Training course on Cybersecurity for Operational Technology (OT) in Infrastructure

Professional Development Training Course Outline

Category	Civil Engineering and Infrastructure Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Modern infrastructure is characterized by an increasing convergence of Information Technology (IT) and Operational Technology (OT), a trend significantly propelled by digitalization and the pervasive Industrial Internet of Things (IIoT). While this convergence offers substantial benefits in terms of enhanced efficiency and remote management capabilities, it simultaneously exposes critical infrastructure systems—such as intricate power grids, essential water treatment plants, complex transportation networks, and sophisticated manufacturing facilities—to unprecedented and evolving cyber risks. Cyberattacks targeting OT systems can precipitate severe consequences, ranging from tangible physical damage and widespread operational disruption to significant environmental harm, substantial economic losses, and even direct threats to public safety. Consequently, establishing robust OT cybersecurity measures is not merely advantageous but an absolute imperative for safeguarding national security and ensuring societal well-being.

Training Course on Cybersecurity for Operational Technology (OT) in Infrastructure is meticulously designed to provide participants with a comprehensive understanding of the unique challenges and critical best practices for securing OT environments within various infrastructure sectors. The curriculum will delve into the distinct characteristics that differentiate OT systems from IT counterparts, and participants will master advanced risk assessment methodologies specifically tailored for industrial control systems (ICS) and SCADA environments. A significant focus will be placed on developing robust defense-in-depth strategies, implementing secure network architectures (e.g., the Purdue Model), and effectively managing incident response protocols crucial for critical infrastructure. Through a balanced blend of essential theoretical foundations, hands-on exercises, and realistic simulated scenarios, this course will prepare attendees to confidently identify vulnerabilities, implement effective security controls, and skillfully respond to complex cyber threats in operational technology environments.

Programme Curriculum

Training Course on Cybersecurity for Operational Technology (OT) in Infrastructure

Introduction

Modern infrastructure is characterized by an increasing convergence of Information Technology (IT) and Operational Technology (OT), a trend significantly propelled by digitalization and the pervasive Industrial Internet of Things (IIoT). While this convergence offers substantial benefits in terms of enhanced efficiency and remote management capabilities, it simultaneously exposes critical infrastructure systems—such as intricate power grids, essential water treatment plants, complex transportation networks, and sophisticated manufacturing facilities—to unprecedented and evolving cyber risks. Cyberattacks targeting OT systems can precipitate severe consequences, ranging from tangible physical damage and widespread operational disruption to significant environmental harm, substantial economic losses, and even direct threats to public safety. Consequently, establishing robust OT cybersecurity measures is not merely advantageous but an absolute imperative for safeguarding national security and ensuring societal well-being.

Training Course on Cybersecurity for Operational Technology (OT) in Infrastructure is meticulously designed to provide participants with a comprehensive understanding of the unique challenges and critical best practices for securing OT environments within various infrastructure sectors. The curriculum will delve into the distinct characteristics that differentiate OT systems from IT counterparts, and participants will master advanced risk assessment methodologies specifically tailored for industrial control systems (ICS) and SCADA environments. A significant focus will be placed on developing robust defense-in-depth strategies, implementing secure network architectures (e.g., the Purdue Model), and effectively managing incident response protocols crucial for critical infrastructure. Through a balanced blend of essential theoretical foundations, hands-on exercises, and realistic simulated scenarios, this course will prepare attendees to confidently identify vulnerabilities, implement effective security controls, and skillfully respond to complex cyber threats in operational technology environments.

Course Objectives

Upon completion of this course, participants will be able to:

1. Analyze the fundamental concepts of Operational Technology (OT) and its unique cybersecurity challenges in infrastructure.
2. Comprehend the principles of IT/OT convergence, industrial control systems (ICS), SCADA, and IIoT architectures.
3. Master various risk assessment methodologies specifically tailored for OT environments.
4. Develop expertise in designing and implementing defense-in-depth cybersecurity strategies for critical infrastructure.
5. Formulate strategies for secure network segmentation and robust access control in OT systems.
6. Understand the critical role of incident response planning and forensic analysis in OT cyber incidents.
7. Implement robust approaches to patch management, vulnerability assessment, and threat intelligence for OT.
8. Explore key strategies for ensuring compliance with relevant OT cybersecurity standards (e.g., NIST, IEC 62443).
9. Apply methodologies for securing remote access and wireless communication in industrial environments.
10. Understand the importance of security awareness training and human factors in OT cybersecurity.

11. Develop preliminary skills in utilizing specialized OT security tools for monitoring and threat detection.
12. Design a comprehensive OT cybersecurity program and roadmap for an infrastructure organization.
13. Examine global best practices and future trends in securing critical infrastructure from cyber threats.

Target Audience

This course is ideal for professionals involved in the security, operation, and management of industrial and infrastructure systems:

1. OT Engineers & Technicians: Managing industrial control systems and automation.
2. Cybersecurity Professionals: Specializing in critical infrastructure protection.
3. IT Professionals: Transitioning into or collaborating with OT security.
4. Infrastructure Operations Managers: Overseeing the security and resilience of facilities.
5. Risk Management Professionals: Assessing and mitigating cyber risks in industrial environments.
6. Compliance & Audit Officers: Ensuring adherence to cybersecurity regulations and standards.
7. System Integrators: Designing and deploying secure OT/ICS solutions.
8. Government & Defense Personnel: Involved in critical infrastructure protection policies.

