Strategic Security for Oil and Gas Asset Protection Training Course



21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM1167_132099

Course Introduction / Overview:

The global energy sector operates within an increasingly complex and volatile environment, where the security of oil and gas assets is paramount to national stability and economic prosperity. This course provides a comprehensive framework for understanding and managing the multifaceted threats facing critical energy infrastructure. Drawing on principles outlined by security experts like Daniel Yergin in his seminal work, "The Prize: The Epic Quest for Oil, Money, and Power," we explore the intersection of geopolitical risk, technological vulnerabilities, and operational security. Participants will delve into proactive strategies for asset protection, moving beyond reactive measures to build resilient security architectures. This program, offered by BIG BEN Training Center, is meticulously designed to equip professionals with the advanced skills needed to conduct thorough risk assessments, implement integrated security solutions, and lead effective crisis response operations. It addresses both physical and cyber threats, ensuring a holistic understanding of the contemporary security landscape for oil and gas operations from exploration to distribution.

Target Audience / This training course is suitable for:

- Security Managers and Directors.
- Asset Protection Specialists.
- Operations Managers and Supervisors.
- Risk Management Professionals.
- HSE (Health, Safety, and Environment) Officers.
- Corporate Security Team Leaders.
- Facility and Plant Managers.
- Government Officials and Regulators in the energy sector.
- Intelligence and Security Analysts.
- Emergency Response and Crisis Management Personnel.

Target Sectors and Industries:

- Upstream Oil and Gas (Exploration and Production).
- Midstream Oil and Gas (Transportation and Storage).
- Downstream Oil and Gas (Refining and Marketing).
- Petrochemical and Chemical Manufacturing.
- Liquefied Natural Gas (LNG) and Gas Processing.
- Maritime, Shipping, and Port Operations.
- Energy Utilities and Power Generation.
- Government agencies, regulatory bodies, and national security organizations.
- Engineering, Procurement, and Construction (EPC) companies.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Operations and Production.
- Health, Safety, and Environment (HSE).
- Risk Management and Compliance.
- Information Technology (IT) and Cybersecurity.
- Logistics and Supply Chain Management.
- Facilities Management.
- Crisis Management and Business Continuity.
- Government and Public Relations.
- Legal and Regulatory Affairs.

Course Offerings:

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

- Conduct comprehensive security risk assessments for diverse oil and gas assets.
- Develop and implement integrated physical security plans for critical infrastructure.
- Analyze and mitigate cybersecurity threats targeting Industrial Control Systems (ICS) and SCADA.
- Design robust crisis management and emergency response protocols.
- Evaluate and counter threats from terrorism, sabotage, and organized crime.
- Apply intelligence gathering and analysis techniques to predict and prevent security incidents.
- Ensure compliance with international security standards and regulations like ISPS Code.
- Strengthen supply chain security from source to destination.
- Manage security for both onshore and offshore facilities effectively.
- Lead security teams with strategic foresight and operational excellence.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster an immersive and practical learning experience. This course moves beyond traditional lectures to engage participants through a dynamic blend of interactive techniques. Central to our approach are real-world case studies of major security incidents in the oil and gas industry, allowing for in-depth analysis of successes and failures in a controlled environment. Participants will work in collaborative teams on simulation exercises that challenge them to develop and execute security plans, respond to evolving crisis scenarios, and make critical decisions under pressure. Expert-led discussions, interactive workshops, and peer-to-peer knowledge sharing sessions ensure that theoretical concepts are firmly grounded in practical application. We emphasize a hands-on approach, where participants receive continuous feedback to refine their strategic thinking and operational skills, ensuring they leave with tangible capabilities ready to be deploy
d in their respective roles.

Course Agenda (Course Units):

Unit One: The Global Energy Security Landscape

- Understanding the Geopolitics of Oil and Gas.
- Identifying the Spectrum of Threats: State and Non-State Actors.
- Key Vulnerabilities in Upstream, Midstream, and Downstream Operations.
- Introduction to Security Risk Management Frameworks (ISO 31000).
- Legal and Regulatory Compliance in the Energy Sector.
- Historical Case Studies of Major Security Incidents.
- The Role of Intelligence in Proactive Security.

Unit Two: Physical Security and Asset Hardening

- Principles of Critical Infrastructure Protection (CIP).
- Designing Layered Security Systems for Onshore Facilities.
- Perimeter Security, Access Control, and Intrusion Detection Systems.
- Advanced Surveillance and Monitoring Technologies (CCTV, Drones, Radar).
- Maritime and Offshore Platform Security (ISPS Code).
- Pipeline and Transportation Network Security.
- Executive Protection and Personnel Security Protocols.

Unit Three: Cybersecurity for Industrial Control Systems

- Introduction to Operational Technology (OT) and ICS/SCADA Security.
- Common Cyber Threats and Attack Vectors in the Energy Sector.
- The Convergence of IT and OT Security.
- Implementing the Purdue Model for Network Segmentation.
- Developing a Robust Cybersecurity Incident Response Plan.
- Threat Hunting and Anomaly Detection in OT Environments.
- Protecting Against Ransomware and Data Breaches.

Unit Four: Crisis Management and Emergency Response

- Fundamentals of Crisis Management and Command Structures.
- Developing and Testing Emergency Response Plans (ERPs).
- Incident Command System (ICS) for the Oil and Gas Industry.
- Managing Media and Communications During a Crisis.
- Business Continuity and Disaster Recovery Planning.
- Responding to Sabotage, Terrorism, and Active Assailant Scenarios.
- Post-Incident Investigation and Lessons Learned.

Unit Five: Advanced Security Operations and Future Trends

- Integrating Intelligence into the Security Planning Cycle.
- Managing Insider Threats and Corporate Espionage.
- Security Considerations for New Energy Technologies.
- The Impact of Digitalization and AI on Security Operations.
- Building a Resilient Security Culture Across the Organization.
- Conducting Security Audits and Drills.
- Strategic Security Leadership and Stakeholder Management.

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:

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

As digital transformation accelerates the convergence of physical and operational technology domains, how must traditional security leadership evolve to effectively manage hybrid threats against national energy infrastructure?

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

This course distinguishes itself by adopting a truly integrated and strategic perspective on oil and gas security, a quality often missing from programs that focus on singular threats. We move beyond siloed training in either physical or cybersecurity to address the complex interplay between them, preparing leaders for the reality of modern, hybrid threats. The curriculum is built on a foundation of strategic risk management, emphasizing proactive intelligence-led prevention rather than purely reactive defense. Unlike other courses that may rely on outdated examples, our content is dynamically updated with contemporary case studies reflecting the latest geopolitical shifts, technological vulnerabilities, and adversary tactics. Furthermore, the program places a significant emphasis on leadership and decision-making under pressure through realistic, high-fidelity simulations. Participants do not just learn about security protocols; they practice applying them in crisis scenarios, honing the critical thinking and communication skills necessary to protect high-value national assets effectively.