



Intelligent Transportation Cyber Monitoring and Response Training Course

30 May – 3 June 2027
Nairobi

Intelligent Transportation Cyber Monitoring and Response Training Course

Ref: 767_158369 **Date:** 30 May – 3 June 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Intelligent Transportation Cyber Monitoring and Response Training Course is a five-day intermediate course for transport operators, traffic management center teams, cybersecurity analysts, incident responders, and mobility engineers who leave with an ITS Cyber Monitoring and Response Playbook. Participants connect transport OT monitoring, security event triage, detection logic, escalation, coordinated response, evidence handover, and service continuity across control centers, roadside systems, tolling, traveler information, and vehicle-to-infrastructure services. Agile Leaders Training Center develops intelligent transportation cyber response practice.

Who Should Attend

- Transport operations functions responsible for safe and continuous mobility services
- Traffic management functions responsible for connected signals and roadside systems
- Cybersecurity monitoring functions responsible for transport IT and OT alerts
- Incident response functions responsible for containment, coordination, and recovery
- Infrastructure engineering functions responsible for connected mobility platforms

The course assumes participants can interpret operational alarms and follow authorized escalation procedures, and leaves out vehicle product engineering, penetration testing, malware reverse engineering, and generic enterprise SOC certification.

Departments and Industries

The course supports departments and industries operating connected transportation and mobility services.

- Road authorities and traffic management centers
- Public transport and rail operations
- Tolling, parking, and traveler-information services
- Mobility platform and roadside equipment providers
- Emergency coordination and infrastructure maintenance

Learning Objectives

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



- Apply an ITS asset and telemetry mapping method
- Analyze transport security events against operational context
- Build detection and escalation rules for connected infrastructure
- Prioritize containment actions using safety and service criteria
- Evaluate recovery readiness and evidence continuity
- Build an ITS Cyber Monitoring and Response Playbook

Course Agenda

Day 1: Map the ITS Monitoring Environment

- ITS IT-OT Asset and Service Dependency Map
- Traffic Management Center Data-Flow Diagram
- Roadside Unit and Connected Signal Trust Boundary Method
- Transport Service Criticality and Safety Matrix
- Telemetry Source Coverage Register

Day 2: Detect and Triage Security Events

- ITS Security Event Classification Taxonomy
- ETSI TS 102 940 Security Event Logging Concepts
- Misbehavior Indicator and Plausibility Check Catalogue
- Transport Alert Enrichment and Correlation Worksheet
- Operational Impact Triage Decision Tree

Day 3: Manage Escalation and Response

- Incident Declaration and Severity Matrix
- IT-OT Response Responsibility Map
- Third-Party Notification and Coordination Checklist
- Safety-Aware Containment Options Table
- Evidence Capture and Event Timeline Log

Day 4: Protect Continuity and Recovery

- Transport Service Continuity Priority Board
- Fallback Operations and Manual Control Checklist
- System Restoration Dependency Sequence
- Recovery Validation and Monitoring Plan
- Evidence-Ready Incident Handover Pack



Day 5: Practice ITS Cyber Response

- Exercise: Map a Traffic Control Service Dependency Chain
- Exercise: Triage Connected Roadside Security Events
- Exercise: Select Safety-Aware Containment Actions
- Exercise: Coordinate Recovery and Stakeholder Handover
- Capstone: ITS Cyber Monitoring and Response Playbook

Practical Exercises

The course uses suggested activities based on traffic control, tolling, traveler-information, and public transport disruptions.

- Suggested activity: correlate roadside alerts with control-center telemetry and service impact.
- Suggested activity: classify a suspected false-message event and select an escalation path.
- Suggested activity: compare containment options against safety, availability, and evidence needs.
- Suggested activity: assemble response, recovery, communication, and handover records into a playbook.

FAQs

Who suits intelligent transportation cyber monitoring training, and what does it assume?

Transport operators, control-center teams, cyber analysts, responders, and mobility engineers suit the training; it assumes they can interpret operational alarms and follow authorized escalation procedures.

How does intelligent transportation cyber response differ from generic SOC training?

Intelligent transportation cyber response applies monitoring and incident decisions to safety-sensitive IT-OT services, connected roadside infrastructure, service continuity, and transport stakeholder coordination rather than general enterprise alert handling.

What events should ITS cybersecurity monitoring prioritize?

ITS cybersecurity monitoring should prioritize abnormal device behavior, implausible messages, access anomalies, telemetry gaps, configuration changes, communications disruption, and events that could affect safety or service delivery.

How should transport teams contain a cyber incident without disrupting safety?

Transport teams should compare containment options against safety, operational availability, fallback capability, dependencies, evidence needs, and stakeholder responsibilities before applying an authorized action.



What belongs in an ITS incident handover?

An ITS incident handover should include scope, chronology, affected services, correlated evidence, containment actions, continuity decisions, third-party communications, restoration status, residual risks, and monitoring requirements.

Conclusion

Participants take back an ITS Cyber Monitoring and Response Playbook linking assets, telemetry, triage, escalation, containment, continuity, recovery, and evidence handover. It changes fragmented alerts into a safety-aware response workflow for connected transport services. The playbook supports coordinated decisions across operations, cybersecurity, engineering, suppliers, and emergency partners.