

CompTIA CySA+ (Cybersecurity Analyst) Course Outline

Duration: 40-50 Hours (Global Standards)

Level: Intermediate

Delivery Mode: Online/Offline

Certification: CompTIA CySA+

Global Exam Code: CS0-003 (Latest Version)

Module 1: Introduction to Threat Management

Duration: 3-5 Hours

- Overview of CompTIA CySA+ Certification and Exam Structure
 - Introduction to Threat Management in Cybersecurity
 - Key Concepts of Cyber Threats, Attacks, and Vulnerabilities
 - The Role of a Cybersecurity Analyst in an Organization
 - Types of Cybersecurity Threats:
 - Malware, Phishing, DDoS, Insider Threats, Advanced Persistent Threats (APT)
 - Understanding the Threat Landscape: National and Global Perspectives
-

Module 2: Security Operations and Monitoring

Duration: 6-8 Hours

- Security Operations Centers (SOCs) and Their Role in Cybersecurity
 - Monitoring Tools and Techniques for Security Analysts
 - SIEM (Security Information and Event Management) Systems
 - IDS/IPS (Intrusion Detection/Prevention Systems)
 - Log Management and Event Correlation
 - Real-Time Security Monitoring Techniques
 - Analyzing Network Traffic for Malicious Activities
 - Threat Hunting and Indicator of Compromise (IOC) Analysis
 - Hands-on Lab: Configuring and Using SIEM Tools for Monitoring
-

Module 3: Vulnerability Management

Duration: 6-8 Hours

- Introduction to Vulnerability Management and Scanning
 - Identifying Vulnerabilities in Networks, Systems, and Applications
 - Common Vulnerabilities and Exposure (CVE) Database
 - Conducting Vulnerability Assessments and Penetration Testing
 - Tools and Techniques for Vulnerability Scanning
 - Nessus, OpenVAS, Qualys
 - Prioritizing Vulnerabilities and Risk Mitigation Strategies
 - Patch Management and Security Updates
-

Module 4: Incident Response and Recovery

Duration: 6-8 Hours

- Incident Response Process: Detection, Containment, Eradication, Recovery
 - Understanding and Classifying Security Incidents
 - Incident Response Plan Development and Execution
 - Managing Security Incidents and Breaches
 - Hands-on Lab: Responding to Simulated Security Incidents
 - Post-Incident Activities: Root Cause Analysis and Reporting
 - Business Continuity Planning (BCP) and Disaster Recovery
-

Module 5: Compliance and Security Frameworks

Duration: 4-6 Hours

- Understanding Security Frameworks and Standards
 - NIST, ISO/IEC 27001, COBIT, CIS Controls
 - Regulatory Compliance Requirements
 - GDPR, HIPAA, PCI-DSS, SOX, FISMA
 - Data Privacy and Protection Regulations
 - Data Retention, Encryption, and Handling Sensitive Data
 - How Compliance Affects Security Practices and Cybersecurity Analysts' Roles
-

Module 6: Threat Intelligence and Analysis

Duration: 6-8 Hours

- The Importance of Threat Intelligence in Cybersecurity
 - Collecting, Analyzing, and Applying Threat Intelligence
 - Open-Source Intelligence (OSINT) and Threat Sharing Platforms
 - Threat Intelligence Platforms (TIPs) and Their Role in Security Operations
 - Types of Threat Intelligence: Tactical, Operational, Strategic
 - Understanding and Analyzing Cyber Threat Indicators
 - IOCs (Indicators of Compromise), TTPs (Tactics, Techniques, and Procedures)
 - Hands-on Lab: Analyzing and Sharing Threat Intelligence
-

Module 7: Network and System Security

Duration: 5-7 Hours

- Network Security Fundamentals for Cybersecurity Analysts
 - Network Architecture and Segmentation
 - Firewall, VPN, and Proxy Configuration
 - System Security: Hardening and Securing Operating Systems
 - OS Security for Windows, Linux, and MacOS
 - Security Configurations and Patch Management
 - Endpoint Security and Protection Strategies
 - Anti-virus, EDR (Endpoint Detection and Response), HIPS (Host Intrusion Prevention Systems)
 - Application Security and Secure Software Development
-

Module 8: Risk Management and Assessment

Duration: 5-7 Hours

- Introduction to Risk Management and Assessment
 - Risk Analysis: Likelihood vs. Impact
 - Risk Mitigation Strategies and Treatment
 - Conducting Risk Assessments for Systems, Networks, and Applications
 - Risk Management Frameworks (RMF) and Security Control Assessments
 - Asset Management and Threat Modeling Techniques
 - Calculating Risk Metrics: Risk Score, Impact, and Likelihood
 - Security Control Auditing
-

Module 9: Cybersecurity Tools and Technologies

Duration: 5-7 Hours

- Overview of Common Cybersecurity Tools for Analysts
 - Network Scanners, Vulnerability Scanners, and SIEM
 - Packet Sniffers: Wireshark, tcpdump
 - Network Traffic Analyzers
 - Security Automation and Orchestration Tools
 - SOAR (Security Orchestration, Automation, and Response)
 - Introduction to Cybersecurity Automation Tools (Ansible, Puppet, Chef)
 - Hands-on Lab: Using Cybersecurity Tools for Threat Hunting and Incident Response
-

Module 10: CySA+ Exam Review and Preparation

Duration: 3-4 Hours

- Review of Key CySA+ Exam Domains
 - Threat Management, Vulnerability Management, Incident Response
 - Security Operations and Monitoring, Compliance, and Risk Management
 - Practice Exam Questions and Case Studies
 - Exam Preparation Strategies and Tips
 - How to Register for the CompTIA CySA+ Exam
-

Module 11: CompTIA CySA+ Certification Exam

- Final Exam: **CompTIA CySA+ CS0-003**
- Post-Exam: Understanding Results and Career Opportunities