€TRAINING

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

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

Introduction

The most crucial tasks to carry out in a powerful defense system against cyberattacks on an ITS are covered in this training course on cybersecurity monitoring, event management, and incident response in intelligent transportation systems. The cyberspace and everything it implies, including ITS, are no longer the same after the recent "supply chain attack" on cybersecurity firms in the USA like SolarWinds early in December 2020. The SolarWinds cybersecurity breach, which has shown that no system is secure regardless of how precisely it is designed, is maybe the biggest one to date. The enormity of this incident's scope, importance, and harm will probably only increase when more information about the breach comes to light.

Although the SolarWinds breach only impacted data confidentiality, it is just a matter of time before similar attacks also undermine other security features including application-related data integrity. It can have severe effects on the industry if data integrity related to any physical real-world functionality, like the ITS infrastructure, is compromised. Delegates taking this training session will have a thorough understanding of the essential actions needed to fulfill this general criterion in an ITS environment. Cybersecurity demands resilience in addition to robust defenses.

Course Objectives

At the end of this course, Participants will be able to:

- List and describe major ITS Cybersecurity Threats and Vulnerabilities Understanding the ITS environment and its architecture
- Create mitigation methods after doing an ITS Cybersecurity Risk Assessment.
- Create an incident response and ITS monitoring plan.
- List and evaluate the most significant present-day and future defensive strategies.
- List and understand the most significant ITS and Cybersecurity Standards

Targeted Audience

- Project Managers
- Technology Engineers, Chief Technology Officers CTOs and Chief Information Officers CIOs
- Strategic Development Personnel
- Transport Operators, Engineers, Managers, and Researchers
- ITS and Cybersecurity Industry Consultants
- IT and Cybersecurity Professionals
- Operators and Professionals of Transport Systems
- City governments Involved in Transport Systems
- Enterprises involved in the design of Transport System

Course Outline

Unit 1: 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

Unit 2: 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

Unit 3: ITS Monitoring and Incident Response

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

Unit 4: ITS & Cybersecurity Standards - Current and Future Practices

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

Unit 5: 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