Industrial Control Systems Cybersecurity Standards Training Course

16 - 20 Nov 2026

Sharm El-Sheikh

4100 € (Per Person)

Ref: #ERE1826_273689

Course Introduction / Overview:

The convergence of Information Technology (IT) and Operational Technology (OT) has created unprecedented efficiencies but also exposed critical infrastructure to new and sophisticated cyber threats. Industrial Control Systems (ICS), which manage essential services in sectors like energy, manufacturing, and water treatment, are now prime targets for cyberattacks. This course provides a comprehensive and practical understanding of the standards and best practices required to secure these vital systems. As discussed by experts like Eric J. Knapp in his seminal work, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems," a specialized approach is necessary to protect environments where safety and availability are paramount. This program, offered by BIG BEN Training Center, moves beyond theoretical concepts to provide actionable strategies based on globally recognized frameworks such as IEC 62443 and the NIST Cybersecurity Framework. Participants will gain the essential knowledge to design, implement, and manage a robust cybersecurity program for their ICS and SCADA environments, ensuring operational resilience and protecting national critical infrastructure from evolving threats.

Target Audience / This training course is suitable for:

- Control Systems Engineers and Technicians.
- Operational Technology (OT) Security Professionals.
- IT Security Professionals transitioning to OT environments.
- SCADA System Operators and Administrators.
- Plant Managers and Operations Supervisors.
- Automation and Instrumentation Engineers.
- Industrial Network Architects.
- Incident Response Team Members.
- Compliance and Risk Managers in industrial sectors.

Target Sectors and Industries:

- Energy and Utilities (Electricity, Oil, and Gas).
- Manufacturing and Industrial Automation.
- Water and Wastewater Management.
- Chemical and Pharmaceutical Production.
- Transportation and Logistics (Rail, Aviation, Maritime).
- Food and Beverage Processing.
- Mining and Materials.
- Government agencies responsible for critical infrastructure protection.

Target Organizations Departments:

- Operations and Production.
- Engineering and Maintenance.
- Information Technology (IT) and Cybersecurity.
- Health, Safety, and Environment (HSE).
- Plant Management.
- Risk and Compliance.
- Physical Security.
- Research and Development (R&D).

Course Offerings:

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

- Differentiate between IT and OT security principles and priorities.
- Apply the Purdue Model for secure industrial network architecture.
- Implement key security controls from the IEC 62443 standard.
- Utilize the NIST Cybersecurity Framework for ICS risk management.
- Conduct a comprehensive risk assessment for an OT environment.
- Secure common industrial protocols like Modbus, DNP3, and OPC.
- Develop and implement an effective ICS incident response plan.
- Integrate threat intelligence into an OT security strategy.
- Manage vulnerabilities in systems with high-availability requirements.
- Design a defense-in-depth security posture for critical infrastructure.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster deep understanding and practical skill acquisition. This course employs a blended learning approach that combines expert-led instruction with interactive, hands-on activities. Participants will engage with real-world case studies of significant ICS cyber incidents, analyzing attack vectors, impacts, and mitigation strategies. The curriculum is structured around practical application, moving from foundational concepts to advanced security implementation based on standards like IEC 62443. Group discussions and collaborative problem-solving sessions will encourage participants to share experiences and develop solutions for challenges specific to their industries. Simulated lab environments will provide a safe space to practice network segmentation, firewall rule configuration, and incident response drills without impacting live systems. Our experienced instructors facilitate a dynamic learning environment, providing continuous feedback and ensuring that theoretical knowledge is translated into tangible skills that can be immediately applied to protect critical operational technology assets.

Course Agenda (Course Units):

Unit One: Fundamentals of ICS and OT Cybersecurity

- Introduction to Industrial Control Systems (ICS), SCADA, and DCS.
- The critical differences between IT and OT security objectives.
- Understanding the Purdue Enterprise Reference Architecture.
- Common threats, vulnerabilities, and attack vectors in OT environments.
- The consequences of an ICS security breach.
- Historical ICS cyber incidents and lessons learned.
- The convergence of IT and OT and its security implications.

Unit Two: Core ICS Security Standards and Frameworks

- Deep dive into the ISA/IEC 62443 series of standards.
- Applying the NIST Cybersecurity Framework (CSF) to ICS.
- Overview of other relevant standards (NERC CIP, ISO 27001).
- Establishing security zones and conduits.
- Understanding Security Levels (SLs) and their application.
- Mapping security requirements to industrial processes.
- Building a standards-based ICS cybersecurity program.

Unit Three: Architecting and Securing ICS Networks

- Principles of defense-in-depth for OT networks.
- Implementing robust network segmentation and segregation.
- Configuring firewalls and unidirectional gateways for OT.
- Deploying and managing Intrusion Detection Systems (IDS) in ICS.
- Securing industrial protocols (e.g., Modbus TCP, DNP3, S7).
- Wireless security considerations in industrial environments.
- Secure remote access solutions for vendors and operators.

Unit Four: ICS Risk Management and Vulnerability Assessment

- Conducting a comprehensive ICS risk assessment.
- Asset identification and inventory management in OT.
- Threat modeling for industrial processes.
- Vulnerability scanning and management in sensitive OT environments.
- Patch management strategies for systems that cannot be rebooted.
- Implementing compensating controls for legacy systems.
- Leveraging OT-specific threat intelligence feeds.

Unit Five: Incident Response and Recovery for OT Systems

- Developing an ICS-specific incident response plan.
- Key roles and responsibilities in an OT incident response team.
- Detection, analysis, and containment of an OT security incident.
- Digital forensics and evidence collection in an industrial setting.
- Business continuity and disaster recovery planning for OT.
- Safe and secure system restoration procedures.
- Tabletop exercises and simulation drills for incident response readiness.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As IT and OT systems continue to converge, how can organizations balance the operational requirements of availability and safety with the security imperative of confidentiality and integrity without stifling innovation?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing squarely on the practical application of globally recognized standards within real-world industrial environments. Unlike purely theoretical programs, our curriculum is built around the ISA/IEC 62443 and NIST frameworks, teaching participants not just what to do, but precisely how to implement these standards to build a defensible security architecture. We bridge the critical gap between IT security professionals and OT engineers by fostering a common language and understanding of the unique challenges in operational technology, where safety and uptime are non-negotiable. The course content is enriched with detailed case studies of actual ICS cyber incidents, providing invaluable lessons on attack methodologies and effective defensive strategies. Our instructors are seasoned professionals with extensive field experience in securing critical infrastructure, offering insights that go far beyond textbooks. The emphasis is on developing a strategic mindset for risk management and incident response, empowering participants to make informed decisions that protect their organization's most critical assets from sophisticated cyber threats.