ACTIVE CLEARANCE · MISSION: CERTIFICATION

FREE PREVIEW

CLEARED GOVTECH PARTNERS

CompTIA CySA+ CS0-003

Exam Preparation Booklet — Free Preview

300 scenario questions · full answer key · glossary
study plan · career roadmap · exam-day strategy · glossary quiz

Prepared for our transitioning servicemembers and veterans.
Aligned to the current CS0-003 exam objectives. · This free preview contains a sample of the full 300-question booklet.

CONTENTS

What’s in this preview

Welcome ..... **incl.**

Exam at a glance ..... **incl.**

Visual reference — The Incident Response Lifecycle ..... **incl.**

Sample questions — Security Operations ..... **incl.**

Sample answer key & explanations ..... **incl.**

Unlock the full booklet ..... **incl.**

In the full booklet — not in this preview

All 300 scenario questions across every domain ..... LOCKED

Full answer keys with exam cues for every question ..... LOCKED

8-week study schedule & recommended resources ..... LOCKED

Career roadmap, acronym glossary & glossary quiz ..... LOCKED

Exam-day quick reference & funding guide ..... LOCKED

WELCOME

This Is the Analyst’s Chair.

CySA+ is where you stop memorizing definitions and start making calls. It is the defensive, operational credential — reading logs, triaging alerts, prioritizing vulnerabilities, running an incident, and writing it up. It is the DoD 8140 baseline for CSSP Analyst, Infrastructure Support, and Incident Responder roles, which makes it one of the most directly hireable certs in the cleared SOC market.

The exam is hands-on and judgment-heavy. A single IP touches 340 accounts with one attempt each; a host beacons out every 60 seconds; an email fails SPF and DKIM with your CEO’s name on it. The question is never ‘what is this term’ — it is ‘what is happening, and what do you do next.’ That is the analyst’s craft, and it is what we drill.

If you ran intel, comms, or operations in uniform, this is the closest civilian analog to that work. You already know how to read a picture from incomplete signals and act on it. Let’s point that instinct at a SOC console.

— The team at Cleared GovTech Partners

BEFORE YOU BEGIN

The CySA+ (CS0-003) exam at a glance

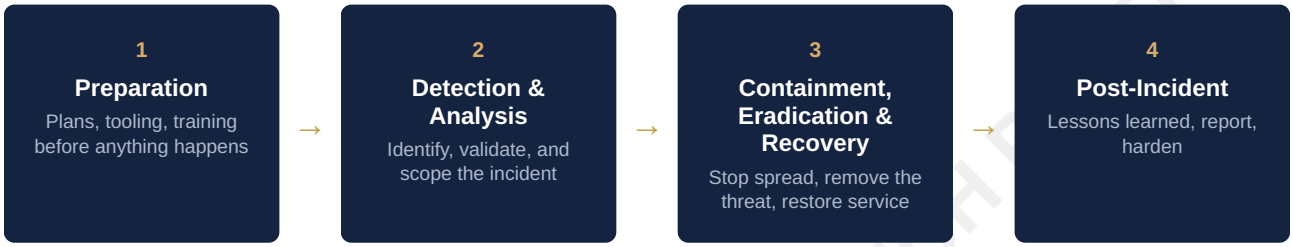
Exam code	CS0-003 (CompTIA Cybersecurity Analyst — CySA+)
Format	Up to 85 questions — multiple-choice and performance-based (PBQs)
Time limit	165 minutes
Passing score	750 on a scale of 100–900 (about 83%)
Structure	Four domains — weighted, analyst-focused, hands-on
Eligibility	No required prerequisite; Network+, Security+, and ~4 years of hands-on security experience are recommended
Renewal	Valid 3 years; renew with 60 CEUs (or re-take the current exam)
DoD value	DoD 8570/8140 approved — a baseline for CSSP Analyst, CSSP Infrastructure Support, and CSSP Incident Responder roles. Strong in the cleared market.
Style	Defensive and operational — reading logs, triaging alerts, prioritizing vulnerabilities, running an incident, and writing it up

A note on price. A CySA+ voucher runs roughly $370–$425 in the U.S. depending on seller and region — budget around $400, and confirm the current cost on CompTIA's site before you pay. See the funding page near the back, because you may not have to pay it yourself. CS0-003 replaced the older CS0-002; this booklet targets the current CS0-003 blueprint.

SEE IT TO LEARN IT

The Incident Response Lifecycle

Many CySA+ questions hinge on order: you contain before you eradicate, and you never skip the after-action. This is the NIST SP 800-61 flow.



The order is the answer to many questions: contain before you eradicate, and never skip the after-action review.

DOMAIN 1

Security Operations

Scenario questions · the analyst's core

OFFICIAL EXAM OBJECTIVES FOR THIS DOMAIN

- Interpret system and network data to identify anomalous and malicious activity
- Distinguish indicators of compromise (IoCs) from adversary tactics, techniques, and procedures (TTPs)
- Apply detection and analysis frameworks such as MITRE ATT&CK
- Tune detections to reduce false positives without losing coverage

Source: CompTIA CySA+ CS0-003 exam objectives. These are summarized objective statements for this domain; download the complete, authoritative objectives directly from CompTIA at comptia.org/certifications/cybersecurity-analyst.

How this booklet helps you excel here

This is the heart of the analyst's day: reading signals, separating noise from a real threat, and naming what you see with a shared framework. Every question puts you at the console with partial information and asks for the next correct move — which is exactly how the exam, and the job, work.

Sample of 5 questions from this domain. The full booklet contains all 300.

1. A Tier-1 analyst notices that, over four minutes, a single external IP attempted one login each against 340 different employee accounts, and exactly two of those attempts succeeded. Account-lockout thresholds were never tripped. Which of the following BEST describes this activity?

