AVIATION CYBER AND INFORMATION SECURITY

Tuition: US $ 2750

Location: Online

About the Program**:** Aviation Cybersecurity certificate program provides students with an understanding of the key elements of cybersecurity, the Internet of Things (IoT), and aviation cybersecurity. Learn the history, core principles, threats and attacks, defensive strategies, regulations and guidelines, and real-world examples. The Aviation Cybersecurity certificate focuses on defining the operational issues involved in preventing and mitigating cybersecurity threats in the aviation domain. The program begins with overview courses examining cybersecurity and the Internet of Things (IoT), then provides practical application of these concepts to the aviation industry.

Who Should Attend

The Aviation Cybersecurity certificate is designed to provide a strong foundation for those students interested in learning more about aviation cybersecurity. It is intended both for students new to the subject and the more experienced cybersecurity professional interested in learning more about aviation cybersecurity.

Key Topics

Upon completion of the program, students should be able to demonstrate a comprehensive understanding of the following high-level learning objectives:Contrails forming behind plane in flight

- Core principles of cybersecurity threats, attacks, and defense
- Functions, characteristics, and cybersecurity vulnerabilities of the Internet of Things (IoT)
- Cybersecurity principles as they relate to aviation:
  - Functions, characteristics, and cybersecurity vulnerabilities of aviation IoT
  - Specific cybersecurity threats and attacks against the aviation domain
  - Application of the principles of cybersecurity defense to the aviation domain
- Professional verbal and written cybersecurity communication skills
- Industry-standard techniques for protecting aviation networks and data

Course Specifics

The courses are taught by an instructor in an asynchronous modality. Courses have designated start and end dates and required weekly assignments, though students are not required to log in at a specified time or day during the week. Students interact with instructors and classmates through discussion boards, assignments, and email.

Course Unit I: Understanding Cybersecurity

In this first course, students will review the evolution of cybersecurity and learn about the core cybersecurity goals of confidentiality, integrity, and availability as they apply to protect systems and information. Students will explore the operational aspects of cybersecurity, including access control, physical security, networking and telecommunications, business continuity, applications, and risk management. Students will examine the principle of defense-in-depth as a key strategy in cybersecurity defense. The course will also review cyber-attacks, including types of attacks, methodology and tools used in attacks, and motivations of attackers. The course will include a global review of cybersecurity frameworks, laws, and regulations. Lastly, students will examine best practices in building an operational cybersecurity defense plan.

Course Objectives

- Multiple computers in a control room
- Examine the core principles of cybersecurity, including confidentiality, integrity, and availability (CIA).
- Evaluate the design and implementation of layered cybersecurity defense.
- Analyze cybersecurity vulnerabilities, threats, and attack vectors.
- Assess the types and motivations of cybersecurity attackers and methods of attack.
- Apply operational cybersecurity defense principles to support resilience and risk mitigation.
- Distinguish global laws, regulations, frameworks, and policies related to cybersecurity defense.
- Demonstrate appropriate professional communication skills

Course Unit II: Exploring Internet of Things (IOT)

The course unit examines all aspects of this new and ever-expanding field. The Internet of Things (IoT) is comprised of processors, sensors, and actuators embedded in a wide variety of physical devices connected by the Internet, wired, and wireless networks. Billions of IoT devices are embedded in buildings, homes, cars, planes, energy systems, personal devices, and more. Many of these IoT devices have poor security and are therefore vulnerable to cybersecurity attacks. This connectivity and vulnerability extends to aviation cybersecurity, making the study of IoT crucial in the industry.

In this course, students examine the elements that comprise the Internet of Things (IoT), including its history, the technology used to build connected devices, how the devices communicate, and how they store and share data. Course content reviews the many uses of IoT devices in the aviation industry, including aircraft manufacturing, maintenance, tracking of passengers and luggage, passenger entertainment, building maintenance, avionics, and more. The course also examines cybersecurity vulnerabilities, threats, and attacks against IoT systems as well as strategies to use in securing IoT devices and systems. Finally, students review the vulnerabilities, threats, and attacks specific to the aviation IoT infrastructure.

This course consists of 6 Modules:

- Module 1 - Course Introduction and Overview and the History of the Internet of Things
- Module 2 - Understanding Cyber-Physical Systems
- Module 3 - IoT Architecture and Applying the IoT Architecture
- Module 4 - IoT Vulnerabilities and Attack Vectors and Securing IoT Systems
- Module 5 - The Future of IoT
- Module 6 - Course Summary & Key Points

Course Objectives

- Examine the history and core functions of the Internet of Things (IoT).
- Describe the characteristics of cyber-physical systems.
- Evaluate the design and implementation of the IoT Architecture.
- Analyze cybersecurity vulnerabilities, threats, and attack methods related to IoT systems.
- Apply operational cybersecurity defense principles in the prevention and mitigation of IoT attacks.
- Apply IoT concepts, architecture, and cyber-security risks to the aviation industry.
- Assess the future of IoT systems.
- Demonstrate appropriate professional communication skills.

Course Unit III: Introduction to Aviation Cybersecurity

In this unit, students will examine how cybersecurity impacts nearly every aspect of aviation including commercial air traffic, unmanned aircraft systems, air traffic control, and aerospace. Students will review the threats to aviation security and mitigations of those threats. Students will also review regulations, recommendations and best practices in aviation cybersecurity and how these can be incorporated into an operational plan of securing aviation systems.

Course Objectives

- Review the elements of the aviation infrastructure.
- Identify vulnerabilities, threats, and attack opportunities against the aviation infrastructure.
- Analyze the role of the pilot in mitigating aviation cyber-attacks.
- Assess the regulations and best practices to prevent and mitigation aviation cyber-attacks.
- Apply operational cybersecurity defense principles to an aviation cyber defense plan.
- Demonstrate appropriate academic and professional communication skills.

Course Unit IV: Aviation Cybersecurity Threats, Actors, Tools & Techniques

In Aviation Cybersecurity Threats, Actors, Tools & Techniques, students explore the cybersecurity threats and actors that pose risks to aviation. Course content reviews both tools and techniques used by malicious actors and those used to defend against threats and attacks. Students learn the fundamentals of developing an incident response plan and operational defense plan to prepare an organization to respond to cybersecurity threats and attacks.

Course Objectives

- Review vulnerabilities in, threats to, and attack opportunities in the aviation infrastructure
- Examine specific aviation cyber-attack methods and techniques
- Evaluate cyber-defense tools, techniques and processes to prevent or mitigation aviation cyber-attacks
- Apply operational cybersecurity defense principles to build a strong defense against aviation cyber-attacks
- Demonstrate appropriate academic and professional communication skills