AMERICAN GLOBAL INSTITUTE FOR PRIVATE TRAINING

External Training Course

NextGen AI-Powered Cybersecurity for Oil & Gas

From 27 Oct. To 31 Oct. 2025
From 17 Nov. To 21 Nov. 2025
From 22 Dec. To 26 Dec. 2025

Mercure Paris Notre Dame Saint Germain des Prés Hotel, Paris, France

Mr. Ghanem F. Al-Otaibi
GM & Institute Owner
Tel.: 00965 22248901 **Fax: 00965 22204999**
Mob.: 00965 65548855 **Mob.: 00965 97273712**
Email: admin@agi-kw.com **Email: agi-kw@hotmail.com**
W/SITE: WWW.AGI-KW.COM

American Global
Institute For Private Training

Tel. 00965 - 22248901
Mob. 00965 - 65548855
Email admin@agi-kw.com
W/Site www.agi-kw.com

External Training Course:

NextGen AI-Powered Cybersecurity for Oil & Gas

From 27 Oct. To 31 Oct. 2025 **Fees: 2250 KD**
From 17 Nov. To 21 Nov. 2025 **Fees: 2250 KD**
From 22 Dec. To 26 Dec. 2025 **Fees: 2250 KD**

Course Overview

The oil & gas sector is one of the world's most critical and high-value industries, making it a prime target for cyber-attacks. With the increasing adoption of digitalization, IoT, and smart operational technologies, traditional cybersecurity is no longer sufficient. This comprehensive 5-day training equips participants with advanced skills to harness Artificial Intelligence (AI) for cybersecurity defense. The course blends practical techniques, case studies, and strategic frameworks to ensure energy companies remain resilient in the face of evolving cyber threats.

Course Objectives

By the end of this program, participants will be able to:

- Understand the unique cybersecurity challenges within the oil & gas sector.
- Apply AI-driven solutions to detect, prevent, and respond to cyber threats.
- Enhance the protection of SCADA, IoT, and industrial control systems.
- Build cyber resilience frameworks aligned with international best practices.
- Implement predictive analytics for threat anticipation and prevention.
- Develop strategies to secure digital transformation projects.
- Lead organizational preparedness in handling cyber incidents.
- Design future-proof cybersecurity roadmaps for oil & gas operations.

Training Methodology

Instructor-led lectures with global industry experts.
Case studies from real-world oil & gas cyber incidents.
Hands-on labs with AI-based cybersecurity tools.
Workshops & group discussions for collaborative learning.
Simulated attack-defense scenarios for practical readiness.
Strategic planning exercises for organizational application.

Organizational Impact

Stronger defense of mission-critical oil & gas digital assets.
Reduced downtime and financial losses from cyber-attacks.
AI-enabled continuous monitoring and rapid incident response.
Enhanced compliance with international cybersecurity standards (ISO/IEC 27001, NIST, API).
Increased trust from partners, regulators, and stakeholders.
Improved readiness for future cyber challenges and digital transformation.

Personal Impact

Advanced knowledge of AI-driven cyber defense techniques.
Improved ability to detect, analyze, and respond to threats in real time.
Hands-on skills with AI-based cybersecurity platforms.
Expertise in OT/ICS protection within the oil & gas environment.
Stronger leadership capabilities in managing cyber risk.
Competitive advantage in the digital oil & gas workforce.

Course Content & Outlines

Day 1: Cybersecurity Landscape in Oil & Gas

- Cyber threat landscape and trends in the energy sector.
- Key vulnerabilities in upstream, midstream, and downstream operations.
- Role of AI in transforming cybersecurity defense.
- Lessons from major global cyber-attacks (e.g., Colonial Pipeline, Aramco incidents).
- Mapping cyber risks to oil & gas business impact.

Day 2: AI-Driven Cyber Defense Technologies

- Machine learning for intrusion detection and anomaly detection.
- Predictive analytics for identifying emerging threats.
- Natural Language Processing (NLP) in threat intelligence analysis.
- Autonomous response systems and AI-powered firewalls.
- Case demonstration: AI vs. traditional cybersecurity models.

