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+ (CS0-003) exam and the behavioral analytics skills needed to provide increased visibility into cyber threats.

Who should attend

- Cybersecurity and vulnerability analysts
- Cybersecurity specialists
- SOC staff
- Cyber Threat Hunting Professionals
- Security managers and leaders
- 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+ (CS0-003) 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+ (CS0-003) objectives

This CySA+ exam (CS0-003) was updated in 2023 to align with current cybersecurity analyst work roles. The exam is focused on four domain areas:

- Security Operations
- Vulnerability Management
- Incident Response and Management
- Reporting and Communication

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 5 job categories, including:

- Information Assurance Technical (IAT) level 2
- CSSP Analyst
- CSSP Infrastructure Support
- CSSP Incident Responder
- 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	Course Introductions Security Operations	Vulnerability Management	Incident Response and Management	Reporting and Communication	Domain Wrap-up and Review Exam Tips
Afternoon session	Security Operations (Cont)	Vulnerability Management (cont.)	Incident Response and Management (cont.)	Reporting and Communication (cont.)	Exam review Take CS0-003 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

1.0 Security Operations

- 1.1 System and network architecture concepts in security operations
- 1.2 Analyzing indicators of potentially malicious activity
- 1.3 Tools or techniques for determining malicious activity
- 1.4 Threat-intelligence and threat-hunting concepts
- 1.5 Efficiency and process improvement in security operations

2.0 Vulnerability Management

- 2.1 implementing vulnerability scanning methods and concepts
- 2.2 Analyzing outputs from vulnerability assessment tools
- 2.3 Analyzing data to prioritize vulnerabilities
- 2.4 Recommending controls to mitigate attacks and software vulnerabilities.
- 2.5 Concepts in vulnerability response, handling, and management.

3.0 Incident Response and Management

- 3.1 Concepts related to attack Methodology frameworks.
- 3.2 Performing incident response activities
- 3.3 preparation and post-incident activity phases of the incident management life cycle.

4.0 Reporting and Communication

- 4.1 Importance of vulnerability management reporting and communication.
- 4.2 Importance of incident response reporting and communication.