OT/IoT Security: Industrial Control Systems & Smart Devices Training Course



16 - 20 Nov 2026

Cape town

4600 € (Per Person)

Ref: #CYB6977_264035

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity professionals and engineers with the specialized knowledge and skills required to protect operational technology (OT) and the Internet of Things (IoT) devices. The convergence of IT and OT has created new vulnerabilities. This has made securing industrial control systems and smart devices more critical than ever. A successful cyberattack on these systems can lead to physical damage, operational downtime, or a loss of public trust. This program goes beyond traditional IT security to focus on the unique challenges posed by a world where everything from factory robots to smart thermostats is connected to the internet. Participants will learn how to identify vulnerabilities, implement robust access controls, and respond to threats that could compromise physical systems and data privacy. We will cover key topics like network segmentation for industrial environments, threat modeling for smart devices, and the integration of IT and OT security practices. Drawing from the academic research of renowned authors like Edward Amoroso and his book "Cybersecurity: The Essential Body of Knowledge," this program provides a strategic and practical framework for safeguarding our most vital physical and digital assets. This course at BIG BEN Training Center will empower you to protect industrial and consumer environments from modern cyber threats.

Target Audience / This training course is suitable for:

- OT and IoT security specialists.
- Industrial control systems (ICS) engineers.
- Cybersecurity analysts.
- Network architects.
- Product security managers.
- IT administrators.
- Risk managers in industrial and smart sectors.

Target Sectors and Industries:

- Manufacturing.
- Energy and utilities.
- Smart cities and smart homes.
- Healthcare.
- Automotive.
- Government agencies and equivalents.
- Telecommunications.

Target Organizations Departments:

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

Course Offerings:

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

- Secure industrial control systems (ICS).
- Implement a security program that aligns with OT environments.
- Assess and mitigate vulnerabilities in smart devices.
- Develop a robust incident response plan for an OT or IoT attack.
- Manage privileged access to critical systems.
- Ensure compliance with industry standards and regulations.
- Conduct a risk assessment for an interconnected environment.

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 OT and IoT security. The program includes a series of simulated attack scenarios on a virtualized industrial network and a network of smart devices. Participants will work with specialized tools to identify vulnerabilities, detect intrusions, and practice emergency response procedures. The course emphasizes a proactive and a practical approach. It teaches participants how to not only deploy technology but also how to manage the lifecycle security of smart devices. 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 and consumer roles. This approach ensures the knowledge and skills gained are directly applicable to protecting physical assets and data privacy.

Course Agenda (Course Units):

Unit One: The Converged IT/OT/IoT Landscape

- Introduction to OT and IoT.
- The difference between IT, OT, and IoT security.
- New attack vectors and vulnerabilities.
- The expanded attack surfaces.
- The importance of physical security.
- Operational continuity is a top priority.
- Case study: a compromised manufacturing plant.

Unit Two: Industrial Control System Security

- Securing SCADA and DCS systems.
- Network segmentation for industrial networks.
- Secure remote access.
- Firewalls and intrusion detection systems for OT.
- Vulnerability management for industrial systems.
- Hardening industrial servers and controllers.
- Practical lab: a network segmentation exercise.

Unit Three: IoT Security and Privacy

- The IoT threat landscape.
- Common IoT vulnerabilities.
- Securing smart devices and sensors.
- Data privacy and collection in IoT.
- Device authentication and access control.
- Managing the lifecycle security of IoT devices.
- Case study: a simulated smart home breach.

Unit Four: Risk Management and Incident Response

- Conducting a risk assessment for OT and IoT.
- Developing an incident response plan for a converged environment.
- Forensics in OT and IoT.
- Threat intelligence for industrial and smart devices.
- Compliance with industry standards (e.g., NIST, IEC 62443).
- Auditing a security program.
- Practical lab: an incident response scenario.

Unit Five: The Future of OT/IoT Security

- The role of AI and machine learning.
- Predictive security analytics.
- Securing the Industrial Internet of Things (IIoT).
- The challenge of legacy systems.
- The future of smart cities.
- Final project: a comprehensive security plan.
- Emerging threats.
- 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:

As smart devices become more embedded in our daily lives, how can security professionals balance the need for continuous security patching with the practical challenges of managing thousands of devices that may be in the hands of non-technical users?

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

This course stands out by providing a unique and vital focus on the security of interconnected OT and IoT environments. Unlike generic cybersecurity training, this program addresses the distinct challenges of securing both industrial control systems and consumer-facing smart devices. The curriculum is built around a practical, hands-on approach. It teaches you how to manage the unique risks posed by systems where a cyberattack can lead to physical damage or a loss of personal privacy. The emphasis on real-world case studies and simulated attack scenarios gives you a direct, actionable understanding of how to apply security principles to a converged and dynamic environment. This course is for professionals who are ready to move beyond traditional IT security to protect our physical world.