Certified Security Principles+ (CSP+)

Course Overview

This course will introduce students to IT security, as well as teach them about risk management, understanding of cryptography, understanding identity and access management, managing data security, managing network security, managing server/host security, application security for non-developers, understanding mobile device security (IoT), managing day to day security, and understanding compliance and auditing.

Course Introduction 16m
Course Introduction

Chapter 01 - Introduction to IT Security 1h 57m
Topic A: Navigate the PowerPoint Environment
Introduction to IT Security
Section 1 - Understanding Security
Section 2 - Responsibilities
Section 3 - Building a Security Program
Section 4 - CIA Triad
Section 5 - Governance, Risk, Compliance
Section 6 - State of Security Today

Chapter 02 - Risk Management 2h 44m
Risk Management
Section 1 - Risk Management
Section 2 - Risk Assessment
Section 3 - Types of Risk, Threats and Vulnerabilities
Section 4 - Mitigating Attacks
Section 5 - Discovering Vulnerabilities and Threats
Section 6 - Responding to Risk

Chapter 03 - Understanding of Cryptography 1h 35m
Understanding of Cryptography
Section 1 - Understanding Cryptography
Section 2 - Symmetric Encryption
Section 3 - Asymmetric Encryption
Section 4 - Hashing
Section 5 - PKI
Section 6 - Cryptography in Use

Chapter 04 - Understanding Identity and Access Management 1h 12m
Understanding Identity and Access Management
Section 1 - Identity Management
Section 2 - Authentication Techniques
Section 3 - Single Sign-on
Section 4 - Access Control Monitoring

Chapter 05 - Managing Data Security 1h 17m
Managing Data Security
Section 1 - Different Types of Storage
Section 2 - Encryption Options
Section 3 - Data Management

Chapter 06 - Managing Network Security 2h 13m
Managing Network Security
Section 1 - Protocols and Services
Section 2 - Network and Security Devices
Section 3 - Network Design
Section 4 - Wireless Networking

Chapter 07 - Managing Server/Host Security 1h 56m
Managing Server/Host Security
Section 1 - The Operating Systems
Section 2 - Hardening the OS
Section 3 - Physical Security

Chapter 08 - Application Security for Non-Developers 1h 22m
Application Security for Non-Developers
Section 1 - Application Security Principles
Section 2 - Software Development Life Cycle
Section 3 - OWASP Top 10
Section 4 - Hardening Web Applications
Section 5 - Patch/Update/Configuration Management

Chapter 09 - Understanding Mobile Device Security (IoT) 1h 4m
Understanding Mobile Device Security (IoT)
Section 1 - What devices are we talking about?
Section 2 - What is the risk?
Section 3 - Hardening Mobile/IoT Devices
Section 4 - Corporate Management

Chapter 10 - Managing Day to Day Security 2h 25m
Managing Day to Day Security
Section 1 - Company Responsibilities
Section 2 - Product Management
Section 3 - Business Continuity Basics
Section 4 - Incident Response
Section 5 - Why train?

Chapter 11 - Understanding Compliance and Auditing 57m
Understanding Compliance and Auditing
Section 1 - Benefits of Compliance
Section 2 - Assurance Frameworks
Section 3 - What is auditing?

Total Duration: 18h 57m