOMATION & DIGITAL TECHNOLOGIES
INDUSTRIAL ENGINEERING, MAINTENANCE & OPERATIONS

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Industrial Cybersecurity & OT Security Training Course provides a comprehensive and practical framework for protecting industrial environments, operational technology, industrial control systems, and critical infrastructure from cybersecurity threats. The course is designed to help cybersecurity professionals, engineers, IT and OT specialists, managers, and decision makers understand the unique security requirements of operational environments where safety, availability, reliability, and continuity are essential.

The program examines the architecture and security characteristics of Operational Technology environments, including Industrial Control Systems, Supervisory Control and Data Acquisition systems, Distributed Control Systems, Programmable Logic Controllers, instrumentation and control systems, and industrial communication networks. Participants will develop a clear understanding of how cybersecurity principles must be adapted to environments where operational continuity and system stability are critical.

A major focus of the course is industrial cybersecurity risk management. Participants will learn how to identify and classify critical OT assets, analyze threats and vulnerabilities, assess operational and safety impacts, and establish security priorities based on business and operational risk. The course also addresses network segmentation, access control, remote access, asset management, patch and change management, backup strategies, and third-party security.

The course further develops practical capabilities in security monitoring, incident detection, industrial incident response, recovery planning, and cyber resilience. Through industrial case studies, risk assessment exercises, network security activities, and incident response simulations, participants will develop practical approaches for strengthening OT security while maintaining operational requirements. The Industrial Cybersecurity & OT Security Training Course supports organizations in reducing cybersecurity exposure and improving the resilience, security, and continuity of critical industrial operations.

Objectives

- Analyze the architecture of Operational Technology environments and identify critical industrial assets and associated cybersecurity risks during the first day of the course.
- Evaluate cybersecurity threats and vulnerabilities affecting Industrial Control Systems and

industrial networks using a structured risk-based approach.

- Develop a practical framework for classifying OT assets and prioritizing cybersecurity risks based on operational impact.
- Apply industrial network segmentation and access control principles to reduce unauthorized access and limit potential attack propagation.
- Design appropriate security controls for Industrial Control Systems while considering safety, availability, reliability, and operational continuity.
- Assess remote access, third-party, and supplier risks and identify appropriate controls to reduce exposure.
- Apply practical security monitoring techniques to identify abnormal activities and potential indicators of compromise within OT environments.
- Develop industrial cybersecurity incident response procedures covering detection, containment, investigation, recovery, and operational coordination.
- Evaluate asset management, patch management, change management, and backup practices to strengthen OT security and operational resilience.
- Prepare an actionable industrial cybersecurity improvement plan that aligns cybersecurity priorities with operational objectives and business continuity requirements.

Who Should Attend

The Industrial Cybersecurity & OT Security Training Course is designed for professionals working in cybersecurity, information technology, operational technology, engineering, industrial control, automation, network management, and industrial systems administration. It is particularly relevant to Industrial Control System engineers, instrumentation and control engineers, automation engineers, industrial network specialists, cybersecurity specialists, information security professionals, and OT security professionals.

The course is also suitable for operations, maintenance, engineering, cybersecurity, and IT managers; industrial security managers; control system specialists; industrial project managers; third-party and supplier risk professionals; and business continuity specialists. It is highly relevant to executives and decision makers in government entities, ministries, public-sector organizations, oil and gas companies, energy organizations, utilities, manufacturing facilities, and critical infrastructure organizations that depend on industrial automation, control systems, and operational technology.

Learning Outcomes

- Explain the fundamental differences between IT security and OT security and the specific requirements of industrial environments.
- Identify major Industrial Control System components and classify critical operational assets according to security and operational importance.
- Analyze cybersecurity threats and vulnerabilities affecting industrial control systems, devices, and networks.
- Assess cybersecurity risks and connect them to potential impacts on safety, availability, production, and operational continuity.
- Design appropriate principles for industrial network segmentation and isolation of critical systems.
- Apply identity, privilege, access control, and remote access security principles within OT environments.
- Assess supplier and third-party cybersecurity risks and develop appropriate security requirements.
- Develop practical monitoring, detection, and incident response procedures for industrial cybersecurity events.
- Evaluate asset management, patching, change management, and backup practices from an OT cybersecurity perspective.
- Prepare an actionable OT security and cyber resilience improvement plan aligned with operational and organizational requirements.

Course Outline

DAY 01

Industrial Cybersecurity and Operational Technology Fundamentals

- Introduction to industrial cybersecurity and OT security
- Differences between Information Technology and Operational Technology environments
- Industrial Control System architecture and components
- Supervisory Control and Data Acquisition systems
- Distributed Control Systems

DAY 01 — CONTINUED

- Programmable Logic Controllers and instrumentation and control systems
- Industrial networks and communication protocols
- Identification and classification of critical industrial assets
- Cybersecurity risks associated with industrial environments

PRACTICAL APPLICATION

Mapping assets and systems within an industrial environment and identifying critical assets requiring protection

DAY 02

Industrial Cybersecurity Risk, Threat and Vulnerability Assessment

- Industrial cybersecurity risk assessment principles and methodologies
- Identifying threat sources and potential attackers
- Vulnerability analysis for industrial systems, devices, and networks
- Assessing operational, safety, and production impacts
- Critical asset classification and risk prioritization
- Industrial attack scenarios and threat analysis
- Managing cybersecurity risks associated with legacy and difficult-to-update systems
- Establishing security priorities based on operational risk
- Developing an OT cybersecurity risk register

PRACTICAL APPLICATION

Conducting an industrial cybersecurity risk assessment and prioritizing high-impact scenarios

DAY 03

Industrial Network and System Security

- Principles of secure industrial network architecture
- Network segmentation and security zone design

DAY 03 — CONTINUED

- Controlling data flows between IT and OT environments
- Identity and privilege management for industrial systems
- Securing remote access to OT environments
- Industrial endpoint and system protection
- Patch and change management in operational environments
- Backup and recovery strategies for critical systems
- Supplier and third-party security management

PRACTICAL APPLICATION

Designing an industrial network security model and assigning appropriate security controls to each operational zone

DAY 04

Security Monitoring and Industrial Incident Response

- Security monitoring principles for OT environments
- Identifying abnormal activities and suspicious behavior
- Security event and log collection and analysis
- Indicators of compromise within industrial environments
- Industrial cybersecurity incident response
- Incident containment and operational impact reduction
- Industrial incident investigation and root cause analysis
- Business continuity and cyber recovery planning
- Incident response readiness testing and exercises

PRACTICAL APPLICATION

Simulating an industrial cybersecurity incident and developing detection, containment, response, and recovery procedures

DAY 05

OT Security Governance, Cyber Resilience and Improvement Planning

- OT cybersecurity governance and organizational responsibilities
- Security policies, procedures, roles, and accountability
- Cybersecurity risk management and regulatory requirements
- Industrial asset lifecycle management
- Assessing cybersecurity maturity and operational resilience
- Developing cybersecurity performance and risk indicators
- Third-party and supplier cybersecurity risk management
- Prioritizing cybersecurity improvement initiatives
- Developing an OT security improvement roadmap

FINAL WORKSHOP

Developing a comprehensive industrial cybersecurity and operational resilience improvement plan

Register or Request More Information

Course page: https://quest-training.com/courses/industrial-cybersecurity-ot-security-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440