# CompTIA Cybersecurity Analyst (CySA+) Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

The **training** is a globally recognised certification designed for **Cyber Security Professionals** responsible for threat detection, incident analysis, and security monitoring. The course focuses on proactive defence strategies, **Threat Intelligence**, **Threat Hunting**, **Vulnerability Management**, and **Incident Response** within modern enterprise environments.

Participants will learn how to identify malicious activity, analyse cyber threats, evaluate security risks, and respond effectively to security incidents using industry-standard tools and methodologies.

## Prerequisites

Recommended knowledge includes:

- **CompTIA Network+** level networking knowledge
- **CompTIA Security+** level security knowledge
- Basic to intermediate experience in **Cyber Security Operations**

## Who Should Attend

This course is ideal for:

- **Security Analysts**
- **SOC Analysts**
- **Incident Response Analysts**
- **Vulnerability Management Analysts**
- **Security Engineers**
- Professionals working within **Security Operations Centers (SOC)**
- IT professionals pursuing a cyber security career

## What You Will Learn

By the end of this training, you will have gained knowledge and skills in the following areas:

- Detect and analyse indicators of malicious activity.
- Apply **Threat Hunting** and **Threat Intelligence** methodologies.
- Prioritise and manage vulnerabilities effectively.
- Execute structured **Incident Response** procedures.
- Communicate security findings and vulnerability reports.
- Recommend security controls based on threat analysis.

## Training Outline

### Module 1: Vulnerability Management and Response

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- **Cyber Security Leadership** concepts
- Security control categories and frameworks
- **Patch Management** best practices
- Vulnerability response strategies

### Module 2: Threat Intelligence and Threat Hunting

- Understanding threat actors
- Identifying active threats
- **Threat Hunting** methodologies
- Threat intelligence analysis

### Module 3: System and Network Architecture

- Core architecture principles
- Network infrastructure concepts
- **Identity and Access Management (IAM)**
- Operational visibility and monitoring

### Module 4: Security Operations Improvement

- Leadership within security operations
- Security operations technologies
- Process optimisation strategies

### Module 5: Vulnerability Scanning Techniques

- Compliance requirements
- **Vulnerability Scanning** methodologies
- Advanced scanning considerations
- Security assessment tools

### Module 6: Vulnerability Analysis

- **CVSS** and vulnerability scoring systems
- Risk prioritisation frameworks
- Vulnerability context analysis

### Module 7: Vulnerability Reporting

- Effective security communication
- Technical reporting methods
- Action plan development
- Security reporting best practices

### Module 8: Incident Response Activities

- **Incident Response Planning**
- Incident lifecycle management
- Security event handling
- Response procedures and workflows

### Module 9: Incident Response Communication

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Communication planning
- Stakeholder engagement
- Incident analysis techniques
- Post-incident review processes

### Module 10: Identifying Malicious Activity

- Detection of malicious behaviour
- **MITRE ATT&CK** methodologies
- Threat detection techniques
- Security investigation tools

### Module 11: Analysing Suspicious Activity

- Network attack indicators
- Host-based attack indicators
- **Vulnerability Assessment Tools**
- Threat indicator analysis

### Module 12: Application Security Assessment

- Web application vulnerabilities
- **Cloud Security Vulnerabilities**
- Application security testing
- Modern attack scenarios

### Module 13: Scripting and Analysis Tools

- Scripting language fundamentals
- Security automation concepts
- Security analysis platforms
- Investigating suspicious activity

### Module 14: Application Security and Attack Mitigation

- **Secure Software Development Practices**
- Secure SDLC methodologies
- Application attack prevention techniques
- Security control implementation
- Strengthening defence-in-depth strategies