Event management, incident response, and cybersecurity monitoring in intelligent transportation systems

Keeping your Assets Safe and Secure in a Fully Connected

Introduction

The most crucial tasks that must be completed in a robust defense system against cyberattacks on an ITS are covered in this Course N Carry Event Management, Incident Response, and Cyber Security Monitoring in Intelligent Transportation Systems training course. The cyberspace and everything that it encompasses, including ITS, are no longer the same following the recent "supply chain attack" on cybersecurity businesses in the USA, such SolarWinds, early in December 2020. Possibly the largest cybersecurity breach to date, the SolarWinds incident has shown that no system, no matter how well-designed, is secure. This catastrophe is massive in scope, importance, and harm, and it will probably get worse when more information about the breach comes to light.

While just data confidentiality was impacted by the SolarWinds vulnerability, it won't be long until similar assaults also jeopardise other security features like application-related data integrity. Data integrity breaches pertaining to any tangible, on-the-ground operation, like the ITS infrastructure, can have catastrophic effects on the sector. Delegates taking this training course will gain a thorough grasp of the essential processes to build resilience and strong defenses, which are prerequisites for cybersecurity in an ITS system.

This instruction session will emphasise:

- The Architecture and Environment of ITS
- The function of data, communications, IT, infrastructure, autonomous cars, and enterprises
- Threats to ITS Cybersecurity, Vulnerabilities, Risk Evaluation, and Mitigation
- Information tracking and incident response for ITS
- The most important standards for cybersecurity and ITS
- Cybersecurity Practices: Present and Prospective

Objectives

Upon completion of this training programme, you will be able to:

- Recognise the ITS environment and describe its design.
- Enumerate and describe the many ITS Cybersecurity Risks and Weaknesses.

- Assess the risks associated with ITS cybersecurity and create mitigation plans.
- Create a plan for incident response and ITS monitoring.
- Enumerate and evaluate the most crucial strong defense techniques from the past, present, and future.
- Enumerate and comprehend the most important Cybersecurity and ITS Standards.

Training Methodology

This training course will cover a lot of ground and provide participants with a thorough education using a variety of methods, such as lectures, discussions, breakout activities, films, and exams. Participant application of the information to real-world circumstances will be facilitated by interactive group discussions throughout the hands-on breakout exercises. The knowledge gained from this training course will be assessed by pre- and post-tests.

Organizational impacts

Understanding the fundamentals of cybersecurity for ITS systems—with a focus on incident response, event management, and monitoring—and how to implement them will be beneficial to the organisation. Organisations wish to use cybersecurity principles to safeguard their assets and those of their stakeholders in light of recent incidents.

Attendees of this Course N Carry training programme will:

- Participate in breakout exercises to improve their analytical and problem-solving abilities.
- Discover how to analyse the infrastructure's cybersecurity for Intelligent Transportation Systems (ITS).
- Possess the ability to use cybersecurity strategies to build robust defences and resilience
- Acquire the knowledge to conduct cybersecurity risk assessments for their company.
- Bolster their companies' cybersecurity
- Create plans for cybersecurity that address event management, incident response, and monitoring.
- Organisations will become more flexible and enhance their cybersecurity while providing the best possible service to stakeholders and the general public.

Personal Imapct

The following will help the attendees better understand and apply Event Management, Incident Response, and Cyber Security Monitoring in Intelligent Transportation Systems;

- Recognising the mechanisms behind assaults in an ITS environment
- Locating potential points of attack in current ITS designs
- Finding ITS vulnerabilities and threats
- Recognising cybersecurity protective structures and creating cybersecurity safeguards

- Creating different cybersecurity plans, such as those for incident response and information monitoring
- Putting event management and incident response best practices into practice
- Utilise techniques to carry out risk assessment and mitigation for cybersecurity.
- Acknowledge the value and necessity of standards
- Get ready for upcoming ITS cybersecurity threats and breaches.

Who should attend?

The people who work in operations, software, services, mobility ITS infrastructure, traffic and transport planning and organisation, IT specialists, and researchers and consultants in cybersecurity, management, big data, communications, project management, and intelligent transport mobility are all intended audiences for this Course N Carry training course.

Though a wide range of professionals can benefit from this training, the following will be especially noted:

- Professionals in IT and Cybersecurity
- Transport System Professionals and Operators
- Municipalities Taking Part in Transportation Systems
- Project managers from businesses engaged in the creation of transport systems
- Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and Technology Engineers
- Personnel for Strategic Development
- Researchers, Managers, Engineers, and Transport Operators
- Industry Consultants for Cybersecurity and ITS

Course Outline

Day 1

Cybersecurity and the Environment of the Intelligent Transportation System (ITS)

- How cyberattacks take place
- Affected Industries
- The Environment of the Intelligent Transportation System (ITS)
- Autonomous cars' role
- Architecture for ITS
- Fresh platforms for mobility
- The Need for ITS Security

Day 2

Infrastructure, Cybersecurity Vulnerabilities & Threats, and ITS Models

- Synopsis of Cybersecurity
- Models of ITS: Operators
- Infrastructure and ITS systems
- Systems of communication: wired and wireless
- Governance, sharing, and management of data
- Risks and weaknesses within ITS

Day 3

Cybersecurity Risk Evaluation and Reduction for ITS

- Evaluation of cybersecurity risks in ITS
- Cybersecurity issues
- Techniques in Cybersecurity for ITS
- Frameworks for cybersecurity protection: NIST and others
- Controls for Cybersecurity

Day 4

ITS Surveillance and Reaction to Events

- ITS Penetration Testing
- Monitoring of Cybersecurity
- Event Supervision
- Response to Incidents
- Optimal procedures for first responders

Day 5

Cybersecurity and ITS Standards: Current and Upcoming Procedures

- Cybersecurity and ITS Standards
- Best Approaches
- Analysis of Gaps
- Action Plan