CompTIA CySA+ (CS0-003) — One-Page Study Guide

BareMetalCyber.com | Cybersecurity Audio Academy
baremetalcyber.com/cybersecurity-audio-academy

Exam Snapshot

- **Exam:** CompTIA Cybersecurity Analyst+ (CySA+) — **CS0-003** (V3)
- **Issuer:** CompTIA • **Target level:** Intermediate (SOC / IR analyst focus)
- **Time limit:** 165 minutes
- **Questions:** Up to 85 (multiple-choice + performance-based)
- **Passing score:** 750 (scaled 100–900)
- **Question format details:** [VERIFY: exact mix of single vs multiple response, drag-and-drop, etc.]

Domain Weights

Domain	Weight
Security Operations	33%
Vulnerability Management	30%
Incident Response & Management	20%
Reporting & Communication	17%

Core Workflow (How the exam "thinks")

- Frame the scenario: goal, scope, constraints, and what "success" means.
- Collect and normalize evidence: alerts, logs, telemetry, tickets, asset context.
- Validate signal vs noise: baselines, false positives, and data quality checks.
- Analyze and correlate: pivot across hosts/users/processes; enrich with threat intel and T T P mapping.
- Prioritize: impact + likelihood (asset value, exposure, exploitability, C V S S context).
- Respond safely: contain, eradicate, recover, and preserve evidence when required.
- Communicate clearly: findings, impact, recommendations, and measurable next steps.
- Improve: tune detections, standardize workflows, and integrate tools for repeatable visibility.

High-Yield Concepts

- **S I E M** basics: log ingestion, normalization, correlation rules, dashboards.
- Log sources and fields: timestamp/time zone, host, user, process, src/dst, action, result.
- Indicators vs behaviors: I O C s (hash/IP/domain) vs T T P s (what the actor does).
- Threat intel: source reliability, confidence level, context, and sharing considerations.
- Vulnerability scanning choices: internal vs external; credentialed vs non-credentialed; agent vs agentless; active vs passive.
- Tool output interpretation: understand what was *observed* vs what is only *inferred*.
- C V S S triage: severity is not priority until exploitability and asset impact are considered.
- Attack frameworks: M I T R E A T T & C K, kill chain, diamond model, O S S T M M, O W A S P testing guide.
- Incident lifecycle: detection/analysis, containment, eradication, recovery, post-incident lessons learned.
- Reporting: executive summary vs technical detail, metrics/K P I s, and action plans tied to owners and dates.

Common Traps

- Trusting scanner or tool output without validation (duplicates, stale findings, false positives).
- Ignoring asset context (criticality, exposure, compensating controls) when prioritizing.
- Confusing "first step" (triage/verify) with "final fix" (remediate) in scenarios.
- Overweighting one indicator without corroboration across logs/telemetry.
- Skipping evidence preservation when the scenario implies investigation, legal, or forensics needs.
- Picking a response that is irreversible before scoping blast radius and impact.
- Reporting symptoms instead of root cause, and omitting measurable next actions.
- Mixing up internal vs external scanning requirements or credentialed vs non-credentialed expectations.

Cheat Sheet (Artifacts & quick cues)

- Core artifacts: alert → ticket → supporting logs → analyst notes → final report with timestamps.
- Key log cues: "who" (account), "what" (process/action), "where" (host/service), "when" (time + zone), "how" (src/dst + protocol).
- I O C types: file hash, I P, domain, U R L, certificate thumbprint, user-agent; always interpret with context.
- Vuln triage: exploit available? exposed service? privilege needed? asset value? compensating control present?
- C V S S: know what the score represents and what it does *not* represent (business impact).
- Incident response outputs: containment evidence, eradication evidence, recovery validation, lessons learned.
- Reporting components: impact statement, root cause, recommended actions, owners, dates, and K P I s.
- Metrics to recognize: M T T D, M T T R, false positive rate, coverage.
  [VERIFY: issuer-preferred KPI definitions]

Exam-Day Tactics

- Time budget: ~2 minutes per item on average; protect a block for heavy scenarios and P B Q s.
- Do a fast first pass: answer sure items, mark long log-analysis items, keep momentum.
- For P B Q s: identify required outputs first, then work backward from the scoring goal.
- Re-read the stem for constraints: scope, time window, tool output provided, and what is being asked (analyze vs recommend vs perform).
- Eliminate distractors by matching the verb and the evidence: choose what the scenario *supports*, not what is generally true.
- When torn between two: prefer the option that validates scope and evidence before a disruptive change, unless active compromise is clearly stated.
- Watch trigger words: *best*, *first*, *most likely*, *least*, and "based on the output."

30-Minute Final Review Plan

- 3 min: skim domain weights; name what each domain expects you to do.
- 7 min: incident phases + core frameworks (A T T & C K, kill chain) and what evidence each produces.
- 7 min: vulnerability scanning modes + validation steps + prioritization logic.
- 6 min: reporting structure (executive vs technical), K P I s, and action-plan wording.
- 7 min: practice one mini log triage: identify time zone, host, user, process, and "next best step."

Source: official exam objectives & exam details. Quick review only; practice required.