CompTIA CySA+ (CS0-003) Quick Summary

Fast 3-5 minute refresh for analyst priorities, comparisons, and incident-response shortcuts.

Best for	Focus	Use with
Ultra-fast memory refresh	Definitions, priorities, and common traps	Use with cheat sheet for deeper review

1. Fast refresh

CySA+ focus	Detection, analysis, response, vulnerability management, and reporting.
Think analyst-first	Most questions want the next best investigative or prioritization move.
Context beats volume	More logs are useless without correlation and purpose.
Evidence matters	Contain quickly, but preserve what you need for analysis.

2. Common traps

Severity vs priority	A 'high' alert is not automatically the first thing to fix.
Detection vs response	Seeing malicious behavior is not the same as containing it.
IOC vs IOA	Indicator of compromise differs from behavioral indicators of attack.
Patch now vs control now	Immediate compensating controls may be the right first move.

3. Analyst shortcuts

Timeline	Build one early.
Scope	Always ask how far it spread.
Logs + EDR + netflow	Correlate instead of trusting one source.
Document actions	You will need the trail later.

4. Reporting shortcuts

Exec summary	Risk, impact, recommendation.
Technical summary	Cause, evidence, scope, remediation.
Metrics	Use them to show improvement, not just activity.
Lessons learned	Controls should change after incidents.