Critical Infrastructure SCADA Security and Defense Training Course



19 - 23 Oct 2026

Cape town

4600 € (Per Person)

Ref: #CYB7153_272578

Course Introduction / Overview:

In an era where industrial automation and connectivity are paramount, the security of Supervisory Control and Data Acquisition (SCADA) systems has become a critical concern for national security and economic stability. This comprehensive training course is meticulously designed to address the unique cybersecurity challenges inherent in Operational Technology (OT) and Industrial Control Systems (ICS) that manage our most vital infrastructure. As highlighted 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," the convergence of IT and OT networks has expanded the attack surface, making these once-isolated systems vulnerable to sophisticated cyber threats. This program, offered by BIG BEN Training Center, moves beyond theoretical concepts to provide actionable strategies and hands-on knowledge. Participants will explore the entire lifecycle of SCADA security, from initial risk assessment and architectural design to advanced threat detection, incident response, and compliance with international standards. We delve into the specific protocols, hardware, and software that define industrial environments, equipping professionals with the specialized skills needed to build a resilient defense against cyber-attacks and ensure the uninterrupted operation of critical services.

Target Audience / This training course is suitable for:

- SCADA and ICS Engineers.
- Control Systems Operators and Technicians.
- Operational Technology (OT) Security Professionals.
- IT Security Analysts and Managers with OT responsibilities.
- Plant Managers and Operations Supervisors.
- Infrastructure Protection and Emergency Response Planners.
- Cybersecurity Consultants specializing in industrial sectors.
- Government and Regulatory Compliance Officers.
- Automation and Process Control Engineers.
- Network and Systems Administrators for industrial environments.

Target Sectors and Industries:

- Energy and Utilities (Electricity, Power Grids, Nuclear).
- Oil and Gas (Upstream, Midstream, Downstream).
- Water and Wastewater Management.
- Manufacturing and Industrial Production.
- Transportation and Logistics (Rail, Aviation, Maritime).
- Pharmaceuticals and Chemical Processing.
- Government agencies and defense contractors.
- Telecommunications and Data Centers.
- Food and Beverage Production.
- Building Management and Automation.

Target Organizations Departments:

- Operations and Plant Management.
- Information Technology (IT) and Cybersecurity.
- Engineering and Maintenance.
- Health, Safety, and Environment (HSE).
- Risk Management and Compliance.
- Physical Security and Asset Protection.
- Research and Development (R&D).
- Internal Audit and Governance.
- Emergency Response and Business Continuity.
- Project Management.

Course Offerings:

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

- Analyze the unique architecture and vulnerabilities of SCADA, DCS, and PLC systems.
- Differentiate between IT and OT security priorities and challenges.
- Conduct comprehensive risk and vulnerability assessments for industrial control systems.
- Implement a defense-in-depth security strategy tailored for OT environments.
- Secure industrial network protocols such as Modbus, DNP3, and Profinet.
- Design and configure secure network segmentation based on the Purdue Model.
- Develop and deploy effective OT monitoring and threat detection capabilities.
- Formulate a robust incident response and recovery plan specific to SCADA systems.
- Apply principles from key industry standards like IEC 62443 and NIST frameworks.
- Evaluate and mitigate security risks associated with the Industrial Internet of Things (IIoT).
- Harden controllers, workstations, and servers within an industrial environment.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster deep understanding and practical skill acquisition through a dynamic, immersive learning experience. This course rejects a passive, lecture-only approach, instead emphasizing active participation and real-world application. Our expert instructors facilitate highly interactive sessions, combining foundational theory with practical case studies of major ICS cyber incidents like Stuxnet and the Ukrainian power grid attacks. Participants will engage in collaborative group exercises and workshops to analyze threat scenarios and design defensive architectures. The curriculum incorporates simulated lab environments where attendees can safely explore SCADA system vulnerabilities and practice implementing security controls without risk to live systems. A significant portion of the course is dedicated to team-based problem-solving, encouraging the exchange of diverse perspectives from various industries. Continuous feedback loops and Q&A sessions are integrated throughout the five days, ensuring that all concepts are clearly understood and that participants can directly relate the training content to the specific challenges they face in their own operational environments. This blended approach ensures that attendees leave not just with knowledge, but with the confidence to apply it effectively.

Course Agenda (Course Units):

Unit One: Fundamentals of SCADA and ICS Cybersecurity

- Introduction to Industrial Control Systems (ICS), SCADA, DCS, and PLCs.
- Comparing and contrasting IT and Operational Technology (OT) security.
- Exploring common SCADA system architectures and components.
- Understanding industrial network protocols (Modbus, DNP3, OPC).
- The critical role of Human-Machine Interfaces (HMIs).
- Key differences in security objectives: Confidentiality, Integrity, and Availability (CIA) in OT.
- The history and evolution of cyber threats against critical infrastructure.

Unit Two: Threat Landscape and Vulnerability Assessment

- Identifying common attack vectors and threat actors in the OT space.
- Analyzing famous ICS malware and attacks (e.g., Stuxnet, Havex, Triton).
- Conducting vulnerability assessments in sensitive OT environments.
- Techniques for asset discovery and inventory in industrial networks.
- Introduction to risk management frameworks for ICS.
- Passive vs. active scanning techniques and their implications.
- Understanding the consequences of a compromised control system.

Unit Three: Designing a Defensible SCADA Architecture

- The Defense-in-Depth security principle for industrial environments.
- Implementing network segmentation using the Purdue Model.
- Configuring and managing firewalls and demilitarized zones (DMZs) for OT.
- Deploying Intrusion Detection and Prevention Systems (IDS/IPS) for ICS.
- Hardening SCADA servers, workstations, and embedded devices.
- Implementing secure remote access solutions for vendors and operators.
- The role of data diodes in ensuring one-way data flow.

Unit Four: OT Security Monitoring and Incident Response

- Establishing a baseline for normal network and process behavior.
- Continuous security monitoring strategies for OT networks.
- Log collection, correlation, and analysis in an ICS context.
- Developing an OT-specific Incident Response (IR) plan.
- Containment, eradication, and recovery strategies for industrial incidents.
- Digital forensics challenges and techniques in SCADA systems.
- Coordinating response efforts between IT, OT, and management teams.

Unit Five: Compliance, Standards, and Future Challenges

- Overview of key ICS security standards and frameworks (IEC 62443, NIST CSF, NERC CIP).
- Achieving and maintaining regulatory compliance.
- Developing effective security policies and procedures for OT.
- The impact of the Industrial Internet of Things (IIoT) on SCADA security.
- Securing wireless technologies in industrial settings.
- The role of artificial intelligence and machine learning in OT defense.
- Building a sustainable culture of security within the organization.

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 become increasingly interconnected, how can organizations balance the need for operational efficiency with the imperative of robust cybersecurity without stifling innovation?

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

This course distinguishes itself by moving beyond generic IT security principles and immersing participants in the specific, high-stakes world of Operational Technology (OT). Unlike programs that simply repackage IT concepts, our curriculum is built from the ground up to address the unique protocols, legacy systems, and stringent availability requirements of critical infrastructure. We emphasize a practical, risk-based approach, teaching not just the "what" but the "why" and "how" of securing complex industrial environments. The course content is deeply rooted in globally recognized standards like IEC 62443, providing a strategic framework for building a mature security program rather than just implementing disparate tools. Furthermore, our focus on real-world case studies and simulated incident response scenarios provides a level of practical insight that is difficult to obtain elsewhere. Participants will learn to think like an attacker targeting industrial systems and, more importantly, how to build a resilient, multi-layered defense. The curriculum bridges the critical gap between engineering, operations, and cybersecurity, fostering a holistic understanding essential for protecting the systems that underpin modern society.