Training Course on Cybersecurity in Oil and Gas Industrial Control Systems (ICS)

Professional Development Training Course Outline

Category	Oil and Gas	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s evolving threat landscape, cybersecurity in Industrial Control Systems (ICS) has become critical, especially in the oil and gas sector, where operational disruptions can lead to catastrophic financial, environmental, and safety consequences. As digital transformation, IIoT integration, and remote operations expand, protecting vital infrastructure against cyberattacks, malware, ransomware, and insider threats is not just a necessity it's a top strategic priority.

Training Course on Cybersecurity in Oil & Gas Industrial Control Systems (ICS) is specifically designed to provide comprehensive, actionable, and industry-aligned cybersecurity training for professionals operating within or servicing ICS/SCADA environments in oil and gas. Through real-world case studies, current threat analysis, and hands-on practical applications, this program bridges the gap between IT and OT security, enabling participants to implement resilient cybersecurity frameworks and ensure the integrity of mission-critical systems.

Programme Curriculum

Training Course on Cybersecurity in Oil & Gas Industrial Control Systems (ICS)

Introduction

In today’s evolving threat landscape, cybersecurity in Industrial Control Systems (ICS) has become critical, especially in the oil and gas sector, where operational disruptions can lead to catastrophic financial, environmental, and safety consequences. As digital transformation, IIoT integration, and remote operations expand, protecting vital infrastructure against cyberattacks, malware, ransomware, and insider threats is not just a necessity it's a top strategic priority.

Training Course on Cybersecurity in Oil & Gas Industrial Control Systems (ICS) is specifically designed to provide comprehensive, actionable, and industry-aligned cybersecurity training for professionals operating within or servicing ICS/SCADA environments in oil and gas. Through real-world case studies, current threat analysis, and hands-on practical applications, this program bridges the gap between IT and OT security, enabling participants to implement resilient cybersecurity frameworks and ensure the integrity of mission-critical systems.

Course Objectives

1. Understand ICS/SCADA architectures and how cyber threats target them.
2. Analyze real-world cyberattacks on oil & gas ICS environments.
3. Apply cybersecurity frameworks (NIST, IEC 62443) for ICS resilience.
4. Implement risk-based security strategies to protect operational assets.
5. Detect and mitigate ransomware threats in critical infrastructure.
6. Integrate IT-OT convergence strategies for cyber-secure operations.
7. Employ network segmentation and zero trust in ICS networks.
8. Utilize intrusion detection systems specific to ICS traffic.
9. Conduct cyber threat hunting and incident response planning.
10. Secure IIoT and legacy systems in oil & gas environments.
11. Strengthen supply chain and third-party cybersecurity controls.
12. Prepare ICS environments for compliance with global regulations.
13. Develop and test disaster recovery and business continuity plans.

Target Audience

1. ICS Engineers and Technicians
2. OT Security Specialists
3. IT Security Professionals in Energy
4. SCADA System Administrators
5. Oil & Gas Operations Managers
6. Cybersecurity Consultants
7. Compliance & Risk Management Officers
8. Government & Regulatory Professionals in Energy

Course Duration: 10 days

Course Modules

Module 1: Introduction to ICS in Oil & Gas

- Overview of ICS architecture
- Components: PLCs, RTUs, HMIs
- Differences between IT and OT
- Common ICS vulnerabilities
- Threat landscape for oil & gas
- **Case Study:** Ukraine power grid attack

Module 2: Cyber Threats in ICS Environments

- Malware, ransomware, and APTs
- Insider threats in OT
- Cyber-physical attack examples
- Threat vectors in ICS
- Cybersecurity incidents in O&G
- **Case Study:** Triton malware incident

Module 3: ICS Network Architecture & Segmentation

- ICS network zones and conduits
- Purdue model for ICS
- DMZ implementation
- Secure remote access
- Role of firewalls and VPNs
- **Case Study:** Colonial Pipeline breach

Module 4: Security Standards & Compliance

- NIST 800-82 and IEC 62443
- ISO/IEC 27001 relevance
- Government mandates and audits
- Aligning ICS with compliance
- Role of industry regulations
- **Case Study:** Cybersecurity audit in refineries

Module 5: ICS Risk Assessment & Management

- Risk identification process
- Impact analysis in ICS
- Vulnerability scanning tools
- Risk treatment strategies
- Security posture assessment
- **Case Study:** LNG terminal risk matrix

Module 6: IT/OT Convergence & Security Integration

- Bridging IT and OT securely
- Challenges in convergence
- Secure data transfer protocols
- Unified threat management
- Industrial data protection
- **Case Study:** Offshore rig digitalization

Module 7: Threat Detection and Monitoring

- ICS-specific IDS/IPS systems
- Anomaly-based monitoring
- Log management and SIEM tools
- Endpoint detection for OT
- Integrating real-time alerts
- **Case Study:** Pipeline SCADA detection

Module 8: Ransomware in ICS & Mitigation Strategies

- Common ransomware strains
- ICS-specific ransomware behavior
- Prevention through segmentation
- Backup and recovery tactics
- Business impact analysis
- **Case Study:** Norsk Hydro ransomware

Module 9: Incident Response & Disaster Recovery

- IR plan development for ICS

- Roles and responsibilities
- Containment and eradication
- Communication protocols
- Post-incident evaluation
- **Case Study:** Refined oil cyberattack IR plan

Module 10: Secure ICS Design and Architecture

- Designing secure control systems
- Hardware and firmware protection
- System hardening techniques
- Secure coding for ICS
- Physical security in OT
- **Case Study:** Refinery ICS redesign

Module 11: ICS Forensics & Post-Attack Analysis

- Basics of OT forensics
- Capturing volatile data
- Chain of custody in ICS
- Event reconstruction
- Reporting and documentation
- **Case Study:** Gas plant forensics operation

Module 12: IIoT Security in Oil & Gas

- IIoT architecture overview
- IIoT device vulnerabilities
- Encryption and device management
- Secure protocols (MQTT, CoAP)
- Edge computing security
- **Case Study:** IoT attack on oil sensors

Module 13: Cloud & Remote Access Security

- Securing remote OT access
- ICS cloud security challenges
- Authentication & identity access
- Zero trust network access
- Multi-factor authentication (MFA)
- **Case Study:** Remote access misconfiguration

Module 14: Supply Chain & Third-Party Risks

- Vendor risk management
- Third-party access policies
- Software and firmware supply chain
- Contractual obligations
- Security assessments and audits
- **Case Study:** Supplier breach in SCADA system

Module 15: Business Continuity & Cyber Resilience

- BCP for ICS operations
- Redundancy and failover plans
- Cyber insurance strategies

- Testing and exercises
- Long-term resilience planning
- **Case Study:** Offshore platform continuity test

Training Methodology

- Interactive instructor-led presentations
- Real-life scenario walkthroughs
- Hands-on labs and simulations
- Group discussions and brainstorming
- Pre- and post-training assessments
- Individual and team-based problem-solving exercises

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com