INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

CompTIA CySA+ Boot Camp

Learn how to use behavioral analytics to prevent, detect and combat cyber threats! This boot camp provides the most comprehensive approach to earning CompTIA's intermediate-level Cybersecurity Analyst (CySA+) certification.

Course description

Infosec's authorized CompTIA CySA+ Boot Camp is a comprehensive five-day training that teaches you the knowledge and skills required to configure and use the latest industry-standard threat detection tools. You'll learn how to perform data analysis to identify vulnerabilities and expose cyber threats — with the ultimate goal of helping organizations protect and secure their applications and systems.

You'll leave with the knowledge required to pass your CySA+ exam and the behavioral analytics skills needed to provide increased visibility into cyber threats.

Who should attend

- Cybersecurity analysts
- Vulnerability analysts
- Cybersecurity specialists
- Anyone interested in builiding their skills as an analyst

Boot camp at a glance

What you'll learn

- ✓ Analyze data to identify vulnerabilities, threats and risks
- ✓ Configure and use threat detection tools
- ✓ Secure and protect applications and systems

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Five days of live, expert CySA+ instruction
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Knowledge Transfer Guarantee

Prerequisites

Although not required, CompTIA recommends three to four years of hands-on information security experience, as well as a Security+ certification or equivalent knowledge.

CySA+ objectives

This CySA+ exam (CS0-002) was updated in 2020 to align with current cybersecurity analyst work roles. The exam is focused on five domain areas:

- Threat and vulnerability management
- Software and systems security
- Security operations and monitoring
- Incident response
- Compliance and assessment

What you'll learn

- Applying environmental reconnaissance techniques and analyzing the results
- Implementing or recommending responses to network-based threats
- Implementing a vulnerability management process
- Identifying common vulnerabilities and analyzing vulnerability scans
- Analyzing threat data to determine the impact of threats
- Preparing toolkits and supporting incident response
- Using data to recommend remediation of security issues

Industry-leading exam pass rates

Infosec's courseware materials are always up to date and synchronized with the latest CySA+ exam objectives. Our industry-leading curriculum and expert instructors have led to the highest pass rates in the industry. More than 93% of Infosec students pass their certification exams on their first attempt.

Attention DoD Information Assurance workers! Meets 8570.1 requirements

The CySA+ certification meets 8570.1 mandate and is approved for five job categories, including:

- Information Assurance Technician Level II
- Cybersecurity Service Provider (CSSP) – Analyst
- CSSP – Incident Respond
- CSSP – Infrastructure Support
- CSSP – Auditor

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

The course was very good, it gave me the information I needed in a direct and sufficient manner. Our instruction was thorough, entertaining and used real life examples to convey the subject matter. He made a challenging situation enjoyable and fun.

Timothy Twyman
Department of Defense

Infosec clearly cared that all participants learn the course material. Our instructor could pick up on the differences between the participants, e.g., learning style, and adjust his interaction to best communicate the material to all participants. He was diligent about making sure no one "got left behind." I could not imagine a better class!

Paul Gatewood
Deloitte Consulting, LLC

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions

CompTIA CySA+ details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Threat and vulnerability management	Software and systems security	Security operations and monitoring	Incident response	Compliance and assessment
Afternoon session	Threat and vulnerability management (cont.)	Software and systems security (cont.)	Security operations and monitoring (cont.)	Incident response (cont.)	Exam review Take CS0-002 exam
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth CySA+ prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Threat and vulnerability management

1.1 Explain the importance of threat data and intelligence

- Intelligence sources
  - Open-source intelligence
  - Proprietary/closed-source intelligence
  - Timeliness
  - Relevancy
  - Accuracy
- Confidence levels
- Indicator management
  - Structured Threat Information eXpression (STIX)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - OpenIoC
- Threat classification
  - Known threat vs. unknown threat
  - Zero-day
  - Advanced persistent threat
- Threat actors
  - Nation-state
  - Hacktivist
  - Organized crime
  - Insider threat
    - Intentional
    - Unintentional
- Intelligence cycle
  - Requirements
  - Collection
  - Analysis
  - Dissemination
  - Feedback
- Commodity malware
- Information sharing and analysis communities
  - Healthcare

