INFOSECTRAIN

CompTIA

CySA+ (CS0-003)

Training & Certification

OVERVIEW

The ***CompTIA CySA+ (Cybersecurity Analyst+) (CS0-003)*** certification training program from InfosecTrain focuses on cybersecurity's technical and hands-on aspects, encompassing cyber threats, secure network architecture, risk management, log analysis, configuration assessments, and more. Upon successful completion, individuals are equipped with the necessary knowledge and skills to effectively identify, analyze, and interpret indicators of malicious activity. They gain a comprehensive understanding of threat intelligence and management, enabling them to respond to various attacks and vulnerabilities proactively. Additionally, candidates learn incident response methodologies to handle security incidents and mitigate their impact efficiently.

Why CompTIA CySA+ Certification Training Course with InfosecTrain?

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our ***CompTIA CySA+ Certification Training Course*** will equip you with a comprehensive overview of essential topics in the field of cyber security.

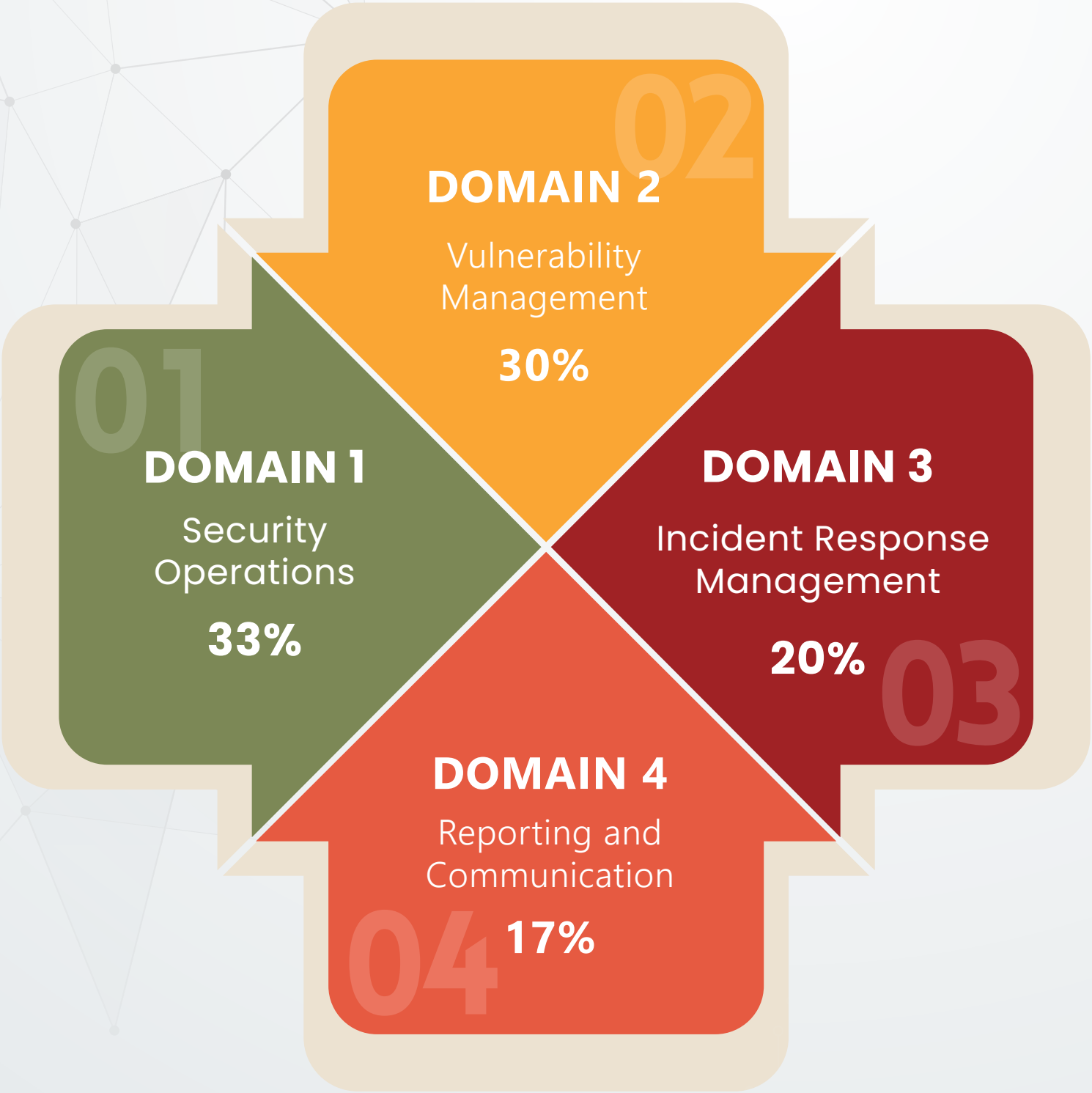
Here's what you get when you choose InfosecTrain as your learning partner :

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Post Training Support with No Expiry Date:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS or recorded sessions for post-training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.

Expert Career Guidance: Free Career Guidance and support from industry experts.

INFOSECTRAIN

CompTIA CySA+ Certification Exam Domains



Target Audience

- IT Security Analysts
- Vulnerability Analysts
- Threat Intelligence Analysts
- Anyone who is trying to get a better understanding of the concepts involved in conducting cybersecurity analysis

Pre-Requisite

- Basic knowledge of Network+, Security+, or equivalent discipline
- Minimum of 4 years of hands-on experience as an Incident Response Analyst or Security Operations Center (SOC) Analyst or similar domain

Exam Information

Exam Code	CS0-003
Number of Questions	Maximum of 85 questions
Type of Questions	Multiple-choice and Performance-based
Duration of Exam	165 minutes
Passing Score	750 (on a scale of 100-900)
Language	English, Japanese, Portuguese, and Spanish to follow

INFOSECTRAIN

Course Objectives

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence concepts
- Use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability management and incident response activities

INFOSECTRAIN

Course Content

Domain 1: Security Operations (33%)

1.1: Explain the Importance of System and Network Architecture Concepts in Security Operations

- Log Ingestion
  - > Time Synchronization
  - > Logging Levels

- Operating System (OS) Concepts
  - > Windows Registry
  - > System Hardening
  - > File Structure

- Configuration File Locations
  - > System Processes
  - > Hardware Architecture

- Infrastructure Concepts
  - > Serverless
  - > Virtualization
  - > Containerization

- Network Architecture
  - > On-Premises
  - > Cloud
  - > Hybrid
  - > Network Segmentation
  - > Zero Trust
  - > Secure Access Secure Edge (SASE)
  - > Software-Defined Networking (SDN)

- Identity and Access Management
  - > Multi Factor Authentication (MFA)
  - > Single Sign-On (SSO)
  - > Federation
  - > Privileged Access Management (PAM)
  - > Passwordless
  - > Cloud Access Security Broker (CASB)

- Encryption
  - > Public Key Infrastructure (PKI)
  - > Public Key Infrastructure (PKI)

- Sensitive Data Protection
  - > Data Loss Prevention (DLP)
  - > Personally Identifiable Information (PII)
  - > Cardholder Data (CHD)

1.2: Given a Scenario, Analyze Indicators of Potentially Malicious Activity

- Network-Related
  - > Bandwidth Consumption
  - > Beaconing
  - > Irregular Peer-to-Peer Communication
  - > Rogue Devices on the Network
  - > Scans/Sweeps
  - > Unusual Traffic Spikes
  - > Activity on Unexpected Ports

- Host-Related
  - > Processor Consumption
  - > Memory consumption
  - > Drive Capacity Consumption

- > Unauthorized Software
- > Malicious Processes
- > Unauthorized Changes
- > Unauthorized Privileges
- > Data Exfiltration
- > Abnormal OS Process Behavior
- > File System Changes or Anomalies
- > Registry Changes or Anomalies
- > Unauthorized Scheduled Tasks

- Application-Related
  - > Anomalous Activity
  - > Introduction of new Accounts
  - > Unexpected Output
  - > Unexpected Outbound Communication
  - > Service Interruption
  - > Application Logs

- Other
  - > Social Engineering Attacks
  - > Obfuscated Links

1.3: Given a Scenario, Use Appropriate Tools or Techniques to Determine Malicious Activity

