Carmel
Trainings & Deployments

CTR-907 CSSP - Cyber Security Preparation Program

About this course

This is a 24-hour course that teaches pupils about cyber security preparedness. Threats to information security are numerous, persistent, and increasingly sophisticated. Students will be able to use what they've learned about CSPP in the real world by the end of the course. Students will have a solid understanding of cyber dangers and the need of eliminating them. This course aims to keep students informed about current events while also stimulating meaningful conversations among a diverse group of people.

Audience profile

This course is designed for individuals that are interested in the profession of network management. It is also designed for those without a previous background in computers and who have an in-depth knowledge of the world of networks, systems, and protection.

At course completion

After completing this course, students will be able to:

- Understand information as it pertains to systems and governance.
- Identify and describe how new data privacy laws are adopted by organizations.
- Describe how cyber threat intelligence is used for the daily workings of an organization
- Examine to contain, eradicate and recover cyber threats or attacks on systems/networks.

Course details

Module 1: Introduction to Cyber Security Preparation

This module will teach about the basics of cyber security preparations, the fundamentals of cyber security, the threats, and the mitigation of attacks. You'll learn about security policies and procedures.

Module 2: Enterprise Architecture and Components

This module is about securing architecture, wireless networks, network security controls, cloud virtualization, BYOD, and IoT security. Students will learn how to test security and major takeaways.

Module 3: Information System Governance and Risk Assessment

This module addresses Information security governance, risk management, and information security programs.

Module 4: Deception Technologies & Incident Management

This module teaches you about developing an incident management response system, digital forensics business continuity, deceptive technology, and response to systems.

Module 5: AI and Machine Learning

This module teaches you about artificial intelligence and modern machine learning as it pertains to cyber security. Here, you'll learn about how these systems offer impressive results and how they represent a fertile research area.

Module 6: GDPR

In this module, you will learn about General Data Protection Regulation and how new data privacy laws are adopted by organizations with clients worldwide, and how organizations meet current and future compliance needs.

Module 7: Application Inventory

This module teaches you how to build a security operation that considers company risk and allocates resources. You will learn about how important application inventory is to a business, and you will learn about collaboration with other parts of the business.

Module 8: Attack Surface Reduction

This module teaches about how modern security operation assumes adversaries will get into internal systems. You will learn about the number of investigations that need to be performed by the security operations team to as to limit cyber-attacks.

Module 9: Cyber Expertise

This module talks about how to detect insecure features and malicious activities within networks and infrastructure. You will know how to implement customized application security assessments for client-based asset risk, and corporate policy compliance as well as to conduct a vulnerability assessment.

Module 10: Assessments

In this module, you will understand the assessment analysis of an organization's cybersecurity controls and its ability to tackle vulnerabilities. These risk assessments are carried out within the context of the organization's business objectives.

Module 11: Cyber Threat Intelligence

This module teaches about cyber threat intelligence as a branch of cybersecurity that focuses on the collection and analysis of data about current and possible attacks that threaten the safety of an organization or its assets. You will learn of the advantages and its proactive security measure and prevention of data breaches.

Module 12: Software

This module teaches you how to protect your internet-connected systems and data from cyber threats. You will understand the practice used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Module 13: Containment, Eradication, and Recovery (Cyber Risk Transfer)

This module teaches you how to shift risk liability and responsibilities. You will know of the actions required to prevent incidents or events from spreading to networks as well as actions required to completely wipe the threat from the network/system and actions required to bring back the network/system to its former functionality and use.

Prerequisites

- Entry Level exam (American test)
- A basic understanding of using operating systems, networks, and the Internet. Be able to download and install the software. A willingness to learn.
- Foundational knowledge about how to practice cybersecurity in the real world.
- This program requires multidisciplinary studies in the system,
- Basic knowledge of Linux & Windows, in the communication of all its shades according to Cisco.