Cybersecurity Monitoring, Event Management and Incident Response in Intelligent Transportation Systems Training Course

Professional Development Training Course Outline

Category	Traffic Management & Road Safety	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid evolution of Intelligent Transportation Systems (ITS) integrating IoT sensors, autonomous vehicles, smart traffic control, V2X communication, and real-time data analytics has created a highly interconnected ecosystem vulnerable to sophisticated cyber threats. As the transportation sector digitalizes, ensuring cyber resilience, operational continuity, and data integrity has become a strategic imperative. Robust cybersecurity monitoring, SIEM-driven event management, and threat-intelligence-enabled incident response are essential to protecting national mobility infrastructures and preventing high-impact disruptions.

Cybersecurity Monitoring, Event Management and Incident Response in Intelligent Transportation Systems Training Course equips cybersecurity professionals, ITS engineers, and risk managers with the skills to deploy intelligent monitoring frameworks, analyze security events, orchestrate incident response playbooks, and apply advanced forensics across transportation networks. Through real-world case studies from traffic signal system breaches to connected vehicle cyberattacks participants will learn how to detect anomalies, mitigate threats, and develop resilient cyber-physical defense strategies aligned with global standards such as ISO 27001, NIST CSF, and IEC 62443.

Programme Curriculum

Cybersecurity Monitoring, Event Management and Incident Response in Intelligent Transportation Systems Training Course

Introduction

The rapid evolution of Intelligent Transportation Systems (ITS) integrating IoT sensors, autonomous vehicles, smart traffic control, V2X communication, and real-time data analytics has created a highly interconnected ecosystem vulnerable to sophisticated cyber threats. As the transportation sector digitalizes, ensuring cyber resilience, operational continuity, and data integrity has become a strategic imperative. Robust cybersecurity monitoring, SIEM-driven event management, and threat-intelligence-enabled incident response are essential to protecting national mobility infrastructures and preventing high-impact disruptions.

Cybersecurity Monitoring, Event Management and Incident Response in Intelligent Transportation Systems Training Course equips cybersecurity professionals, ITS engineers, and risk managers with the skills to deploy intelligent monitoring frameworks, analyze security events, orchestrate incident response playbooks, and apply advanced forensics across transportation networks. Through real-world case studies from traffic signal system breaches to connected vehicle cyberattacks participants will learn how to detect anomalies, mitigate threats, and develop resilient cyber-physical defense strategies aligned with global standards such as ISO 27001, NIST CSF, and IEC 62443.

Course Duration

5 days

Course Objectives

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

1. Implement real-time cybersecurity monitoring dashboards for ITS infrastructures.
2. Deploy SIEM platforms for traffic-related event correlation and threat detection.
3. Analyze anomalous behavior patterns in V2X and IoT-based transportation systems.
4. Apply threat intelligence to anticipate emerging ITS-specific cyber risks.
5. Develop and execute incident response playbooks for cyber-physical transportation networks.
6. Conduct digital forensics on compromised transportation assets.
7. Assess vulnerabilities in connected vehicle ecosystems.
8. Implement network segmentation and zero-trust architecture in ITS environments.
9. Apply MITRE ATT&CK techniques to transportation cyberattack scenarios.
10. Evaluate risk scoring and impact modeling for critical mobility infrastructure.
11. Strengthen OT-IT convergence security within traffic management centers.
12. Integrate cloud-native security controls into ITS data platforms.
13. Ensure compliance with NIST, ISO, and IEC security frameworks for transportation systems.

Target Audience

1. Cybersecurity Analysts
2. ITS Engineers and Technologists
3. Security Operations Center (SOC) Teams
4. Incident Responders
5. Transportation Infrastructure Managers
6. Government Mobility & Smart City Officers
7. Network and System Administrators
8. OT/ICS Security Professionals

Course Modules

Module 1: Foundations of Cybersecurity in Intelligent Transportation Systems

- Overview of ITS architecture and cyber-physical components
- Attack surfaces in connected mobility ecosystems
- Role of cybersecurity in traffic optimization and public safety
- Overview of NIST CSF, ISO 27001, and ITS security standards
- Mapping cyber threats to ITS operational components
  Case Study: Cyberattack on a city's traffic signal synchronization network

Module 2: Cybersecurity Monitoring Tools and Techniques for ITS

- SIEM integration with transportation sensors and control systems
- Network monitoring using IDS/IPS for V2X and IoT devices
- Log analysis, anomaly detection, and alert triage
- Monitoring cloud-based ITS data platforms
- KPI benchmarking for ITS cybersecurity performance
  Case Study: Detecting abnormal data spikes in connected vehicle telemetry

Module 3: Event Management and Traffic Control Center Security Operations

- Event lifecycle in transportation SOC environments
- Event correlation for multi-modal transportation networks
- SOPs for handling traffic-related cybersecurity events
- OT-IT event visibility consolidation
- Automating event routing and prioritization
  Case Study: Security event escalation in a metropolitan traffic management center

Module 4: Threat Intelligence and Attack Surface Management for ITS

- Leveraging global and sector-specific threat intelligence feeds
- Attack surface mapping for roadside and vehicle subsystems
- Identifying emerging threats targeting ITS and smart mobility
- Vulnerability intelligence and patch prioritization
- AI-driven threat forecasting for transportation infrastructures
  Case Study: Threat intelligence alert for malicious firmware targeting traffic cameras

Module 5: Incident Response Frameworks for Transportation Networks

- Incident response lifecycle tailored for ITS
- Creating ITS-specific IR playbooks and escalation protocols
- Coordinating response with government and emergency agencies
- Evidence acquisition from cyber-physical assets
- Post-incident reporting and lessons learned
  Case Study: Coordinated response to ransomware impacting toll collection systems

Module 6: Digital Forensics for Traffic and Transportation Systems

- Forensic imaging of roadside and onboard vehicle devices
- Log forensics for V2X communication networks
- Chain-of-custody for forensic evidence in ITS environments
- Malware analysis relevant to transportation threats
- Reporting forensic findings for legal and compliance purposes
  Case Study: Forensic reconstruction of a compromised traffic sensor array

Module 7: Securing Connected Vehicles and V2X Communication

- V2V, V2I, and V2N cyber risks
- Secure communication protocols for connected vehicles
- Hardening onboard units and roadside units
- Intrusion detection for vehicular networks
- Testing cybersecurity of autonomous navigation systems

  Case Study: Exploitation of a V2X communication vulnerability causing false traffic alerts

Module 8: Building Resilient ITS and Future-Ready Cyber Defense Strategies

- Zero-trust architecture for smart transportation
- Cloud and edge security integration for ITS
- AI-driven threat detection and predictive analytics
- Business continuity and cyber-resilience planning
- Designing future-proof mobility cybersecurity frameworks

  Case Study: Implementing zero-trust segmentation in an intelligent transit system

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- 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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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