- Tools
  - > Packet Capture
    - Wireshark
    - tcpdump
  - > Log Analysis/Correlation
    - Security Information and Event Management (SIEM)
    - Security Orchestration, Automation, and Response (SOAR)

> Endpoint Security
  - Endpoint Detection and Response (EDR)

> Domain Name Service (DNS) and Internet Protocol (IP) Reputation
  - WHOIS
  - AbuseIPDB

> File Analysis
  - Strings
  - VirusTotal

> Sandboxing
  - Joe Sandbox
  - Cuckoo Sandbox

- Common Techniques

> Pattern Recognition
  - Command and Control

> Interpreting Suspicious Commands

> Email Analysis
  - Header
  - Impersonation
  - DomainKeys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Sender Policy Framework (SPF)
  - Embedded Links

> File Analysis
  - Hashing

> User Behavior Analysis
  - Abnormal Account Activity
  - Impossible Travel

- Programming Languages/Scripting
  - > JavaScript Object Notation (JSON)
  - > Extensible Markup Language (XML)
  - > Python
  - > PowerShell
  - > Shell Script
  - > Regular Expressions

1.4: Compare and Contrast Threat-Intelligence and Threat-Hunting Concepts

- Threat Actors
  - > Advanced Persistent Threat (APT)
  - > Hacktivists
  - > Organized Crime
  - > Nation-State
  - > Script Kiddie
  - > Insider Threat
    - Intentional
    - Unintentional
  - > Supply Chain

- Tactics, Techniques, and Procedures (TTP)
- Confidence Levels
  - > Timeliness
  - > Relevancy
  - > Accuracy

- Collection Methods and Sources
  - > Open Source
    - Social Media
    - Blogs/Forums
    - Government Bulletins
    - Computer Emergency Response Team (CERT)

- Cybersecurity Incident Response Team (CSIRT)
- Deep/Dark Web

> Closed Source
- Paid Feeds
- Information Sharing Organizations
- Internal Sources

- Threat Intelligence Sharing
> Incident Response
> Vulnerability Management
> Risk Management
> Security Engineering
> Detection and Monitoring
- Intentional
- Unintentional

- Threat Hunting
> Indicators of compromise (IoC)
- Collection
- Analysis
- Application

> Focus areas
- Configurations/Misconfigurations
- Isolated Networks
- Business-Critical Assets and Processes

> Active Defense
> Honeypot

1.5: Explain the Importance of Efficiency and Process Improvement in Security Operations

- Standardize Processes
  - > Identification of Tasks Suitable for Automation
    - Repeatable/do not Require Human Interaction
  - > Team Coordination to Manage and Facilitate Automation

- Streamline Operations
  - > Automation and Orchestration
    - Security Orchestration, Automation, and Response (SOAR)
  - > Orchestrating Threat Intelligence Data
    - Data Enrichment
    - Threat Feed Combination
  - > Minimize Human Engagement

- Technology and Tool Integration
  - > Application Programming Interface (API)
  - > Webhooks
  - > Plugins

- Single Pane of Glass

Domain 2: Vulnerability Management (30%)

2.1: Given a Scenario, Implement Vulnerability Scanning Methods and Concepts

- Asset Discovery
  - > Map Scans
  - > Device Fingerprinting

- Special Considerations
  - > Scheduling
  - > Operations
  - > Performance
  - > Sensitivity Levels
  - > Segmentation
  - > Regulatory Requirements

- Internal vs. External Scanning
- Agent vs. Agentless
- Credentialed vs. Non-Credentialed
- Passive vs. Active
- Static vs. Dynamic
  - > Reverse Engineering
  - > Fuzzing

- Critical Infrastructure
  - > Operational Technology (OT)
  - > Industrial Control Systems (ICS)
  - > Supervisory Control and Data Acquisition (SCADA)

- Security Baseline Scanning
- Industry Frameworks

- Payment Card Industry Data Security Standard (PCI DSS)
- Center for Internet Security (CIS) Benchmarks
- Open Web Application Security Project (OWASP)
- International Organization for Standardization (ISO) 27000 Series

