

C)SP: Security Principles

Course ID #: 7000-775-ZZ-Z

Hours: 35



Course Content

Course Description:

In this course, you will prepare for security across the entire environment including understanding risk management, identity and access control, network and data security. This is just a short list of everything that we cover within this course, which will include new technologies like IoT and cloud services. This course is intended to prepare you to become a benefit to any company that is attempting to improve its security posture!

Course Objectives:

Upon successful completion of this course, students will be able to:

- Competently take the C)SP exam
- Understand the principle security knowledge to keep companies' IP and IT infrastructure safe

Prerequisites:

- 12 Months of experience with server administration
- C)SA1, C)SA2, C)HT, C)OST and C)NP or Equivalent Knowledge

Target Audience:

- IT Professionals
- Server Administrators
- Virtualization and Cloud Administrators

Topics:

Module 1 – Introduction to IT Security

- Understanding Security
- Responsibilities
- Building a Security Program
- CIA Triad
- Governance, Risk, Compliance
- State of Security Today

Module 2 – Risk Management

- Risk Management
- Risk Assessment
- Types of Risk, Threats and Vulnerabilities
- Mitigating Attacks
- Discovering Vulnerabilities and Threats
- Responding to Risk



C)SP: Security Principles

Course ID #: 7000-775-ZZ-Z

Hours: 35

Module 3 – Understanding of Cryptography

- Understanding Cryptography
- Symmetric Encryption
- Asymmetric Encryption
- Hashing
- PKI
- Cryptography in Use

Module 4 – Understanding Identity and Access Management

- Identity Management
- Authentication Techniques
- Single Sign-on
- Access Control Monitoring

Module 5 – Managing Data Security

- Virtualization Principles
- Key Components Mapped to Cloud Layer
- Key Security Concerns
- Other Technologies Used in the Cloud
- The Layers
- Relevant CCM Controls

Module 6 – Data Security

- Different Types of Storage
- Encryption Options
- Data Management

Module 7 – Managing Server/Host Security

- The Operating Systems
- Hardening the OS
- Physical security
- Virtualization and Cloud Technologies

Module 8 – Application Security for Non-Developers

- Application Security Principle
- Software Development Life Cycle
- OWASP Top 10
- Hardening Web Applications
- Patch/Update/Configuration Management

Module 9 – Understanding Mobile Device Security (IoT)

- What Devices are we talking about?
- What is the risk?
- Hardening Mobile/IoT Devices
- Corporate Management

Module 10 – Managing Day to Day Security

- Company Responsibilities
- Product Management
- Business Continuity Basics
- Incident Response
- Why Train?

Module 11 – Understanding Compliance and Auditing

- Benefits of Compliance
- Assurance Frameworks
- What is Auditing

Labs: None.

Accreditations:



Register for this class by visiting us at:

www.tcworkshop.com or calling us at 800-639-3535