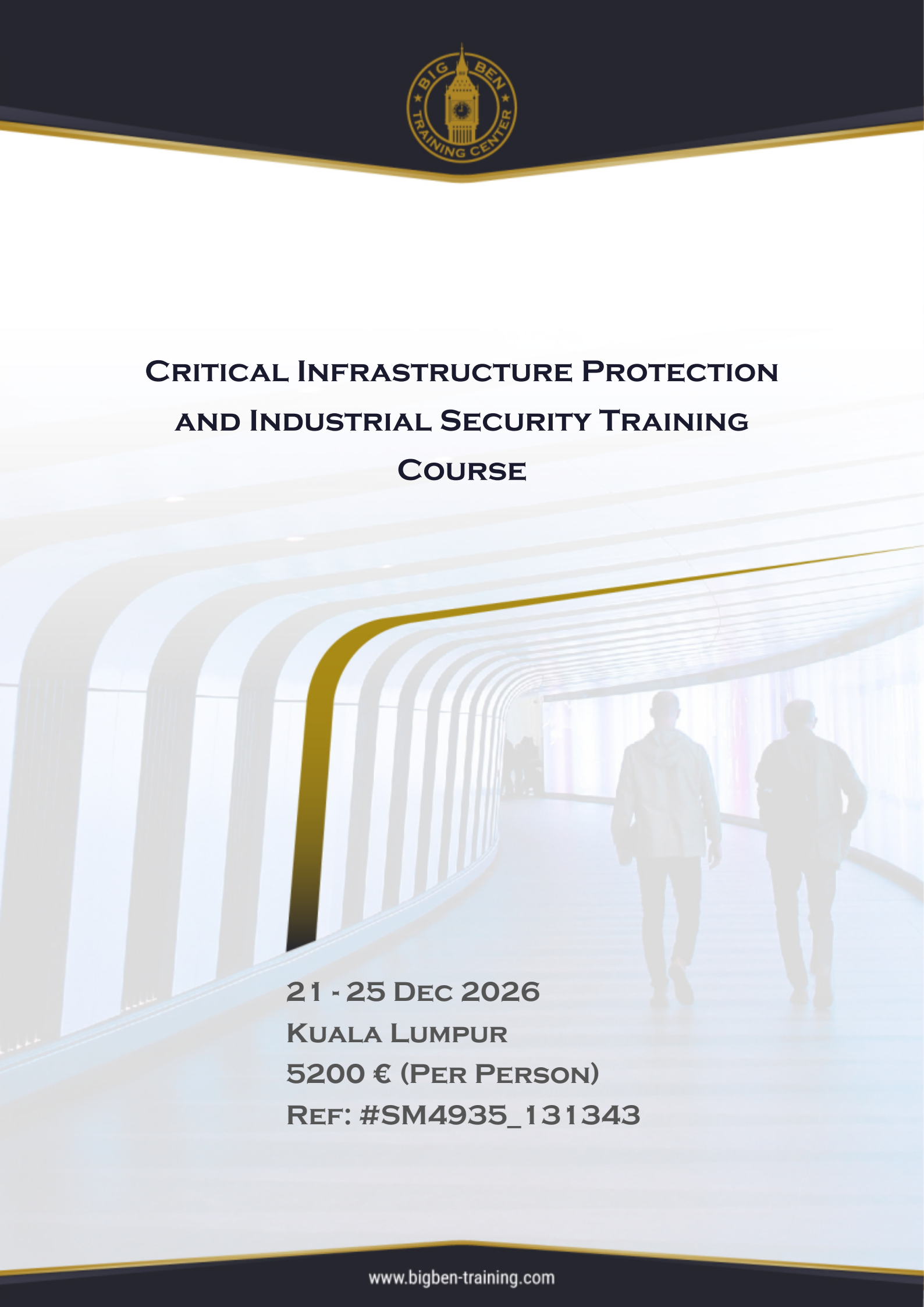
Critical Infrastructure Protection and Industrial Security Training Course



21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM4935_131343

Course Introduction / Overview:

In an era of increasing interconnectivity and sophisticated threats, the protection of national and corporate critical infrastructure is paramount. This course provides a comprehensive framework for understanding and implementing robust industrial security and critical infrastructure protection (CIP) strategies. It delves into the complex interplay between physical security, cybersecurity for operational technology (OT), and organizational resilience. Participants will explore the principles outlined by leading experts like Eric D. Vautrinot, whose work emphasizes a holistic approach to securing cyber-physical systems. The curriculum is designed to move beyond theoretical concepts, drawing from real-world case studies and established frameworks like the NIST Cybersecurity Framework and ISA/IEC 62443. As detailed in texts such as "Critical Infrastructure Protection in an Age of Escalating Threats," the course addresses the entire lifecycle of security management, from risk assessment and vulnerability analysis to incident response and recovery. BIG BEN Training Center has developed this program to equip professionals with the strategic foresight and tactical skills necessary to defend essential services and industrial assets against a dynamic threat landscape, ensuring business continuity and public safety.

Target Audience / This training course is suitable for:

- Security Managers and Directors.
- Industrial Control Systems (ICS) and SCADA Engineers.
- IT and OT Security Professionals.
- Physical Security Specialists.
- Risk and Compliance Analysts.
- Emergency Management Planners.
- Government and Regulatory Officials.
- Facility and Plant Managers.
- Corporate Security Consultants.
- Operations and Maintenance Supervisors.