Course Duration: 5 Days

Course Modules

- **Module 1: Introduction to Operational Technology (OT) and Cyber Risks**
  - Define Operational Technology (OT) and differentiate it from Information Technology (IT).
  - Discuss the architecture of Industrial Control Systems (ICS), SCADA, DCS, and PLC.
  - Understand the unique characteristics of OT environments: real-time, safety-critical, legacy systems.
  - Explore the history of OT cyberattacks and their potential impact on critical infrastructure.
  - Identify the drivers for IT/OT convergence and the resulting cybersecurity challenges.
- **Module 2: OT Cybersecurity Frameworks and Risk Assessment**
  - Comprehend leading OT cybersecurity frameworks (e.g., NIST Cybersecurity Framework, IEC 62443).
  - Learn about risk assessment methodologies specifically adapted for OT environments.
  - Master techniques for identifying critical assets, threat actors, and attack vectors in ICS.
  - Discuss vulnerability assessment and penetration testing considerations for OT systems.
  - Apply risk management principles to prioritize and mitigate OT cyber threats.
- **Module 3: Secure OT Network Architectures and Segmentation**
  - Develop expertise in designing secure network architectures for OT environments (e.g., Purdue Model).
  - Learn about network segmentation, firewalls, and demilitarized zones (DMZs) in ICS networks.
  - Master techniques for implementing robust access control mechanisms: least privilege, role-based access.
  - Discuss the challenges of managing remote access to OT systems securely.
  - Explore the use of secure protocols and encrypted communications in industrial settings.
- **Module 4: Endpoint Security and Industrial IoT (IIoT) Security**
  - Formulate strategies for securing endpoints within the OT environment (PLCs, RTUs, HMI).
  - Understand patch management challenges and strategies for legacy OT systems.
  - Explore techniques for implementing antivirus, whitelisting, and integrity checks on OT devices.
  - Discuss the unique security considerations for Industrial Internet of Things (IIoT) deployments.
  - Apply security best practices for IIoT devices, sensors, and cloud connectivity.

- **Module 5: OT Incident Response and Disaster Recovery**
    - Understand the critical role of incident response planning tailored for OT cyber incidents.
    - Implement robust approaches to incident detection, analysis, containment, eradication, and recovery.
    - Explore techniques for conducting forensic analysis in OT environments without disrupting operations.
    - Discuss communication strategies and stakeholder coordination during an OT cyber incident.
    - Examine disaster recovery and business continuity planning for critical infrastructure.
- **Module 6: Threat Intelligence and Monitoring for OT**
    - Apply methodologies for collecting, analyzing, and disseminating OT threat intelligence.
    - Master techniques for continuous security monitoring of OT networks and systems.
    - Understand the use of Security Information and Event Management (SIEM) for OT environments.
    - Discuss behavioral anomaly detection, intrusion detection systems (IDS), and intrusion prevention systems (IPS) in OT.
    - Explore specialized OT security tools and platforms for visibility and threat hunting.
- **Module 7: Compliance, Governance, and Supply Chain Security**
    - Explore key strategies for ensuring compliance with industry regulations and standards (e.g., NERC CIP, NIS Directive).
    - Learn about establishing robust OT cybersecurity governance structures and policies.
    - Discuss the importance of supply chain cybersecurity for OT components and services.
    - Understand vendor risk management and secure development lifecycle for industrial solutions.
    - Examine legal and ethical considerations in OT cybersecurity.
- **Module 8: Emerging Threats and Future Trends in OT Security**
    - Examine global best practices and lessons learned from major OT cyber incidents.
    - Develop preliminary skills in assessing and responding to emerging threats: ransomware, nation-state attacks.
    - Discuss the impact of AI/ML on both offensive and defensive OT cybersecurity.
    - Explore future trends: quantum-resistant cryptography, zero trust architectures in OT, cybersecurity mesh.
    - Design a strategic roadmap for building a resilient and future-proof OT cybersecurity posture.

Training Methodology

- **Interactive Workshops:** Facilitated discussions, group exercises, and problem-solving activities.
- **Case Studies:** Real-world examples to illustrate successful community-based surveillance practices.
- **Role-Playing and Simulations:** Practice engaging communities in surveillance activities.
- **Expert Presentations:** Insights from experienced public health professionals and community leaders.
- **Group Projects:** Collaborative development of community surveillance plans.
- **Action Planning:** Development of personalized action plans for implementing community-based surveillance.
- **Digital Tools and Resources:** Utilization of online platforms for collaboration and learning.
- **Peer-to-Peer Learning:** Sharing experiences and insights on community engagement.
- **Post-Training Support:** Access to online forums, mentorship, and continued learning resources.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

- Participants must be conversant in English.
- Upon completion of training, participants will receive an Authorized Training Certificate.
- The course duration is flexible and can be modified to fit any number of days.
- Course fee includes facilitation, training materials, 2 coffee breaks, buffet lunch, and a Certificate upon successful completion.
- One-year post-training support, consultation, and coaching provided after the course.
- Payment should be made at least a week before the training commencement to Fineskill Training Center account, as indicated in the invoice, to enable better preparation.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now