- Financial
- Aviation
- Government
- Critical infrastructure

1.2 Given a scenario, utilize threat intelligence to support organizational security

- Attack frameworks
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Kill chain
- Threat research
  - Reputational
  - Behavioral
  - Indicator of compromise (IoC)
  - Common vulnerability scoring system (CVSS)
- Threat modeling methodologies
  - Adversary capability
  - Total attack surface
  - Attack vector
  - Impact
  - Likelihood
- Threat intelligence sharing with supported functions
  - Incident response
  - Vulnerability management
  - Risk management
  - Security engineering
  - Detection and monitoring

1.3 Given a scenario, perform vulnerability management activities

- Vulnerability identification
  - Asset criticality
  - Active vs. passive scanning
  - Mapping/enumeration
- Validation
  - True positive
  - False positive
  - True negative
  - False negative
- Remediation/mitigation
  - Configuration baseline
  - Patching
  - Hardening
  - Compensating controls
  - Risk acceptance
  - Verification of mitigation
- Scanning parameters and criteria
  - Risks associated with scanning activities
  - Vulnerability feed
  - Scope
  - Credentialed vs. non-credentialed
  - Server-based vs. agent-based
  - Internal vs. external
  - Special considerations
    - Types of data
    - Technical constraints
    - Workflow
    - Sensitivity levels
    - Regulatory requirements
    - Segmentation
    - Intrusion prevention system (IPS), intrusion detection system (IDS) and firewall settings

1.4 Given a scenario, analyze the output from common vulnerability assessment tools

- Web application scanner
  - OWASP Zed Attack Proxy (ZAP)
  - Burp suite
  - Nikto
  - Arachni
- Infrastructure vulnerability scanner
  - Nessus
  - OpenVAS
  - Qualys
- Software assessment tools and techniques
  - Static analysis
  - Dynamic analysis
  - Reverse engineering
  - Fuzzing

- Enumeration
  - Nmap
  - hping
  - Active vs. passive
  - Responder
- Wireless assessment tools
  - Aircrack-ng
  - Reaver
  - oclHashcat
- Cloud infrastructure assessment tools
  - ScoutSuite
  - Prowler
  - Pacu

1.5 Explain the threats and vulnerabilities associated with specialized technology

- Mobile
- Internet of Things (IoT)
- Embedded
- Real-time operating system (RTOS)
- System-on-Chip (SoC)
- Field programmable gate array (FPGA)
- Physical access control
- Building automation systems
- Vehicles and drones
  - CAN bus
- Workflow and process automation systems
- Industrial control system
- Supervisory control and data acquisition (SCADA)
  - Modbus

1.6 Explain the threats and vulnerabilities associated with operating in the cloud

- Cloud service models
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Cloud deployment models
  - Public
  - Private
  - Community
  - Hybrid
- Function as a Service (FaaS)/ serverless architecture
- Infrastructure as code (IaC)
- Insecure application programming interface (API)
- Improper key management
- Unprotected storage
- Logging and monitoring
  - Insufficient logging and monitoring
  - Inability to access

1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities

- Attack types
  - Extensible markup language (XML) attack
  - Structured query language (SQL) injection
  - Overflow attack
    - Buffer
    - Integer
    - Heap
  - Remote code execution
  - Directory traversal
  - Privilege escalation
  - Password spraying
  - Credential stuffing
  - Impersonation
  - Man-in-the-middle attack
  - Session hijacking
  - Rootkit
  - Cross-site scripting
    - Reflected
    - Persistent
    - Document object model (DOM)
- Vulnerabilities
  - Improper error handling
  - Dereferencing
  - Insecure object reference
  - Race condition
  - Broken authentication
  - Sensitive data exposure
  - Insecure components

- Insufficient logging and monitoring
- Weak or default configurations
- Use of insecure functions
  - strcpy