2.2: Given a Scenario, Analyze Output from Vulnerability Assessment Tools

- Tools
  - Network Scanning and Mapping
    - Angry IP Scanner
    - Maltego
  - Web Application Scanners
    - Burp Suite
    - Zed Attack Proxy (ZAP)
    - Arachni
    - Nikto
  - Vulnerability Scanners
    - Nessus
    - OpenVAS
  - Debuggers
    - Immunity Debugger
    - GNU Debugger (GDB)
  - Multipurpose
    - Nmap
    - Metasploit Framework (MSF)
    - Recon-ng
  - Cloud Infrastructure Assessment Tools
    - Scout Suite
    - Prowler
    - Pacu

2.3: Given a Scenario, Analyze Data to Prioritize Vulnerabilities

- Common Vulnerability Scoring System (CVSS) Interpretation
  - > Attack Vectors
  - > Attack Complexity
  - > Privileges Required
  - > User Interaction
  - > Scop
  - > Impact
    - Confidentiality
    - Integrity
    - Availability

- Context Awareness
  - > Internal
  - > External
  - > Isolated

- Exploitability/Weaponization
- Asset Value
- Zero-Day

2.4: Given a Scenario, Recommend Controls to Mitigate Attacks and Software Vulnerabilities

- Cross-Site Scripting
  - > Reflected
  - > Persistent

- Overflow Vulnerabilities
  - > Buffer
  - > Integer
  - > Heap
  - > Stack

- Data Poisoning
- Broken Access Control
- Cryptographic Failures
- Injection Flaws
- Cross-Site Request Forgery
- Directory Traversal
- Insecure Design
- Security Misconfiguration
- End-of-life or Outdated Component
- Identification and Authentication Failures
- Server-side Request Forgery
- Remote Code Execution
- Privilege Escalation
- Local File Inclusion (LFI)/Remote File Inclusion (RFI)

2.5: Explain Concepts Related to Vulnerability Response, Handling, and Management

- Compensating Control
- Control Types
  - > Managerial
  - > Operational
  - > Technical
  - > Preventative
  - > Detective
  - > Responsive
  - > Corrective

- Patching and Configuration Management
  - > Testing
  - > Implementation
  - > Rollback
  - > Validation

- Maintenance Windows
- Exceptions
- Risk Management Principles
  - > Accept
  - > Transfer
  - > Avoid
  - > Mitigate

- Policies, Governance, and Service- Level Objectives (SLOs)
- Prioritization and Escalation
- Attack Surface Management
  - > Edge Discovery
  - > Passive Discovery
  - > Security Controls Testing
  - > Penetration Testing and Adversary Emulation
  - > Bug bounty
  - > Attack Surface Reduction

- Secure Coding Best Practices
  - > Input Validation
  - > Output Encoding
  - > Session Management
  - > Authentication
  - > Data Protection
  - > Parameterized Queries

- Secure Software Development Life Cycle (SDLC)
- Threat Modeling

Domain 3: Incident Response Management (20%)

3.1: Explain Concepts Related to Attack Methodology Frameworks

- Cyber Kill Chain
  - > Reconnaissance
  - > Weaponization
  - > Delivery
  - > Exploitation
  - > Installation
  - > Command and Control (C2)
  - > Actions and objective

- Diamond Model of Intrusion Analysis
  - > Adversary
  - > Victim
  - > Infrastructure
  - > Capability

- MITRE ATT&CK
- Open Source Security Testing Methodology Manual (OSSTMM)
- OWASP Testing Guide

3.2: Given a Scenario, Perform Incident Response Activities

- Detection and Analysis
  - > IoC
  - > Evidence Acquisitions
    - Chain of Custody
    - Validating Data Integrity
    - Preservation
    - Legal hold
  - > Data and Log Analysis

- Containment, Eradication, and Recovery
  - > Scope
  - > Impact
  - > Isolation
  - > Remediation
  - > Re-Imaging
  - > Compensating Controls

3.3: Explain the Preparation and Post-Incident Activity Phases of the Incident Management Life Cycle

- Preparation
  - > Incident Response Plan
  - > Tools
  - > Playbooks
  - > Tabletop
  - > Training
  - > Business Continuity (BC)/ Disaster Recovery (DR)

- Post-Incident Activity
  - > Forensic Analysis
  - > Root Cause Analysis
  - > Lessons Learned

Domain 4: Reporting and Communication (17%)

4.1: Explain the Importance of Vulnerability Management Reporting and Communication

