Course Introduction

Acknowledgements
Table of Contents
Getting Started
About This Course
About CompTIA Certifications

Module 1 / Threat Management 1

Module 1 / Unit 1
Cybersecurity Analysts

Cybersecurity Roles and Responsibilities
Frameworks and Security Controls
Risk Evaluation
Penetration Testing Processes

Module 1 / Unit 2
Reconnaissance Techniques

The Kill Chain
Open Source Intelligence
Social Engineering
Topology Discovery
Service Discovery
OS Fingerprinting

Module 1 / Summary
Threat Management 1

Module 2 / Vulnerability Management

Module 2 / Unit 1
Managing Vulnerabilities

Vulnerability Management Requirements
Asset Inventory
Data Classification
Vulnerability Management Processes
Vulnerability Scanners
Microsoft Baseline Security Analyzer
Vulnerability Feeds and SCAP
Configuring Vulnerability Scans
Vulnerability Scanning Criteria
Exploit Frameworks
Module 2 / Unit 2
Remediating Vulnerabilities

Analyzing Vulnerability Scans
Remediation and Change Control
Remediating Host Vulnerabilities
Remediating Network Vulnerabilities
Remediating Virtual Infrastructure Vulnerabilities

Module 2 / Unit 3
Secure Software Development

Software Development Lifecycle
Software Vulnerabilities
Software Security Testing
Interception Proxies
Web Application Firewalls
Source Authenticity
Reverse Engineering

Module 2 / Summary
Vulnerability Management

Module 3 / Threat Management 2

Module 3 / Unit 1
Security Appliances

Configuring Firewalls
Intrusion Detection and Prevention
Configuring IDS
Malware Threats
Configuring Anti-Virus Software
Sysinternals
Enhanced Mitigation Experience Toolkit

Module 3 / Unit 2
Logging and Analysis

Packet Capture
Packet Capture Tools
Monitoring Tools
Log Review and SIEM
SIEM Data Outputs
SIEM Data Analysis
Point-in-Time Data Analysis

Module 3 / Summary
Threat Management 2
Module 4 / Cyber Incident Response

Module 4 / Unit 1
Incident Response

Incident Response Processes
Threat Classification
Incident Severity and Prioritization
Types of Data

Module 4 / Unit 2
Forensics Tools

Digital Forensics Investigations
Documentation and Forms
Digital Forensics Crime Scenes
Digital Forensics Kits
Image Acquisition
Password Cracking
Analysis Utilities

Module 4 / Unit 3
Incident Analysis and Recovery

Analysis and Recovery Frameworks
Analyzing Network Symptoms
Analyzing Host Symptoms
Analyzing Data Exfiltration
Analyzing Application Symptoms
Using Sysinternals
Containment Techniques
Eradication Techniques
Validation Techniques
Corrective Actions

Module 4 / Summary
Cyber Incident Response

Module 5 / Security Architecture

Module 5 / Unit 1
Secure Network Design

Network Segmentation
Blackholes, Sinkholes, and Honeypots
System Hardening
Group Policies and MAC
Endpoint Security
Module 5 / Unit 2
Managing Identities and Access

Network Access Control
Identity Management
Identity Security Issues
Identity Repositories
Context-based Authentication
Single Sign-on and Federation
Exploiting Identities
Exploiting Web Browsers and Applications

Module 5 / Unit 3
Security Frameworks and Policies

Frameworks and Compliance
Reviewing Security Architecture
Procedures and Compensating Controls
Verifications and Quality Control
Security Policies and Procedures
Personnel Policies and Training

Module 5 / Summary
Security Architecture

Taking the Exam

Glossary

Index