Target Sectors and Industries:

- Energy and Utilities (Electricity, Oil, and Gas).
- Water and Wastewater Systems.
- Transportation and Logistics.
- Telecommunications and Information Technology.
- Healthcare and Public Health.
- Financial Services and Banking.
- Chemical and Manufacturing Industries.
- Food and Agriculture.
- Government agencies, defense contractors, and public administration bodies.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Information Technology (IT) and Cybersecurity.
- Operational Technology (OT) and Plant Operations.
- Risk Management and Compliance.
- Engineering and Maintenance.
- Health, Safety, and Environment (HSE).
- Facilities Management.
- Emergency Response and Crisis Management.
- Internal Audit and Governance.

Course Offerings:

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

- Develop a comprehensive security strategy that integrates physical, cyber, and personnel controls.
- Conduct thorough risk assessments and vulnerability analyses for critical industrial assets.
- Apply the principles of the ISA/IEC 62443 standard to secure Industrial Control Systems.
- Design and implement effective security for Operational Technology (OT) environments.
- Create a robust incident response and crisis management plan for industrial security events.
- Analyze the convergence of IT and OT and manage the associated security challenges.
- Enhance supply chain security and mitigate third-party risks to critical infrastructure.
- Foster a strong security culture within the organization through training and awareness programs.
- Ensure compliance with national and international regulations for critical infrastructure protection.
- Evaluate and deploy appropriate security technologies for surveillance, access control, and network monitoring.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. This course moves beyond traditional lectures to foster a dynamic learning environment where participants actively engage with the material. The program is built upon a foundation of expert-led instruction, interactive discussions, and collaborative group exercises that encourage peer-to-peer learning and knowledge sharing. A significant portion of the course is dedicated to analyzing real-world case studies of industrial security breaches and successful protection strategies. Participants will work in teams on practical workshops to develop risk assessments, design security architectures, and simulate incident response scenarios. This hands-on approach ensures that theoretical knowledge is immediately translated into practical skills. Continuous feedback from the instructor and a focus on solving complex, realistic problems empower attendees to confidently apply their new competencies to safeguard their organization's critical infrastructure upon returning to the workplace.

Course Agenda (Course Units):

Unit One: Foundations of Critical Infrastructure and Industrial Security

- Defining critical infrastructure and industrial environments.
- The historical evolution of industrial security threats.
- Understanding the threat landscape: state actors, cybercriminals, and insider threats.
- Key differences between IT and Operational Technology (OT) security.
- Introduction to foundational security principles for cyber-physical systems.
- The role of public-private partnerships in national infrastructure protection.
- Legal, regulatory, and ethical considerations in CIP.

Unit Two: Risk Management and Threat Intelligence Frameworks

- Conducting a comprehensive security risk assessment for industrial facilities.
- Methodologies for vulnerability analysis and asset identification.
- Threat modeling for Industrial Control Systems (ICS).
- Utilizing threat intelligence to proactively defend critical assets.
- Implementing the NIST Cybersecurity Framework in an OT environment.
- Dependency analysis and understanding cascading failures.
- Developing a risk mitigation and treatment plan.

Unit Three: Securing Cyber-Physical Systems and Operational Technology

- Fundamentals of SCADA, DCS, and PLC security.
- An in-depth look at the ISA/IEC 62443 standard for IACS security.
- Architecting secure industrial networks and implementing network segmentation.
- Secure configuration and hardening of industrial devices.
- Managing access control in OT environments.
- Implementing monitoring and intrusion detection for industrial networks.
- Strategies for securing the Industrial Internet of Things (IIoT).

Unit Four: Incident Response, Crisis Management, and Physical Security Integration

- Developing an OT-specific incident response plan.
- Digital forensics and evidence handling in industrial environments.
- Business continuity and disaster recovery planning for critical operations.
- Principles of effective crisis management and communication.
- Integrating physical security controls: access control, surveillance, and perimeter defense.
- Personnel security: background checks, training, and insider threat programs.
- Conducting and evaluating security drills and exercises.

Unit Five: Governance, Compliance, and Building a Resilient Security Culture

- Establishing a security governance structure for converged IT/OT environments.
- Managing supply chain and third-party vendor security risks.
- Building a robust security awareness and training program for all employees.
- Measuring security performance with key metrics and KPIs.
- Preparing for and managing security audits and compliance checks.
- Future trends in industrial security: AI, machine learning, and quantum computing.
- Capstone exercise: Developing a holistic CIP strategy for a model facility.

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 convergence accelerates, how can organizations balance the drive for efficiency and data analytics with the fundamental security principle of network segmentation in critical infrastructure environments?

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

This course distinguishes itself by adopting a holistic, multi-disciplinary perspective that transcends conventional security training. Rather than treating cybersecurity, physical security, and personnel management as separate silos, it integrates them into a unified strategic framework for protecting critical infrastructure. The curriculum is meticulously designed to address the nuanced challenges of securing Operational Technology (OT) and Industrial Control Systems (ICS), an area often overlooked by traditional IT-focused programs. We emphasize strategic resilience over a purely defensive posture, equipping participants with the foresight to build systems that can withstand, adapt to, and recover from sophisticated attacks. The course content is grounded in established international standards like ISA/IEC 62443 and the NIST Framework but is delivered through a practical lens, focusing on implementation rather than mere theory. Through complex case studies and simulation exercises, participants do not just learn about security; they learn to think like security strategists, capable of making informed decisions that balance operational needs with robust protection in high-stakes industrial environments. This focus on strategic thinking and integrated security management provides a depth of understanding that is both rare and essential in today's threat landscape.