SCADA Security & Critical Infrastructure Protection Training Course

Ref: #CYB6049

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity and industrial control systems (ICS) professionals with the specialized knowledge required to secure Supervisory Control and Data Acquisition (SCADA) systems. These systems are the backbone of our critical infrastructure, managing everything from power grids and water treatment plants to oil and gas pipelines. A successful cyberattack on these systems can have devastating real-world consequences, far beyond a typical data breach. This program goes beyond traditional IT security to focus on the unique challenges of securing operational technology (OT) environments, where uptime and safety are the top priorities. Participants will learn how to identify vulnerabilities, implement robust access controls, and respond to threats that could compromise physical systems. We will cover key topics like network segmentation, threat intelligence for SCADA, and the integration of IT and OT security practices. Drawing from the academic work of renowned authors like Eric Byres and his extensive research on industrial network security, this program provides a strategic and practical framework for safeguarding our most vital assets. This course at BIG BEN Training Center will empower you to protect critical infrastructure from modern cyber threats.

Target Audience / This training course is suitable for:

- SCADA engineers.
- Industrial control systems (ICS) security professionals.
- Cybersecurity analysts.
- Plant managers and operators.
- Critical infrastructure security personnel.
- IT and OT convergence specialists.
- Risk managers in industrial sectors.

Target Sectors and Industries:

- Energy and utilities.
- Oil and gas.
- Water treatment and public works.
- Manufacturing.
- Transportation.
- Government agencies and equivalents.
- Defense and military.

Target Organizations Departments:

- Operational Technology (OT).
- Information Technology (IT).
- Cybersecurity.
- Plant Operations.
- Risk Management.
- Engineering.
- Physical Security.

Course Offerings:

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

- Secure SCADA and ICS networks and devices.
- Implement a security program that aligns with OT environments.
- Assess and mitigate vulnerabilities in critical infrastructure.
- Develop a robust incident response plan for an ICS attack.
- Manage privileged access to critical control systems.
- Ensure compliance with industry standards and regulations.
- Conduct a risk assessment for an industrial control system.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, case-study-driven methodology that focuses on the unique challenges of SCADA security. The program includes a series of simulated attack scenarios on a virtualized industrial network. Participants will work with specialized tools to identify vulnerabilities, detect intrusions, and practice emergency response procedures. The course emphasizes a collaborative approach, encouraging IT and OT professionals to work together to solve complex security problems. The instructor will provide expert guidance and feedback throughout the labs, ensuring that you develop the critical thinking and problem-solving skills required for high-stakes industrial roles. This approach ensures the knowledge and skills gained are directly applicable to protecting physical assets and ensuring public safety.

Course Agenda (Course Units):

Unit One: The SCADA Threat Landscape

- Introduction to SCADA and ICS.
- The difference between IT and OT security.
- Unique attack vectors for industrial systems.
- The Stuxnet case study and its lessons.
- The convergence of IT and OT.
- The importance of physical security.
- Operational continuity is a top priority.

Unit Two: SCADA Network Security

- Network segmentation for industrial networks.
- Securing remote access and VPNs.
- Firewalls and intrusion detection systems for OT.
- Securing Human-Machine Interfaces (HMIs).
- Vulnerability management for industrial systems.
- Hardening SCADA servers and controllers.
- Practical lab: a network segmentation exercise.

Unit Three: Incident Response in OT Environments

- Developing a specialized incident response plan for ICS.
- Containment and recovery protocols.
- The challenge of forensics in an OT environment.
- Communication with plant operators and management.
- Reporting requirements and regulatory compliance.
- Lessons learned from past incidents.
- Case study: a simulated SCADA system compromise.

Unit Four: Risk Management and Auditing

- Conducting a risk assessment for SCADA systems.
- Threat modeling for critical infrastructure.
- Vendor and third-party risk management.
- Auditing industrial control systems.
- Security policies and procedures for plant personnel.
- Compliance with industry standards (e.g., NIST, IEC 62443).
- Practical lab: a SCADA risk assessment.

Unit Five: The Future of Critical Infrastructure Security

- The role of AI and machine learning.
- Predictive maintenance and security analytics.
- The challenge of legacy systems.
- The Internet of Things (IoT) in industrial settings.
- Threat intelligence for OT.
- Final project: a comprehensive security plan.
- The future of SCADA security.
- Frequently Asked Questions:

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:

In industrial environments where legacy systems are deeply integrated and cannot be easily patched, how can security professionals effectively mitigate a zero-day vulnerability without disrupting continuous operations?

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

This course stands out by providing a unique and vital focus on securing SCADA systems and critical infrastructure. Unlike generic cybersecurity training, this program addresses the distinct challenges of Operational Technology (OT) environments, where safety and continuous operation are paramount. The curriculum is built around a practical, hands-on approach. It teaches you how to manage the unique risks posed by industrial systems, where a cyberattack can lead to physical damage or public safety issues. The emphasis on real-world case studies and simulated attack scenarios gives you a direct, actionable understanding of how to apply security principles in a high-stakes industrial setting. This course is for professionals who recognize the critical importance of protecting the systems that power our modern world.