Advanced Perimeter Security and Intrusion Detection Training Course



26 - 30 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM5835_132151

Course Introduction / Overview:

This comprehensive training course provides an in-depth exploration of the principles and practices of modern perimeter security and intrusion detection systems. In an era of evolving threats, a robust security posture begins at the boundary. This program is meticulously designed to equip participants with the strategic knowledge and technical skills to design, implement, and manage effective, multi-layered security solutions. Drawing upon established frameworks and forward-thinking concepts, the curriculum moves beyond simple product selection to focus on the core principles of threat assessment, vulnerability analysis, and integrated system design. As highlighted by security expert Mary Lynn Garcia in her seminal work, "The Design and Evaluation of Physical Protection Systems," an effective system is one that successfully detects, delays, and responds to threats. BIG BEN Training Center has structured this course to embody that philosophy, ensuring participants can create resilient security architectures. This training covers everything from traditional physical barriers to advanced sensor technologies and the critical integration of cyber-physical security, preparing professionals to protect critical assets against a wide spectrum of potential intrusions.

Target Audience / This training course is suitable for:

- Security Managers and Directors.
- Physical Security Specialists.
- Facility and Operations Managers.
- Security System Designers and Engineers.
- Law Enforcement and Military Personnel.
- IT Professionals involved in security convergence.
- Security Consultants and System Integrators.
- Risk and Compliance Officers.

Target Sectors and Industries:

- Critical Infrastructure including Energy, Water, and Telecommunications.
- Government, Defense, and Homeland Security Agencies.
- Transportation and Logistics including Airports, Seaports, and Railways.
- Banking, Financial Services, and Data Centers.
- Industrial and Manufacturing Facilities.
- Corporate Campuses and Commercial Real Estate.
- Healthcare and Educational Institutions.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Facilities Management and Operations.
- Information Technology and Cybersecurity.
- Risk Management and Compliance.
- Health, Safety, and Environment (HSE).
- Engineering and Project Management.
- Internal Audit and Investigations.

Course Offerings:

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

- Conduct comprehensive security risk and vulnerability assessments for perimeters.
- Apply the principles of layered security (deter, detect, delay, respond) in design.
- Select appropriate physical barriers, including fencing, gates, and lighting.
- Evaluate and deploy various intrusion detection sensor technologies.
- Design and configure effective CCTV and advanced video surveillance systems.
- Integrate access control systems with perimeter security measures.
- Develop robust alarm monitoring and incident response protocols.
- Understand the convergence of physical and cybersecurity threats.
- Manage the lifecycle of a security system from design to maintenance.
- Create security policies and procedures to support technological systems.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can immediately apply the learned concepts in their professional roles. This course moves beyond theoretical lectures by incorporating a dynamic blend of learning techniques. A significant portion of the training is dedicated to analyzing real-world case studies of security breaches and successful protection strategies, allowing participants to understand the practical implications of design choices. Collaborative group exercises and workshops will challenge participants to work in teams to design a perimeter security system for a hypothetical facility, fostering critical thinking and problem-solving skills. Expert-led discussions will provide a platform for sharing experiences and addressing specific challenges faced by attendees in their own organizations. The methodology emphasizes a hands-on approach, with interactive sessions on system integration and threat modeling. Continuous feedback from the instructor ensures a supportive learning environment where complex topics are made accessible and understandable for all participants.

Course Agenda (Course Units):

Unit One: Foundations of Perimeter Security Strategy

- Principles of Physical Protection Systems (PPS).
- Understanding the Adversary and Threat Modeling.
- Conducting Site Surveys and Vulnerability Assessments.
- The Layered Security Approach (Concentric Circles of Protection).
- Crime Prevention Through Environmental Design (CPTED) Principles.
- Legal and Regulatory Compliance in Security Design.
- Developing a Comprehensive Security Master Plan.

Unit Two: Physical Barriers and Access Control

- Types and Applications of Security Fencing and Walls.
- Hostile Vehicle Mitigation (HVM) Solutions.
- Security Lighting Design and Standards.
- Selection and Placement of Gates, Turnstiles, and Bollards.
- Fundamentals of Electronic Access Control Systems.
- Biometric and Multi-Factor Authentication Technologies.
- Key Management and Control Policies.

Unit Three: Intrusion Detection System (IDS) Technologies

- Overview of Sensor Technologies and their Applications.
- Fence-Mounted and Buried Cable Detection Systems.
- Microwave, Infrared, and Photoelectric Beam Sensors.
- Volumetric Sensors for Interior and Exterior Protection.
- Acoustic and Seismic Sensor Applications.
- Understanding and Mitigating False and Nuisance Alarms.
- Emerging Technologies like Drone Detection Systems.

Unit Four: Surveillance, Monitoring, and Response

- Fundamentals of CCTV and Video Surveillance Systems.
- Camera Selection, Placement, and Field of View Design.
- Introduction to Video Analytics and Artificial Intelligence in Surveillance.
- Designing a Security Control Room and Operations Center (SOC).
- Alarm Assessment and Verification Procedures.
- Developing Effective Incident Response and Escalation Protocols.
- Integration with Physical Security Information Management (PSIM) Platforms.

Unit Five: System Integration, Management, and Future Trends

- Designing an Integrated Security System Architecture.
- The Convergence of Physical and Cyber Security (Cyber-Physical Systems).
- Project Management for Security System Implementation.
- System Commissioning, Testing, and Acceptance Procedures.
- Developing a Proactive Maintenance and System Health Program.
- Budgeting for Security Systems and Calculating Return on Investment.
- The Future of Perimeter Security and Emerging Technologies.

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 cyber-physical convergence accelerates, how might the principles of traditional perimeter security need to evolve to counter threats that originate in the digital realm but manifest physically?

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

This course distinguishes itself by adopting a holistic and strategic approach to perimeter security, moving beyond a narrow focus on individual technologies. Unlike programs that may concentrate on vendor-specific products, this training emphasizes vendor-neutral design principles, empowering participants to select the best solutions for their unique threat landscape rather than simply what is new on the market. A key differentiator is the significant focus on the convergence of physical and cybersecurity. We explore how digital vulnerabilities can compromise physical barriers and detection systems, a critical and often overlooked aspect of modern security design. The curriculum is built on a foundation of risk assessment and threat modeling, ensuring that every design decision is justifiable and evidence-based. Furthermore, the course content is not just theoretical; it is deeply rooted in practical application, with case studies and design exercises that mirror real-world challenges. This strategic, integrated, and practical methodology ensures participants leave not just with knowledge of security components, but with the mastery to architect comprehensive, resilient, and future-proof protection systems.