Certified Professional for Airport IoT Security (CPAIS)

This program is intended to provide a first-hand experience in understanding a cyber attack on IoT and SCADA systems at Airports. It will also provide an insight as to how various IT infrastructures are set up and the possible loopholes or vulnerabilities in each system can be tested.

This exclusive training covers scenarios that are related to cyber threats observed across infrastructures in the Aviation Industry.

The approach of this training would be in the manner of Offensive testing, so as to understand better, of ways to deal with a hack/malware attack. This approach would make sure that the right defense mechanisms are thought and applied.

Summary

- IT & OT Infrastructure in modern Airports
- Cyber Attack Vectors
- IoT Attacks
- Endpoint Systems Compromise
- Preventive Measures
- Regulations and Audits

Level: Beginner / Intermediate

Duration: 10 Hours – 5 Days

GMR AVIATION ACADEMY
A Gateway to Global Aviation Learning
ISO 9001:2015 CERTIFIED

ISAC

CYBERSECURITY PROGRAMS

Participant Requirements

Each participant is expected to carry his own laptop for carrying out a series of challenges and hands-on exercises. Participants are required to have virtualization software installed. The intention is to set up a personal lab for practice.

Deliverables

Each participant will get a training certificate along with a discount voucher to attend the National Security Database certifications programme.

Course Details

Module 1: Introduction

- Overview of IoT
- SCADA
- Security Challenges

Module 2: Overview of Modern IoT / SCADA components of an Airport

- Part 1
  - IoT Sensors / Critical Equipments at operation area
- Part 2
  - Monitoring and Preventing Threats/Attacks on Systems like Flight Display Systems, CUPPS – Common Use Passenger, Platform System, and BRS – Baggage Reconciliation System
- Part 3
  - CUTE – Common Use Terminal Equipment
  - CUSS – Common Use Self Service Systems
  - Central Arrival and Departure Gates Control System
  - Smart Parking

Module 2: Cyber Attack Vectors

- Trojans
- Social Engg. Attacks
- DDoS
- Ransomware

Module 3: Scenario: Discovery of Sensitive Devices

- Hands-on Scenario: Information Discovery
- Hands-on Scenario: Network Hacking via IoT
- Hands-on Scenario: Hacking Smart Devices
- Hands-on Scenario: Ransomware attacks
- Hands-on Scenario: Sabotaging Gate Controls in Airport

Module 4: Controlling SCADA Systems

- Hands-on Scenario: SCADA Security
- Hands-on Scenario: DoS & DDoS
- Hands-on Scenario: Deploying Malware on IoT

Module 5: Defensive Measures

- Hands-on: Threat Intelligence
- Hands-on: Endpoint Protection
- Employee training
- Other Security Softwares
- Hands-on: Conducting effective VAPT on IOT / SCADA
- Reporting best practices

GMR AVIATION ACADEMY
A Gateway to Global Aviation Learning
ISO 9001:2015 CERTIFIED

ISAC

CYBERSECURITY PROGRAMS

New Delhi, Academy, Terminal 2, opp. Departure Gate No. 1, Indira Gandhi International Airport, New Delhi, India – 110037
Contact:+ 91 88103 76483

Hyderabad, Academy, Ground Floor, SSC, GMR Aero Towers, Rajiv Gandhi International Airport, Shamshabad, Hyderabad, India – 500108
Contact:+ 91 70131 89812 / 99896 54915

/gmraviationacademy
/company/gmraviationacademy
/gmraviationacademy

www.gmraviationacademy.org
gmraa.contact@gmrgroup.in

Click Here to Register

To enroll & pay
NEFT/ RTGS details –

Bank Name: IDFC First Bank Limited
Branch Address: Barakhamba Road, New Delhi
Beneficiary Name: GMR Airports Limited
Current Account No. : 10057844842
IFSC Code: IDFB0020101

Or Click Here