EVERY EXAM PREP · CHEAT SHEET

CompTIA CySA+ Cheat Sheet 2026

The night-before summary, built like the exam.

85 Questions	**2h 45m** Time limit	**750 (on a scale of 100-900)** Passing score
— Exam fee	**CompTIA** Governing body	

A condensed, scannable reference for the CompTIA Cybersecurity Analyst+ V4 (CS0-004) exam. Use this alongside full study materials, not as a replacement for them.

Exam Logistics at a Glance

Detail	Value
Question count	Maximum of 85 questions
Duration	165 minutes
Question format	Multiple-choice and performance-based questions (PBQs)
Passing score	750 on a scale of 100-900
Delivery	Physical test center or online proctored (OnVUE)
Delivery provider	Pearson VUE
Certification validity	3 years from certification date
Renewal path	Continuing Education Units (CEUs), no retake required

Who This Certifies

- Aimed at professionals working in a Security Analyst role.
- Validates the ability to detect, analyze, and respond to cybersecurity threats in modern security environments.
- Sits at an intermediate level in the CompTIA cybersecurity pathway, bridging Security+ and more advanced analyst/response roles.

Official Content Domains (Quick List)

The CS0-004 blueprint is organized around the security operations lifecycle. Treat these as your study buckets and allocate practice time proportionally to how heavily each is emphasized in your official exam objectives document:

- Security Operations — system hardening, log analysis, network security monitoring, and identifying indicators of malicious activity.
- Vulnerability Management — vulnerability scanning, scan result analysis, remediation prioritization, and vulnerability response frameworks.
- Incident Response and Management — incident response process, attack methodology frameworks, and post-incident activities like root cause analysis.
- Reporting and Communication — stakeholder communication, metrics reporting, and vulnerability/incident documentation practices.

Key Terms and Concepts to Memorize

- IOC (Indicator of Compromise) — an artifact observed on a network or system that suggests an intrusion has occurred.
- SIEM (Security Information and Event Management) — centralized log aggregation and correlation platform; expect scenario questions built around SIEM alert triage.
- Threat intelligence lifecycle — collection, processing, analysis, dissemination, feedback; know the order and purpose of each stage.
- MITRE ATT&CK framework — tactics and techniques mapping used to classify adversary behavior in incident analysis.
- CVSS (Common Vulnerability Scoring System) — vulnerability severity scoring; know how base, temporal, and environmental metrics shift a score.
- False positive vs. false negative — a recurring distinction in both detection tuning and PBQ scenarios.
- Chain of custody — the documented handling of evidence during incident response and forensics.
- Containment, eradication, and recovery — the core incident response phases tested heavily via scenario ordering questions.

Common Gotchas and Traps

- Performance-based questions front-load the exam in many candidates' experience — don't burn excessive time perfecting the first PBQ at the expense of the multiple-choice section.
- Answer choices often include a technically correct but contextually wrong option; always match the answer to the specific scenario constraints given, not just general best practice.
- Questions frequently blend two domains at once (e.g., a vulnerability management scenario that also tests reporting judgment) — don't assume a question only tests the domain it appears to be about.
- Tool-name recognition alone isn't enough; CySA+ tests what a tool's output means and what action follows, not just what the tool does.
- Time pressure is real given the question count and duration — pace yourself so PBQs don't consume a disproportionate share of your 165 minutes.
- Renewal is often overlooked: because CEUs can extend certification without a retake, some candidates fail to track their 3-year window and let it lapse unnecessarily.

Night-Before Checklist

- Confirm your delivery method — physical test center or OnVUE online proctoring — and verify the exact appointment time and location or system requirements.
- If testing online, test your webcam, microphone, and internet connection, and clear your desk/room per OnVUE proctoring rules.
- Bring required identification matching the name on your Pearson VUE registration.
- Do a final pass on incident response phase ordering, CVSS scoring logic, and MITRE ATT&CK terminology — these show up repeatedly across domains.
- Review your weakest content domain one more time rather than re-reading material you've already mastered.
- Plan your exam-day pacing mentally: with 85 questions in 165 minutes, know roughly how you'll budget time for PBQs versus multiple-choice.
- Get sufficient sleep — recall and scenario judgment both degrade quickly under fatigue during a 165-minute exam.
- Arrive early or log in early for online proctoring to handle any check-in delays without cutting into exam time.

Official sources

- CompTIA — CySA+ Certification V4 (New Version) | CompTIA: https://www.comptia.org/en-us/certifications/cybersecurity-analyst/v4/
- CompTIA — CySA+ Certification V3 (Retiring Version) | CompTIA: https://www.comptia.org/en-us/certifications/cybersecurity-analyst/v3/
- CompTIA — CySA+ Certification | CompTIA (V3 retirement schedule):

https://www.comptia.org/en-us/certifications/cybersecurity-analyst/

Free practice questions for this exam: www.everyexamprep.com/exams/comptia-cysa-plus/practice-test