- Vulnerability Management Reporting
  - > Vulnerabilities
  - > Affected Hosts
  - > Risk Score
  - > Mitigation
  - > Recurrence
  - > Prioritization

- Compliance Reports
- Action Plans
  - > Configuration Management
  - > Patching
  - > Compensating Controls
  - > Awareness, Education, and Training
  - > Changing Business Requirements

- Inhibitors to Remediation
  - > Memorandum of Understanding (MOU)
  - > Service-Level Agreement (SLA)
  - > Organizational Governance
  - > Business Process Interruption
  - > Degrading Functionality
  - > Legacy Systems
  - > Proprietary systems

- Metrics and Key Performance Indicators (KPIs)
  - > Trends
  - > Top 10 Critical Vulnerabilities and Zero-days
  - > SLOs
- Stakeholder Identification and Communication

4.2: Explain the Importance of Incident Response Reporting and Communication

- Stakeholder Identification and Communication
- Incident Declaration and Escalation
- Incident Response Reporting
  - > Executive summary
  - > Who, What, When, Where, and Why
  - > Recommendations
  - > Timeline
  - > Impact

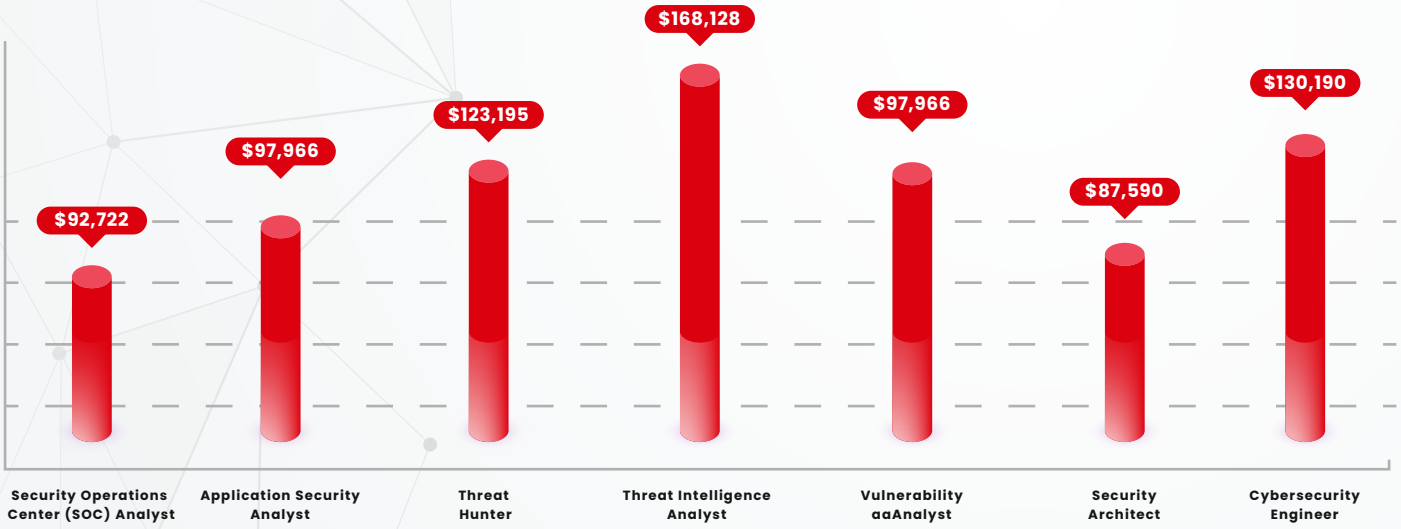
- > Scope
- > Evidence

- Communications
  - > Legal
  - > Public Relations
    - Customer Communication
    - Media
  - > Regulatory reporting
  - > Law enforcement

- Root cause Analysis
- Lessons Learned
- Metrics and KPIs
  - > Mean Time to Detect
  - > Mean Time to Respond
  - > Mean Time to Remediate
  - > Alert Volume

INFOSECTRAIN

Course **Benefits**



HIRING COMPANIES

Source: Indeed, Glassdoor

FOUND THIS USEFUL?

To Get More Insights Through Our FREE

Courses | Workshops | eBooks | Checklists | Mock Tests

INFOSECTRAIN