Software and systems security

2.1 Given a scenario, apply security solutions for infrastructure management

- Cloud vs. on-premises
- Asset management
  - Asset tagging
- Segmentation
  - Physical
  - Virtual
  - Jumpbox
  - System isolation
    - Air gap
- Network architecture
  - Physical
  - Software-defined
  - Virtual private cloud (VPC)
  - Virtual private network (VPN)
  - Serverless
- Change management
- Virtualization
  - Virtual desktop infrastructure (VDI)
- Containerization
- Identity and access management
  - Privilege management
  - Multifactor authentication (MFA)
  - Single sign-on (SSO)
  - Federation
  - Role-based
  - Attribute-based
  - Mandatory
  - Manual review
- Cloud access security broker (CASB)
- Honeypot
- Monitoring and logging
- Encryption
- Certificate management
- Active defense

2.2 Explain software assurance best practices

- Platforms
  - Mobile
  - Web application
  - Client/server
  - Embedded
  - System-on-chip (SoC)
  - Firmware
- Software development life cycle (SDLC) integration
- DevSecOps
- Software assessment methods
  - User acceptance testing
  - Stress test application
  - Security regression testing
  - Code review
- Secure coding best practices
  - Input validation
  - Output encoding
  - Session management
  - Authentication
  - Data protection
  - Parameterized queries
- Static analysis tools
- Dynamic analysis tools
- Formal methods for verification of critical software
- Service-oriented architecture
  - Security Assertions
- Markup Language (SAML)
  - Simple Object Access Protocol (SOAP)
  - Representational State Transfer (REST)
  - Microservices

2.3 Explain hardware assurance best practices

- Hardware root of trust
  - Trusted platform module (TPM)
  - Hardware security module (HSM)
- eFuse

- Unified Extensible Firmware Interface (UEFI)
- Trusted foundry
- Secure processing
  - Trusted execution
  - Secure enclave
  - Processor security extensions
  - Atomic execution
- Anti-tamper
- Self-encrypting drive
- Trusted firmware updates
- Measured boot and attestation
- Bus encryption

Security operations and monitoring

3.1 Given a scenario, analyze data as part of security monitoring activities

- Heuristics
- Trend analysis
- Endpoint
  - Malware
    - Reverse engineering
  - Memory
  - System and application behavior
    - Known-good behavior
    - Anomalous behavior
    - Exploit techniques
  - File system
  - User and entity behavior analytics (UEBA)
- Network
  - Uniform Resource Locator (URL) and domain name system (DNS) analysis
    - Domain generation algorithm
  - Flow analysis
  - Packet and protocol analysis
    - Malware
- Log review
  - Event logs
  - Syslog
  - Firewall logs
  - Web application firewall (WAF)
  - Proxy
  - Intrusion detection system (IDS)/ Intrusion prevention system (IPS)
- Impact analysis
  - Organization impact vs. localized impact
  - Immediate vs. total
- Security information and event management (SIEM) review
  - Rule writing
  - Known-bad Internet protocol (IP)
  - Dashboard
- Query writing
  - String search
  - Script
  - Piping
- E-mail analysis
  - Malicious payload
  - Domain Keys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Sender Policy Framework (SPF)
  - Phishing
  - Forwarding
  - Digital signature
  - E-mail signature block
  - Embedded links
  - Impersonation
  - Header

3.2 Given a scenario, implement configuration changes to existing controls to improve security

- Permissions
- Whitelisting
- Blacklisting
- Firewall
- Intrusion prevention system (IPS) rules
- Data loss prevention (DLP)
- Endpoint detection and response (EDR)
- Network access control (NAC)
- Sinkholing
- Malware signatures

    - Development/rule writing
- Sandboxing
- Port security

3.3 Explain the importance of proactive threat hunting

- Establishing a hypothesis
- Profiling threat actors and activities
- Threat hunting tactics
    - Executable process analysis
- Reducing the attack surface area
- Bundling critical assets
- Attack vectors
- Integrated intelligence
- Improving detection capabilities

3.4 Compare and contrast automation concepts and technologies

- Workflow orchestration
    - Security Orchestration, Automation, and Response (SOAR)
- Scripting
- Application programming interface (API) integration
- Automated malware signature creation
- Data enrichment
- Threat feed combination
- Machine learning
- Use of automation protocols and standards
    - Security Content Automation Protocol (SCAP)
- Continuous integration
- Continuous deployment/delivery

