# CTR-908 CSP - Cyber Security Practitioner

## *About this course*

This is a 50-hour course designed to accommodate the contents and skills taught in various CSP programs offered by different cyber educational institutes around the world. The growing demand for well-educated and knowledgeable cyber defense experts requires a broad and in-depth background in the practical, technological solutions which are embedded in this well-established hands-on rich program. The CSP curriculum is designed to train cyber defense experts who can implement, guide, and make decisions on information security defense tasks, in the technological, hands-on aspects. These abilities will be acquired through mastery of the best practice strategies, techniques, and industry-relayed regulations of the field, including risk management skills.

## *Audience profile*

This course is designed for those who have theoretical and practical experience in system and networking and a fundamental understanding of cybersecurity, preferably with some experience in programming (python).

## *At course completion*

After completing this course, students will be able to:

- Implement, monitor, and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity, and availability.
- Understand the broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) to ensure its relevancy across all disciplines in the field of information security.
- Identify various domains such as access controls, security operations, and administration, risk Identification, monitoring, and analysis
- Identify and explain various incident response and recovery, cryptography networks, and communications security.
- Examine systems and application Security.

## *Course details*

**Module 1: Introduction to Cyber Security**

This module will teach you all you need to know about cybersecurity. This program looks at the ontology of information security and cyber, types of offenders, motivation for attacks, vulnerabilities kinds, implications of cyber-attacks, organizational coping methods, human components, information policies, and procedures in project management. You'll also study how cyber-security has been utilized in impacting employee reliability.

**Module 2: Physical Security**

This module is about the guidelines of the law regarding cyber security, what to protect, and security & monitoring measures to prevent unauthorized access. This

session delves into the measures used in dealing with various extreme events such as power outages, earthquakes, war & other natural disasters.

**Module 3: Securing the Network**

The goal of this course is to teach you about Security and protection products for LAN / WAN, Wireless and Bluetooth, Remote access to organizational resources and protection of these access routes, handling access via computers / mobile devices such as smartphones, iPad, Setting up a VLAN, aspects of information security/networks/organization when connecting the organization's network to the Internet, network security technologies and products, construction of DMZ, description of the applicative protocols, HTML5, HTML3, WebRTC, applications, and security aspects. This module covers Web Filtering and WAF (web application firewall).

**Module 4: Cryptography and Authentication**

This module focuses on symmetric and asymmetric encryption - DES DES3, RSA, and authentication of users. You'll also learn about protocols that support encryption and authentication such as IPSEC, SSL, HTTPS, and SSH.

**Module 5: Severs and OS Hardening**

This module teaches you of Implementation of information security within the framework of the following operating system services: Unix, Win, Android, VM, basics of User Identification and Verification Processes, Kerberos, object and Subject permissions, files, operating system logs that support information security. This session covers the principles of the hardening process, basic operations of the various operating systems Unix, Win, VM, server hardness test, products support hardening, and anomalies detection.

**Module 6: Aspects of information security in databases**

This module educates students about the Database Basics: SQL, Relational DB, MongoDB, Architecture, aspects of information security in the above systems, operating system support for maintaining the database, support for the database software on security issues, and referential integrity. This session covers a range of analyses on Storage systems and their information security in them.

**Module 7: BCP/DRP**

This module will teach you the theory of DRP and BCP, methodology for backup and recovery - full, partial backup, use of blogs as backup, environmentally dependent methods - split computer sites, different operating systems, operating system services for backup, and recovery, complementary external products. You'll learn about organizational aspects of disaster recovery and information security aspects of backup and recovery.

**Module 8: Malware and Anomaly Detection**

This session provides an in-depth understanding of malware such as trojans, worms, and viruses, as well as the backdoor or remote access that malware has. You will learn

how to spot abnormalities using static analysis, dynamic analysis, code analysis, and memory forensics in this module.

**Module 9: Access control**
This module will explore User identification and authentication theory, the concept of multifactor authentication, additional software/hardware for user identification and authentication such as Tokens, Smart cards, and Biometric devices, processes of linking the hardware component to a specific user, definition, and use of Identity management systems, Interface with DNS for user management, event alert. recognizing access to permitted mobile devices (BYOD access), application management, and access to the - MAM (Mobile application management) products and actions to prevent the connection of unauthorized equipment such as a laptop to the organization's network.

**Module 10: DLP**
In this module, you will study the definition of the concept, routs of data leakage, identifying data leakage, means and existing methods for preventing/reducing the phenomenon, for identification and detection, law aspects of DLP, Protection/prevention/reduction of information leaks in databases, storage systems, protection/prevention/reduction of information leaks in mobile devices such as smartphones, laptops. You'll learn about the detachable memory devices - disk-on-key and products and technologies for prevention/detection/identification - such as content filtering products.

**Module 11: Management and registration of information security events (Audit)**
In this session, you will study SOC (security operation center) products, SIEM products (security information event management), Network access control (NAC) products, and sensors - installation and configuration. This module covers the process definition of product rules, false alerts versus true alerts, tracking, updating, maintenance, integration of these products into the organization, reporting routes, and the dealings with the warning information received from an external or internal source to the organization.

**Module 12: Aspects of information security in network and hardening equipment**
In this module you will learn about the principles of the hardening process, hardening depends on network equipment (for example a CISCO router versus a router from another manufacturer) and software update, firmware, and networking equipment. This session teaches you about the equipment used in the hardening test, the products supporting hardening, and synchronization with security products to report anomalies.

**Module 13: Cloud computing, hosting services, virtualization**
This module delves into the familiarities, the different types of cloud computing, receiving reports from the various logs and understanding them, and identifying anomalies and products that support guest and host security. You will understand the need for the VM environment, its types, and security aspects.

**Module 14: Application Security**

This module identifies the risks facing software/application systems, determining information security requirements for the software system/application. You will learn the various activities, in terms of information security, that must be performed at every stage of the software/application development life cycle.

***Prerequisites:***

- Entry Level exam (American test)
- Practical knowledge and experience in IT systems (Linux and Microsoft) and networking.
- Familiarity (basic level) with cybersecurity solutions and products or BSc (or equivalent) in Computer Science or Software Engineering
- Good command of the English language
- Preferably: basic knowledge of python