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

INTRODUCTION

- This Cybersecurity Monitoring, Event Management, and Incident Response in Intelligent Transportation Systems training course covers the most important activities to be performed in a strong defense system against cyberattacks to an ITS. After the recent “supply chain attack” on cybersecurity companies in the USA such as SolarWinds early in December 2020, the cyberspace and all it entails including ITS is no longer the same. The SolarWinds cybersecurity breach is perhaps the major one thus far and has demonstrated that no system, no matter how carefully designed, is secure. The scale, significance, and damage of this incident is huge and will likely grow as more details of the breach are discovered.
- Although the SolarWinds breach affected only the confidentiality of data, it is just a matter of time before other security properties such as application related data integrity is also compromised by similar attacks. If data integrity related to any physical real-world functionality such as the ITS infrastructure is compromised this can lead to disastrous consequences in the industry. Cybersecurity requires resilience as well as strong defenses and delegates attending this training course will get a deep understanding of crucial steps to achieve such generic requirement in an ITS environment.

This training course will highlight:

- The ITS Environment and Architecture
- Role of Enterprises, IT, Infrastructure, Autonomous vehicles, Communications, and Data
- ITS Cybersecurity Threats, Vulnerabilities, Risk Assessment and Mitigation
- ITS information monitoring and Incident Response
- Most significant ITS and Cybersecurity Standards
- Current and Future Cybersecurity Practices

OBJECTIVES

At the end of this training course, you will learn to:

- Understand the ITS environment and explain its architecture
- List and explain various ITS Cybersecurity Threats and Vulnerabilities
- Perform an ITS Cybersecurity Risk Assessment and develop mitigation strategies
- Develop an ITS monitoring and incident response plan
- List and analyze the most important current and future practices of strong defenses
- List and understand the most significant ITS and Cybersecurity Standards

TRAINING METHODOLOGY

- Participants to this training course will receive a thorough training using several techniques that include coverage of material, discussions, breakout exercises, videos, and tests. The hands-on breakout exercises will be performed in groups and will enable participant to apply the material to real world scenarios with active discussions with other members of the group. Pre-tests and post-tests will measure what was learned in this training course.

ORGANISATIONAL IMPACT

- The organization will benefit from understanding the principles of cybersecurity of ITS systems with emphasis on monitoring, event management, and incident response and how these can be applied. In light of recent incidents, organizations want to apply the principles of cybersecurity to protect their assets and those of their stakeholders.

The participants on this training course, will:

- Enhance their analytical and problem-solving skills through participation in breakout exercises
- Learn how to analyze the cybersecurity of the Intelligent Transport Systems (ITS) infrastructure
- Be able to apply cybersecurity techniques to implement resilience and strong defenses
- Learn how to perform cybersecurity risk assessments for their organization
- Improve the cybersecurity of their organizations
- Develop cybersecurity plans including those for monitoring, event management, and incident response
- Organization will become adaptive and improve their cybersecurity while at the same time serve stakeholders and the public at the highest level

PERSONAL IMPACT

The participants will gain or enhance their understanding and application of cybersecurity monitoring, event management and incident response by:

- Understanding how attacks happen in an ITS environment
- Identifying attack vectors in existing ITS architectures
- Identifying threats and vulnerabilities in ITS
- Understanding cybersecurity protection frameworks and designing cybersecurity controls
- Developing various cybersecurity plans including information monitoring and incident response
- Applying best practices for event management and incident response
- Apply methods to perform cybersecurity risk assessment and mitigation
- Recognize the need and benefits of standards
- Prepare for the future cybersecurity attacks and breaches in ITS

WHO SHOULD ATTEND?

- This training course is designed for all the people involved in operations, software, services, mobility ITS infrastructure, traffic and transport planning and organization, IT experts, as well as researchers and consultants involved in cybersecurity, management, big data, communications, project management and intelligent transport mobility.

This training course is suitable to a wide range of professionals but will greatly benefit:

- IT and Cybersecurity Professionals
- Operators and Professionals of Transport Systems
- City governments Involved in Transport Systems
- Enterprises involved in the design of Transport Systems
- 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

Course Outline

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

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

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

ITS Monitoring and Incident Response

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

ITS & Cybersecurity Standards – Current and Future Practices

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