

# Table of Contents

## SYO-501

### **Part 1: Threats, Attacks and Vulnerabilities**

**Chapter 1:** Malware and Indicators of Compromise

**Chapter 2:** Attacks

**Chapter 3:** Threat Actors

**Chapter 4:** Vulnerability Scanning and Penetration Testing

**Chapter 5:** Vulnerabilities and Impacts

### **Part 2: Technologies and Tools**

**Chapter 6:** Network Components

**Chapter 7:** Security Tools and Technologies

**Chapter 8:** Troubleshoot Common Security Issues

**Chapter 9:** Deploy Mobile Devices Securely

**Chapter 10:** Implementing Secure Protocols

### **Part 3: Architecture and Design**

**Chapter 11:** Architecture Frameworks and Secure Network Architectures

**Chapter 12:** Secure Systems Design and Deployment

**Chapter 13:** Embedded Systems

**Chapter 14:** Application Development and Deployment

**Chapter 15:** Cloud and Virtualization

**Chapter 16:** Resiliency and Automation strategies

**Chapter 17:** Physical Security Controls

### **Part 4: Identity and Access Management**

**Chapter 18:** Identity, Access and Accounts

**Chapter 19:** Identity and Access Services

**Chapter 20:** Identity and Access Management Controls

### **Part 5: Risk Management**

**Chapter 21:** Policies, Plans and Procedures

**Chapter 22:** Risk Management and Business Impact Analysis Concepts

**Chapter 23:** Incident Response, Disaster Recovery and Continuity of Operation

**Chapter 24:** Digital forensics

**Chapter 25:** Compare and contrast various types of controls

**Chapter 26:** Data Security and Privacy Practices

### **Part 6: Cryptography and PKI**

**Chapter 27:** Cryptography Concepts

**Chapter 28:** Cryptography Algorithms

**Chapter 29:** Wireless Security

**Chapter 30:** Public Key Infrastructure