

CompTIA CySA+

Course Outline

Module 1 – Threat Management 1

- **Cybersecurity Analysts**
 - Cybersecurity Roles and Responsibilities
 - Frameworks and Security Controls
 - Risk Evaluation
 - Penetration Testing Processes
- **Reconnaissance Techniques**
 - The Kill Chain
 - Open Source Intelligence
 - Social Engineering
 - Topology Discovery
 - Service Discovery
 - OS Fingerprinting

Module 2 – Threat Management 2

- **Security Appliances**
 - Configuring Firewalls
 - Intrusion Detection and Prevention
 - Configuring IDS
 - Malware Threats
 - Configuring Anti-virus Software
 - Sysinternals
 - Enhanced Mitigation Experience Toolkit
- **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 – Vulnerability Management

- **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
- **Remediating Vulnerabilities**
 - Analyzing Vulnerability Scans
 - Remediation and Change Control
 - Remediating Host Vulnerabilities
 - Remediating Network Vulnerabilities
 - Remediating Virtual Infrastructure Vulnerabilities
- **Secure Software Development**
 - Software Development Lifecycle
 - Software Vulnerabilities
 - Software Security Testing
 - Interception Proxies
 - Web Application Firewalls
 - Source Authenticity
 - Reverse Engineering

Module 4 – Cyber Incident Response

- **Incident Response**
 - Incident Response Processes
 - Threat Classification
 - Incident Severity and Prioritization
 - Types of Data
- **Forensics Tools**
 - Digital Forensics Investigations
 - Documentation and Forms
 - Digital Forensics Crime Scene
 - Digital Forensics Kits
 - Image Acquisition
 - Password Cracking
 - Analysis Utilities
- **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 5 – Security Architecture

- **Secure Network Design**
 - Network Segmentation
 - Blackholes, Sinkholes, and Honeypots
 - System Hardening

- Group Policies and MAC
 - Endpoint Security
- **Managing Identities and Access**
 - Network Access Control
 - Identity Management
 - Identity Security Issues
 - Identity Repositories
 - Context-based Authentication
 - Single Sign-On and Federations
 - Exploiting Identities
 - Exploiting Web Browsers and Applications
- **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