

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

DAY 1

Cybersecurity & The Intelligent Transportation (ITS) System Environment

- How cyber-attacks happen
- Industries affected
- The Intelligent Transportation System (ITS) Environment
- Role of Autonomous vehicles
- ITS Architecture
- New mobility platforms
- A Need to Secure ITS

DAY 2

ITS models, Infrastructure, Cybersecurity Threats & Vulnerabilities

- Overview of Cybersecurity
- ITS Models: Operators
ITS systems and infrastructure
- Communication systems, wired, wireless
- Data management, sharing, and governance
- Threats & vulnerabilities in ITS

DAY 3

ITS Cybersecurity Risk Assessment and Mitigation

- Cybersecurity Risk assessment in ITS
- Cybersecurity challenges
- Approaches in ITS cybersecurity
- Cybersecurity protection frameworks: NIST and others
- Cybersecurity Controls

DAY 4

ITS Monitoring and Incident Response

- Penetration Testing for ITS
- Cybersecurity Monitoring
- Event Management
- Incident Response
- Best practices for first responders

DAY 5

ITS & Cybersecurity Standards – Current and Future Practices

- ITS & Cybersecurity Standards
- Good Practices
- Gap Analysis
- Plan of action
- Innovative approaches: AI, blockchain