Document Generated: 11/08/2026

Learning Style: Virtual Classroom

Technology: CompTIA

Difficulty: Intermediate

Course Duration: 5 Days

Next Course Date: November 30, 2026

CompTIA CySA+



As attackers have learned to evade traditional signature-based solutions, such as firewalls and anti-virus software, an analytics-based approach within the IT security industry is increasingly important for organizations. CompTIA CySA+ applies behavioral analytics to networks to improve the overall state of security through identifying and combating malware and advanced persistent threats (APTs), resulting in an enhanced threat visibility across a broad attack surface. It will validate an IT professional’s ability to proactively defend and continuously improve

the security of an organization. CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

Course Objectives:

- Security Operations
- Security Monitoring and Log Analysis
- Threat Intelligence and Threat Hunting
- Vulnerability Management
- Vulnerability Assessment and Remediation
- Security Information and Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Network Traffic Analysis
- Incident Response and Management
- Digital Forensics and Evidence Collection
- Security Automation and Orchestration
- Risk Assessment and Mitigation
- Security Reporting and Communication
- Security Controls and Compliance

- Cybersecurity Frameworks and Attack Analysis

Audience:

- Cybersecurity Analysts
- SOC (Security Operations Center) Analysts
- Threat Intelligence Analysts
- Vulnerability Analysts
- Incident Response Analysts
- Security Engineers

Prerequisites:

While there is no required prerequisite, the CompTIA CySA+ certification is intended to follow CompTIA Security+ or equivalent experience. It is recommended for CompTIA CySA+ certification candidates to have the following:

- 3-4 years of hands-on information security or related experience
- Network+, Security+, or equivalent knowledge

Course Outline:

Module 1: Security Operations

- Security operations center (SOC) fundamentals.
- Security monitoring and log analysis.
- Security information and event management (SIEM).
- Endpoint detection and response (EDR).
- Security orchestration, automation, and response (SOAR).
- Network traffic monitoring and analysis.
- Security operations tools and technologies.

Module 2: Vulnerability Management

- Vulnerability scanning and assessment.
- Vulnerability identification and classification.
- Common Vulnerabilities and Exposures (CVE).
- Common Vulnerability Scoring System (CVSS).
- Vulnerability prioritization and remediation.
- Patch management and configuration management.

- Vulnerability assessment tools and reporting.

Module 3: Incident Response and Management

- Cyberattack methodologies and frameworks.
- MITRE ATT&CK framework.
- Cyber Kill Chain methodology.
- Diamond Model of Intrusion Analysis.
- Incident response lifecycle and procedures.
- Incident detection, analysis, and triage.
- Incident containment, eradication, and recovery.
- Digital forensics and evidence collection.
- Chain of custody and evidence preservation.
- Root cause analysis and post-incident reviews.

Module 4: Reporting and Communication

- Vulnerability assessment reporting.
- Incident response documentation.
- Security metrics and key performance indicators (KPIs).
- Risk assessment and executive reporting.
- Technical and non-technical stakeholder communication.
- Incident escalation procedures.
- Security findings and remediation recommendations.
- Compliance reporting and regulatory requirements.
- Security dashboards and reporting tools.

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges