

Autonomous Mining OT Cyber Defence and Response Training Course

26 – 30 September 2027
Nairobi

AGILE LEADERS
Training Center

Autonomous Mining OT Cyber Defence and Response Training Course

Ref: 2147_257260 **Date:** 26 – 30 September 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Autonomous Mining OT Cyber Defence and Response Training Course is a one-week advanced course for mine technology, control-system, autonomous fleet, safety, and incident-response teams, who leave with an Autonomous Mining OT Defense and Response Plan. Participants integrate autonomous mining OT security, industrial network segmentation, secure remote operations, cyber-safety coordination, and OT incident recovery across connected mines. Agile Leaders Training Center presents autonomous mining cyber defense.

Who Should Attend

- Personnel responsible for mining OT and industrial cybersecurity
- Teams responsible for autonomous haulage, fleet management, and machine control
- Operators responsible for remote operations centers and site communications
- Personnel responsible for functional safety, system safety, and operational risk
- Responders responsible for detection, containment, recovery, and continuity

The course assumes participants can interpret industrial architectures and mining operations, and it leaves equipment programming, penetration testing, and product-specific maintenance outside its scope.

Departments and Industries

The course supports departments and sectors operating connected, automated, and safety-critical mining technology.

- Surface and underground mining operations
- Autonomous haulage and mobile equipment teams
- Operational technology and industrial control functions
- Remote operations and mine communications centers
- Engineering, maintenance, safety, and emergency management

Learning Objectives

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

- Analyze autonomous mining assets, data flows, dependencies, and attack paths.
- Build zones, conduits, remote-access, and identity controls.
- Evaluate cyber threats alongside operational and safety consequences.
- Design monitoring, detection, and response decision processes.
- Prioritize containment, recovery, and operational continuity actions.
- Build an Autonomous Mining OT Defense and Response Plan.

Course Agenda

Day 1: Map Autonomous Mining OT

- Autonomous Mining System and OT Asset Inventory
- Haulage, Fleet, Dispatch, and Machine-Control Data-Flow Map
- Remote Operations, Wireless, and Positioning Dependency Model
- Safety-Critical Function and Cyber Consequence Matrix
- Mining OT Threat Scenario and Attack-Path Register

Day 2: Engineer Layered OT Defense

- Industrial Zone and Conduit Segmentation Architecture
- OT Firewall, DMZ, and Jump-Server Access Pattern
- Vendor and Remote Maintenance Access Control Matrix
- Identity, Privilege, and Session Accountability Model
- Secure Configuration and Change-Control Baseline

Day 3: Protect Autonomous Operations

- Autonomous Haulage Command Integrity Control Set
- Fleet Management and Dispatch Resilience Assessment
- Wireless Communications and Positioning Assurance Checklist
- Cybersecurity and System Safety Coordination Framework
- Software, Firmware, and Upgrade Impact Review Gate

Day 4: Detect, Respond, and Recover

- Mining OT Network Visibility and Detection Use Cases
- Cyber-Physical Alert Triage and Severity Matrix
- Safety-Aware Containment and Isolation Decision Tree
- OT Incident Communication and Evidence Protocol
- Backup, Restoration, and Controlled Restart Framework

Day 5: Practice Mining Cyber Defense

- Suggested Exercise: Trace an Autonomous Haulage Attack Path
- Suggested Exercise: Review a Remote Vendor Session
- Suggested Exercise: Triage a Cyber-Safety Event
- Suggested Exercise: Plan a Controlled OT Recovery
- Capstone Exercise: Complete an Autonomous Mining OT Defense and Response Plan

Practical Exercises

The course uses suggested activities based on autonomous haulage, remote operations, industrial wireless links, and control-system disruption.

- Suggested activity: map assets, trust boundaries, data flows, safety functions, remote dependencies, and attack paths.
- Suggested activity: assess segmentation, access, configuration, monitoring, and change evidence against operational constraints.
- Suggested activity: coordinate cybersecurity, operations, engineering, maintenance, and safety decisions during an event.
- Suggested activity: sequence containment, backup restoration, validation, restart, and post-incident improvement actions.

FAQs

Who suits autonomous mining OT cyber defense training, and what does it assume?

Autonomous mining OT cyber defense training suits mine technology, OT security, fleet engineering, remote operations, safety, and incident-response personnel. It assumes familiarity with industrial architectures and mining operations.

How does autonomous mining OT security differ from general SCADA security training?

Autonomous mining OT security adds mobile equipment, fleet dispatch, machine control, wireless and positioning dependencies, remote operations, dynamic safety consequences, and coordinated recovery across dispersed mine sites.

Why must cyber defense and system safety be coordinated in autonomous mining?

Cyber defense and system safety must be coordinated because a security action can change machine behavior, communications, separation controls, production, or safe-state decisions. Shared consequence assessment supports proportionate containment and recovery.

AGILE LEADERS
Training Center

What should secure remote access protect in mining OT?

Secure remote access should protect identities, privileges, approved destinations, session paths, authentication, activity records, time limits, vendor accountability, and emergency revocation while preserving operational availability.

How should an autonomous mine recover from an OT cyber incident?

Recovery should prioritize personnel and environmental safety, verify containment, restore trusted configurations and data, test dependencies, approve controlled restart criteria, monitor performance, and record lessons for future resilience.

Conclusion

Participants take back an Autonomous Mining OT Defense and Response Plan. It combines asset visibility, segmentation, remote access, autonomous-system protection, monitoring, cyber-safety decisions, incident response, restoration, and controlled restart. The plan changes disconnected technical controls into an operational defense system aligned with mine safety, production continuity, and recovery responsibilities.