OVERVIEW

The SSCP training provides a comprehensive review of the knowledge required to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data con dentiality, integrity and availability. This training course will help students review and refresh their knowledge and identify areas they need to study for the SSCP exam.

SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP)

COURSE DURATION: 5 DAYS

COURSE OBJECTIVES

After completing this course, the student will be able to:

- Understand the different Access Control systems and how they should be implemented to protect the system and data using the different levels of confidentiality, integrity and availability
- Understand the processes necessary for working with management and information owners, custodians and users so that proper data classifications are defined. This will ensure the proper handling of all hard copy and electronic information as it is applied by the Security Operations and Administration.
- Identify, measure and control losses associated with adverse events, and review, analyze, select and evaluate safeguards for mitigating risk
- Identify how to handle Incident Response and Recovery using consistent, applied approaches including the use of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) concepts to mitigate damages, recover business operations, avoid critical business interruption, and apply emergency response and post-disaster recovery
- Identify and differentiate key cryptographic concepts and how to apply them, implement secure protocols, key management concepts, key administration and validation, and Public Key Infrastructure as it applies to securing communications in the presence of third parties
- Define and identify the Networks and Communications Security needed to secure network structure, data transmission methods, transport formats, and the security measures used to maintain integrity, availability, authentication and confidentiality of the information being transmitted
- Identify and define technical and non-technical attacks and how an organization can protect itself from these attacks including the concepts in endpoint device security, cloud infrastructure security, securing big data systems and securing virtual environments.

TARGET STUDENT

The training seminar is ideal for those working in positions such as but not limited to:

- Network Security Engineer
- Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator.

COURSE CONTENT

Lesson 1: Access Controls

Lesson 2: Security Operations and Administration

Lesson 3: Risk Identification, Monitoring and Analysis

Lesson 4: Incident Response and Recovery

Lesson 5: Cryptography

Lesson 6: Network and Communications Security

Lesson 7: Systems and Application Security