Cybersecurity in Mining Systems Training Course

Professional Development Training Course Outline

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

Course Introduction

The Cybersecurity in Mining Systems Training Course is a specialized, industry-focused program designed to equip professionals with cutting-edge skills to defend modern mining operations against evolving cyber threats. As mining becomes increasingly digitized through Industrial IoT (IIoT), SCADA systems, autonomous haulage fleets, remote operations centers, and smart sensors, the attack surface has expanded dramatically. Cybersecurity in Mining Systems Training Course provides deep insight into securing critical mining infrastructure against ransomware, insider threats, Advanced Persistent Threats (APTs), and operational technology (OT) sabotage.

With global mining enterprises adopting Industry 4.0, digital twin technology, cloud-based mine management systems, and AI-driven exploration tools, cybersecurity has become a mission-critical requirement rather than an optional layer. Participants will gain hands-on expertise in OT cybersecurity, SCADA protection, network segmentation, zero trust architecture, threat intelligence, incident response, and regulatory compliance tailored specifically for mining environments. The course bridges the gap between IT security and industrial control systems, ensuring operational continuity, safety, and resilience in high-risk mining operations.

Programme Curriculum

Cybersecurity in Mining Systems Training Course

Introduction

The Cybersecurity in Mining Systems Training Course is a specialized, industry-focused program designed to equip professionals with cutting-edge skills to defend modern mining operations against evolving cyber threats. As mining becomes increasingly digitized through Industrial IoT (IIoT), SCADA systems, autonomous haulage fleets, remote operations centers, and smart sensors, the attack surface has expanded dramatically. Cybersecurity in Mining Systems Training Course provides deep insight into securing critical mining

infrastructure against ransomware, insider threats, Advanced Persistent Threats (APTs), and operational technology (OT) sabotage.

With global mining enterprises adopting Industry 4.0, digital twin technology, cloud-based mine management systems, and AI-driven exploration tools, cybersecurity has become a mission-critical requirement rather than an optional layer. Participants will gain hands-on expertise in OT cybersecurity, SCADA protection, network segmentation, zero trust architecture, threat intelligence, incident response, and regulatory compliance tailored specifically for mining environments. The course bridges the gap between IT security and industrial control systems, ensuring operational continuity, safety, and resilience in high-risk mining operations.

Course Duration

10 Days

Course Objectives

1. Master OT Cybersecurity Frameworks for Mining Systems
2. Implement SCADA Security Hardening Techniques
3. Understand Industrial IoT (IIoT) Risk Management
4. Deploy Zero Trust Architecture in Mining Networks
5. Detect and Mitigate Ransomware in Mining Operations
6. Build Threat Intelligence Systems for Mining Assets
7. Strengthen ICS/SCADA Network Segmentation Strategies
8. Apply IEC 62443 Industrial Security Standards
9. Manage Cyber Risk in Autonomous Mining Equipment
10. Develop Incident Response Plans for OT Environments
11. Secure Remote Operations Centers (ROC)
12. Conduct Vulnerability Assessments in Mining Infrastructure
13. Ensure Compliance with Mining Cybersecurity Regulations

Target Audience

1. Mining Engineers and Operations Managers
2. OT/SCADA System Engineers
3. Cybersecurity Analysts in Industrial Sectors
4. IT Infrastructure Managers in Mining Companies
5. Control Systems Technicians
6. Risk & Compliance Officers (Mining Sector)
7. Government Mining Regulators & Inspectors
8. Industrial Automation & PLC Programmers

Course Modules

Module 1: Introduction to Mining Cybersecurity

- Evolution of digital mining ecosystems
- IT vs OT convergence risks
- Threat landscape in mining sector
- Real-world mining cyberattack overview
- **Case Study:** WannaCry impact on global industrial systems

Module 2: SCADA Systems Security

- SCADA architecture in mining
- Protocol vulnerabilities (Modbus, DNP3)
- Access control mechanisms
- Monitoring SCADA traffic anomalies
- **Case Study:** Ukraine power grid attack lessons

Module 3: Industrial IoT (IIoT) Security

- Sensor network risks in mines
- IoT device authentication
- Firmware exploitation risks
- Secure communication protocols
- **Case Study:** Smart factory IoT breach scenario

Module 4: Network Segmentation in Mining

- OT/IT separation strategies
- VLAN and micro-segmentation
- Firewalls for industrial networks
- Lateral movement prevention
- **Case Study:** Norsk Hydro ransomware containment

Module 5: Zero Trust Architecture

- Identity-centric security model
- Continuous verification methods
- Least privilege enforcement
- Device trust validation
- **Case Study:** Colonial Pipeline cyber disruption

Module 6: Ransomware Defense in Mining

- Attack vectors in mining systems
- Backup and recovery strategies
- Endpoint protection in OT
- Incident isolation methods
- **Case Study:** Global NotPetya industrial impact

Module 7: Threat Intelligence for Mining

- Mining-specific threat feeds
- Dark web monitoring
- Indicators of Compromise (IoCs)
- Predictive threat modeling
- **Case Study:** APT attacks on energy/mining sector

Module 8: ICS Protocol Security

- Vulnerabilities in industrial protocols
- Encryption challenges in OT
- Secure protocol alternatives
- Packet inspection techniques

- **Case Study:** Stuxnet ICS manipulation

Module 9: Autonomous Mining Equipment Security

- Autonomous haulage risks
- GPS spoofing threats
- Remote control hijacking
- Sensor integrity validation
- **Case Study:** Self-driving industrial vehicle exploit

Module 10: Incident Response in OT Environments

- OT-specific IR planning
- Isolation vs shutdown decisions
- Forensic data collection
- Recovery workflows
- **Case Study:** Mining plant cyber downtime response

Module 11: Cloud Security in Mining Operations

- Cloud-based mine analytics risks
- API security issues
- Data leakage prevention
- Hybrid cloud OT integration
- **Case Study:** Cloud misconfiguration breach

Module 12: Cyber Risk Management

- Risk assessment frameworks
- Asset criticality mapping
- Business impact analysis
- Cyber insurance in mining
- **Case Study:** Major mining company outage analysis

Module 13: Regulatory & Compliance Standards

- IEC 62443 framework
- ISO 27001 alignment
- Mining safety + cyber overlap
- Audit readiness strategies
- **Case Study:** Regulatory penalty due to breach

Module 14: Digital Twin Security

- Mining simulation environments
- Data integrity risks
- Model manipulation threats
- Secure twin architecture
- **Case Study:** Digital twin sabotage scenario

Module 15: Advanced Persistent Threats (APT) Defense

- APT lifecycle in industrial attacks

- Nation-state targeting mining assets
- Long-term infiltration detection
- Behavioral analytics defense
- **Case Study:** Critical infrastructure espionage campaign

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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
23 Nov 2026	04 Dec 2026	Online	$2,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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