Day 3: Securing Critical Oil & Gas Infrastructure

- Protecting SCADA, IoT, and Industrial Control Systems (ICS).
- AI-enabled monitoring for pipelines, refineries, and offshore rigs.
- Zero-trust architecture for energy companies.
- Vulnerability management and continuous risk assessment.
- Cyber-physical security integration.

Day 4: Incident Response and Recovery with AI

- AI-enhanced Security Information & Event Management (SIEM).
- Real-time threat detection, triage, and automated alerts.
- Crisis management frameworks in oil & gas.
- Building digital forensics capabilities with AI tools.
- Designing business continuity and disaster recovery plans.

Day 5: Strategy, Governance, and Future Trends

- Developing enterprise-wide AI-powered cybersecurity frameworks.
- Regulatory requirements and compliance (NIST, ISO, API, GDPR, local laws).
- Ethical considerations of AI in cybersecurity.
- Future of AI in cyber defense: quantum computing, deep learning, autonomous systems.
- Capstone Workshop: Designing a Cybersecurity Roadmap for Oil & Gas.

Course Agenda:

(1st Day) Agenda

8.30	9.00	Opening Remarks (30 Min.).
9.00	11.30	Discuss the main points of the training course: • Cybersecurity Landscape in Oil & Gas. • AI-Driven Cyber Defense Technologies. • Securing Critical Oil & Gas Infrastructure. • Incident Response and Recovery with AI. • Strategy, Governance, and Future Trends.
11.30	12.00	Coffee Break
12.00	14.00	Cybersecurity Landscape in Oil & Gas: • Cyber threat landscape and trends in the energy sector. • Key vulnerabilities in upstream, midstream, and downstream operations. • Role of AI in transforming cybersecurity defense. • Lessons from major global cyber-attacks (e.g., Colonial Pipeline, Aramco incidents). • Mapping cyber risks to oil & gas business impact.
14.00	14.30	Questions and Discussion
14.30		Buffet Lunch

(2nd Day) Agenda

9.00	11.30	AI-Driven Cyber Defense Technologies: • Machine learning for intrusion detection and anomaly detection. • Predictive analytics for identifying emerging threats. • Natural Language Processing (NLP) in threat intelligence analysis.
11.30	12.00	Coffee Break
12.00	14.00	AI-Driven Cyber Defense Technologies: • Autonomous response systems and AI-powered firewalls. • Case demonstration: AI vs. traditional cybersecurity models.
14.00	14.30	Questions and Discussion
14.30		Buffet Lunch

(3rd Day) Agenda

9.00	11.30	Securing Critical Oil & Gas Infrastructure: • Protecting SCADA, IoT, and Industrial Control Systems (ICS). • AI-enabled monitoring for pipelines, refineries, and offshore rigs. • Zero-trust architecture for energy companies.
11.30	12.00	Coffee Break
12.00	14.00	Securing Critical Oil & Gas Infrastructure: • Vulnerability management and continuous risk assessment. • Cyber-physical security integration.
14.00	14.30	Questions and Discussion
14.30		Buffet Lunch

(4th Day) Agenda

9.00	11.30	Incident Response and Recovery with AI: • AI-enhanced Security Information & Event Management (SIEM). • Real-time threat detection, triage, and automated alerts. • Crisis management frameworks in oil & gas.
11.30	12.00	Coffee Break
12.00	14.00	Incident Response and Recovery with AI: • Building digital forensics capabilities with AI tools. • Designing business continuity and disaster recovery plans.
14.00	14.30	Questions and Discussion
14.30		Buffet Lunch

(5th Day) Agenda

9.00	11.30	Strategy, Governance, and Future Trends: • Developing enterprise-wide AI-powered cybersecurity frameworks. • Regulatory requirements and compliance (NIST, ISO, API, GDPR, local laws). • Ethical considerations of AI in cybersecurity.
11.30	12.00	Coffee Break
12.00	14.00	Strategy, Governance, and Future Trends: • Future of AI in cyber defense: quantum computing, deep learning, autonomous systems. • Capstone Workshop: Designing a Cybersecurity Roadmap for Oil & Gas.
14.00	14.30	Questions, Discussion & Conclusion Training Course.
14.30		Buffet Lunch