Secure Network Design for Critical Infrastructure Training Course



23 - 27 Nov 2026

Cape town

4600 € (Per Person)

Ref: #NO2137_279227

Course Introduction / Overview:

This comprehensive training course provides an in-depth exploration of the principles and practices required to design and implement secure network architectures for critical infrastructure and industrial control systems. In an era where the convergence of Information Technology (IT) and Operational Technology (OT) exposes essential services to new and sophisticated cyber threats, a proactive and robust security posture is no longer optional, but a fundamental necessity. This program, offered by BIG BEN Training Center, moves beyond generic IT security to address the unique challenges of OT environments, where safety, reliability, and availability are paramount. Drawing upon foundational concepts detailed by experts like Andrew Ginter and in seminal works such as "Industrial Network Security" by Eric D. Knapp, participants will learn to apply proven methodologies like the Purdue Model and defense-in-depth strategies. The curriculum is meticulously designed to equip professionals with the skills to build resilient, segmented, and defensible networks that protect national infrastructure, industrial processes, and public safety from cyber-physical attacks. This course is the definitive guide for professionals tasked with safeguarding the systems that power our modern world.

Target Audience / This training course is suitable for:

- Network Engineers and Architects.
- Cybersecurity Analysts and Consultants.
- Industrial Control System (ICS) and SCADA Engineers.
- IT and OT Managers.
- Plant and Operations Managers.
- Infrastructure Planners and Designers.
- Security Operations Center (SOC) personnel.
- Compliance and Risk Management Officers.
- System Integrators.
- Automation Engineers.

Target Sectors and Industries:

- Energy and Utilities (Electricity, Oil, and Gas).
- Water and Wastewater Management.
- Manufacturing and Industrial Production.
- Transportation Systems (Rail, Aviation, and Maritime).
- Healthcare and Public Health.
- Chemical and Petrochemical Industries.
- Telecommunications.
- Financial Services Infrastructure.
- Government, Defense, and Public Sector Agencies.
- Food and Agriculture.

Target Organizations Departments:

- Information Technology (IT) and Cybersecurity.
- Operational Technology (OT) and Process Control.
- Engineering and Maintenance.
- Corporate Security and Physical Security.
- Risk Management and Compliance.
- Operations and Production.
- Research and Development.
- Facilities Management.
- Internal Audit.

Course Offerings:

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

- Analyze the unique threats and vulnerabilities facing critical infrastructure networks.
- Apply the Purdue Model for enterprise and industrial control system network segmentation.
- Design and implement a defense-in-depth security strategy for OT environments.
- Develop secure network architectures using firewalls, DMZs, and unidirectional gateways.
- Harden industrial network devices such as PLCs, RTUs, and HMIs.
- Implement security controls for industrial protocols like Modbus TCP, DNP3, and OPC UA.
- Conduct risk assessments specific to industrial control systems.
- Develop and integrate an OT-specific incident response plan.
- Evaluate and apply principles from standards like IEC 62443 and the NIST Cybersecurity Framework.
- Design secure remote access solutions for OT environments.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants not only learn theoretical concepts but can also apply them effectively in real-world scenarios. This course utilizes a blended learning approach that combines expert-led instruction with hands-on exercises, collaborative workshops, and in-depth case study analysis. Participants will engage in group activities to design secure network diagrams, debate risk mitigation strategies, and develop incident response playbooks. The sessions are structured to encourage active participation, with facilitated discussions and Q&A segments allowing for a deep dive into complex topics. We will analyze historical cyber-physical incidents to understand attack vectors and defensive failures, fostering a proactive security mindset. The learning environment is built on a foundation of continuous feedback and peer-to-peer knowledge sharing, empowering attendees to master the art and science of securing critical infrastructure networks. This practical, hands-on approach ensures that skills are not just learned but are retained and immediately applicable in the participant's professional role.

Course Agenda (Course Units):

Unit One: Foundations of Critical Infrastructure Security

- Introduction to Critical Infrastructure and Operational Technology (OT).
- Understanding the differences between IT and OT security priorities.
- Key threats, vulnerabilities, and attack vectors in ICS environments.
- Overview of major cyber-physical incidents and lessons learned.
- Introduction to industry standards and frameworks (NIST CSF, IEC 62443).
- The convergence of IT and OT networks and its security implications.
- Defining the roles and responsibilities in OT security.

Unit Two: Secure Network Architecture and Design Principles

- The Purdue Model for ICS Network Segmentation.
- Implementing defense-in-depth strategies for OT.
- Designing secure zones, conduits, and industrial demilitarized zones (IDMZ).
- Principles of network segregation using VLANs and firewalls.
- Secure design for remote access to OT systems.
- Understanding the role of unidirectional gateways and data diodes.
- Physical security considerations in network design.

Unit Three: Securing Industrial Protocols and Devices

- Vulnerabilities in common industrial protocols (Modbus, DNP3, S7).
- Strategies for securing legacy systems and protocols.
- Hardening endpoints: PLCs, RTUs, HMIs, and engineering workstations.
- Implementing secure network device management and configuration.
- Patch management strategies in an OT environment.
- Application whitelisting and access control for industrial systems.
- Cryptography and its application in OT networks.

Unit Four: Network Monitoring and Threat Detection

- Establishing a baseline for normal network behavior in OT.
- Deploying and configuring Intrusion Detection Systems (IDS) for industrial networks.
- Log management and Security Information and Event Management (SIEM) in OT.
- Passive vs. active network monitoring techniques.
- Integrating threat intelligence into OT security operations.
- Developing an effective OT network visibility strategy.
- Anomaly detection and its role in early threat identification.

Unit Five: Risk Management and Incident Response

- Conducting cyber risk and vulnerability assessments for OT systems.
- Developing and implementing an OT-specific incident response plan.
- Business continuity and disaster recovery planning for critical infrastructure.
- Forensics and evidence collection in an industrial environment.
- Building a resilient network architecture against advanced persistent threats (APTs).
- Exploring emerging concepts like Zero Trust architecture for OT.
- Future trends and challenges in critical infrastructure security.

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 networks continue to converge, how can an organization maintain the operational reliability and safety of its critical infrastructure while adopting modern, data-driven security paradigms like Zero Trust?

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

This training course distinguishes itself by focusing squarely on the architectural and design-centric aspects of securing critical infrastructure, a perspective often overlooked by product-specific or purely policy-based training. While other courses may teach how to configure a specific firewall, our program teaches the fundamental principles of where to place that firewall, why it is needed there, and how it fits into a holistic, resilient security posture based on proven models like Purdue and defense-in-depth. The curriculum is vendor-agnostic, providing participants with transferable skills and strategic knowledge applicable across any technology stack. We emphasize the unique operational constraints of OT environments, where uptime and safety are non-negotiable, and integrate these realities into every module. By analyzing real-world case studies and engaging in hands-on design workshops, participants move beyond theory to develop a deep, intuitive understanding of how to build defensible networks from the ground up. The course cultivates a proactive, risk-based mindset, empowering professionals not just to react to threats, but to anticipate and architect systems that are inherently secure and resilient by design.