A. Normal authentication noise from a misconfigured service account
B. A brute-force attack against a single high-value account
C. A credential-stuffing attack using a breached database
D. A password-spraying attack

2. While reviewing firewall logs, an analyst sees an internal host connect outbound to the same external IP on port 443 every 60 seconds, almost to the second, transferring a few hundred bytes each time, around the clock. No user is logged in during most of these connections. Which of the following is the MOST likely explanation?

A. Command-and-control beaconing from an infected host
B. A misconfigured NTP client
C. Normal TLS keep-alive traffic
D. A software update agent checking for patches

3. A threat-intel feed your SOC subscribes to publishes the MD5 hash of a newly observed malware sample along with the specific sequence of living-off-the-land binaries the actor uses to establish persistence. Which statement BEST distinguishes how your team should treat these two items?

A. Neither is actionable without a CVE attached

B. Both are indicators of compromise and should be used identically

C. The hash is a TTP; the LOLBin sequence is an IoC

D. The hash is an IoC for detection/blocking; the LOLBin sequence is a TTP that informs hunting and detection logic

4. An analyst observes the following on a workstation: a Microsoft Word process spawned powershell.exe, which then launched an encoded command that reached out to a remote host and wrote a file to a Run registry key. The team wants to label the persistence step using a common framework so detections can be shared. Which framework is designed for exactly this mapping?

A. The Diamond Model of Intrusion Analysis

B. The Lockheed Martin Cyber Kill Chain

C. OWASP Top 10

D. MITRE ATT&CK

5. A SOC is flooded with alerts from a new detection rule, and after investigation the analysts confirm that 95% of them are benign administrative activity. Leadership asks for a response that preserves real detections while cutting the noise. Which action BEST addresses the problem?

A. Disable the detection rule entirely to stop the noise

B. Tune the rule by adding exclusions for the verified-benign administrative patterns and refining its logic

C. Route all alerts straight to a long-term archive without review

D. Raise the severity of every alert so analysts take them seriously

Reference

Answer Keys & Explanations

Detailed rationale for every question in the full booklet

DOMAIN 1 — ANSWER KEY

Security Operations

1. Correct answer: D — A password-spraying attack.

Password spraying tries a small number of common passwords across many accounts to stay under per-account lockout thresholds, which is exactly the one-attempt-per-account-across-340-accounts pattern here. The low-and-wide shape is the signature: a single source touching many identities with very few attempts each, deliberately avoiding the lockout that a traditional brute force against one account would trigger.

Cue: many accounts, few attempts each, lockouts never fire — think spraying, and pivot to the two successes immediately, because those are now suspected compromised.

2. Correct answer: A — Command-and-control beaconing from an infected host.

Regular, fixed-interval, low-volume connections to a single external host — especially with no user present — are the classic fingerprint of C2 beaconing, where implanted malware ‘phones home’ on a timer to fetch instructions. The tight periodicity and small, consistent payloads are what separate a beacon from ordinary traffic, which tends to be bursty and tied to user activity.

Cue: ‘same destination, fixed heartbeat, tiny payloads, no user’ — beaconing until proven otherwise; the next step is to capture and analyze the traffic and isolate the host.

3. Correct answer: D — The hash is an IoC for detection/blocking; the LOLBin sequence is a TTP that informs hunting and detection logic.

A file hash is an atomic indicator of compromise — brittle, easily changed by the adversary, best used for fast matching and blocking. The sequence of techniques an actor uses (their tradecraft) is a TTP, which sits higher on the Pyramid of Pain: it is far costlier for the adversary to change, so building hunts and behavioral detections around it yields durable value.

Cue: a hash/IP/domain is an IoC you match on; ‘how they operate’ is a TTP you hunt on — and TTP-based detection survives the attacker swapping infrastructure.

4. Correct answer: D — MITRE ATT&CK.

MITRE ATT&CK is a curated matrix of real-world adversary tactics and techniques, so a behavior like ‘Registry Run Keys for persistence’ maps to a specific technique ID that SOCs use as a shared language for detections and coverage gaps. The Kill Chain describes intrusion stages at a high level but isn’t a technique catalog; the Diamond Model links adversary/capability/infrastructure/victim for intel pivoting; OWASP covers web-app risks.

Cue: when a question asks you to label or map a specific observed technique so detections can be shared, it's ATT&CK.

5. Correct answer: B — Tune the rule by adding exclusions for the verified-benign administrative patterns and refining its logic.

Detection tuning — refining the rule's logic and excluding well-understood benign patterns — keeps the true positives while removing the false-positive flood, which is the analyst's core craft for keeping a SOC effective. Blanket-disabling the rule throws away the real detections it was built to catch, and simply re-prioritizing or archiving does nothing about the underlying noise.

Cue: 'reduce false positives without losing coverage' always points to tuning/exclusions, not to turning the detection off.

YOU'VE SEEN THE SAMPLE

Unlock the full CySA+ booklet

This preview is a taste. The complete 300-question booklet takes you through every domain with the same scenario-driven questions and plain-language explanations — built to match how the real CS0-003 exam thinks.

- ✓ All 300 scenario questions across every domain
- ✓ Full answer keys with exam cues for every question
- ✓ 8-week study schedule & recommended resources
- ✓ Career roadmap, acronym glossary & glossary quiz
- ✓ Exam-day quick reference & funding guide

You may not have to pay for this yourself.

Transitioning servicemembers and veterans can often fund the exam fee and training through Credentialing Assistance (Army CA / COOL), the GI Bill, or VET TEC. The full booklet includes a step-by-step funding guide. Ask us how to get your voucher covered before you pay out of pocket.