# CompTIA CySA+ (CS0-004)

# Training TOC

Duration:8 hours/day

Day 1: Cybersecurity Foundations & Threat Landscape

Objective: Build core understanding of security concepts and modern threats

1.1 Introduction to CySA+ (CS0-004)

- Exam objectives overview
- Security Operations Analyst role
- SOC structure and workflows

1.2 Core Security Concepts Refresher

- CIA triad & security principles
- Authentication, authorization, accounting (AAA)
- Security controls: preventive, detective, corrective

1.3 Threat Landscape

- Modern cyber threats (APT, ransomware, phishing)
- Malware types and behaviors
- Attack vectors and kill chain

1.4 Threat Intelligence Fundamentals

- Threat intelligence lifecycle

- Indicators of Compromise (IoC)
- Indicators of Attack (IoA)
- Threat intelligence sources (OSINT, dark web, internal logs)

Day 2: Security Monitoring & Data Collection

Objective: Understand log sources, SIEM, and monitoring tools

2.1 Security Monitoring Concepts

- Continuous monitoring principles
- SOC monitoring objectives

2.2 Log Management

- Types of logs (network, endpoint, application, firewall)
- Log formats (syslog, JSON, Windows Event Logs)

2.3 SIEM Fundamentals

- SIEM architecture and components
- Correlation rules
- Dashboards and alerting

2.4 Data Sources & Sensors

- IDS vs IPS
- EDR/XDR tools
- Network traffic analysis tools (Wireshark basics)

2.5 Alert Triage Basics

- Alert prioritization
- False positives vs false negatives
- Basic incident categorization

Day 3: Vulnerability Management & Analysis

Objective: Identify, assess, and prioritize vulnerabilities

3.1 Vulnerability Management Lifecycle

- Discovery → Assessment → Remediation → Verification

3.2 Vulnerability Scanning Tools

- Authenticated vs unauthenticated scans
- Tools overview (Nessus, OpenVAS concepts)

3.3 Vulnerability Scoring

- CVSS scoring system
- Risk vs severity vs impact

3.4 Attack Surface Analysis

- Asset inventory
- Exposure assessment

3.5 Malware & Behavioral Analysis Basics

- Static vs dynamic analysis
- Sandbox environments
- Fileless malware overview

Day 4: Incident Detection, Response & Recovery

Objective: Handle security incidents from detection to containment

4.1 Incident Response Lifecycle

- Preparation
- Detection & Analysis
- Containment
- Eradication
- Recovery
- Lessons learned

4.2 Incident Classification & Handling

- Incident severity levels
- Escalation procedures
- Communication flow in SOC

4.3 Digital Forensics Basics

- Evidence collection principles
- Chain of custody
- Volatile vs non-volatile data

4.4 Response Tools & Techniques

- Endpoint isolation

- Network containment strategies
- IOC-based investigation

4.5 Recovery & Post-Incident Activities

- System restoration
- Root cause analysis
- Reporting

Day 5: Security Architecture, Automation & Exam Preparation

Objective: Integrate knowledge and prepare for exam success

5.1 Security Architecture Concepts

- Network segmentation
- Zero Trust model
- Defense in depth

5.2 Automation & Orchestration

- SOAR concepts
- Playbooks and workflows
- Security automation use cases

5.3 Risk Management & Compliance

- Risk types (inherent, residual)
- Policies, procedures, and governance
- Compliance frameworks overview

## 5.4 Threat Hunting Basics

- Hypothesis-driven hunting
- Behavioral analytics
- MITRE ATT&CK framework overview