Incident response

4.1 Explain the importance of the incident response process

- Communication plan
    - Limiting communication to trusted parties
    - Disclosing based on regulatory/ legislative requirements
    - Preventing inadvertent release of information
    - Using a secure method of communication
    - Reporting requirements
- Response coordination with relevant entities
    - Legal
    - Human resources
    - Public relations
    - Internal and external
    - Law enforcement
    - Senior leadership
    - Regulatory bodies
- Factors contributing to data criticality
    - Personally identifiable information (PII)
    - Personal health information (PHI)
    - Sensitive personal information (SPI)
    - High value asset
    - Financial information
    - Intellectual property
    - Corporate information

4.2 Given a scenario, apply the appropriate incident response procedure

- Preparation
    - Training
    - Testing
    - Documentation of procedures
- Detection and analysis
    - Characteristics contributing to severity level classification
    - Downtime
    - Recovery time
    - Data integrity
    - Economic
    - System process criticality
    - Reverse engineering
    - Data correlation
- Containment
    - Segmentation
    - Isolation
- Eradication and recovery

- Vulnerability mitigation
- Sanitization
- Reconstruction/reimaging
- Secure disposal
- Patching
- Restoration of permissions
- Reconstitution of resources
- Restoration of capabilities and services
- Verification of logging/communication to security monitoring

- Post-incident activities
  - Evidence retention
  - Lessons learned report
  - Change control process
  - Incident response plan update
  - Incident summary report
  - IoC generation
  - Monitoring

4.3 Given an incident, analyze potential indicators of compromise

- Network-related
  - Bandwidth consumption
  - Beaconing
  - Irregular peer-to-peer communication
  - Rogue device on the network
  - Scan/sweep
  - Unusual traffic spike
  - Common protocol over non-standard port
- Host-related
  - Processor consumption
  - Memory consumption
  - Drive capacity consumption
  - Unauthorized software
  - Malicious process
  - Unauthorized change
  - Unauthorized privilege
  - Data exfiltration
  - Abnormal OS process behavior
  - File system change or anomaly
  - Registry change or anomaly
  - Unauthorized scheduled task
- Application-related
  - Anomalous activity
  - Introduction of new accounts
  - Unexpected output
  - Unexpected outbound communication
  - Service interruption
  - Application log

4.4 Given a scenario, utilize basic digital forensics techniques

- Network
  - Wireshark
  - tcpdump
- Endpoint
  - Disk
  - Memory
- Mobile
- Cloud
- Virtualization
- Legal hold
- Procedures
- Hashing
  - Changes to binaries
- Carving
- Data acquisition

Compliance and assessment

5.1 Understand the importance of data privacy and protection

- Privacy vs. security
- Non-technical controls
  - Classification
  - Ownership
  - Retention
  - Data types
  - Retention standards
  - Confidentiality
  - Legal requirements
  - Data sovereignty

- Data minimization
- Purpose limitation
- Non-disclosure agreement (NDA)

- Technical controls
  - Encryption
  - Data loss prevention (DLP)
  - Data masking
  - Deidentification
  - Tokenization
  - Digital rights management (DRM)
    - Watermarking
  - Geographic access requirements
  - Access controls

5.2 Given a scenario, apply security concepts in support of organizational risk mitigation

- Business impact analysis
- Risk identification process
- Risk calculation
  - Probability
  - Magnitude
- Communication of risk factors
- Risk prioritization
  - Security controls
  - Engineering tradeoffs
- Systems assessment
- Documented compensating controls
- Training and exercises
  - Red team
  - Blue team
  - White team
  - Tabletop exercise
- Supply chain assessment
  - Vendor due diligence
  - Hardware source authenticity

5.3 Explain the importance of frameworks, policies, procedures and controls

- Frameworks
  - Risk-based
  - Prescriptive
- Policies and procedures
  - Code of conduct/ethics
  - Acceptable use policy (AUP)
  - Password policy
  - Data ownership
  - Data retention
  - Account management
  - Continuous monitoring
  - Work product retention
- Category
  - Managerial
  - Operational
  - Technical
- Control type
  - Preventative
  - Detective
  - Corrective
  - Deterrent
  - Compensating
  - Physical
- Audits and assessments
  - Regulatory
  - Compliance

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC