CompTIA CySA+ (CS0-003) Cheat Sheet

One-page cram sheet for security operations, vulnerability management, incident response, reporting, and tooling.

Best for	Focus	Use with
Last review before drills or exam day	Analyst workflow + prioritization + response logic	Use with ports sheet and commands sheet

1. Security operations

Alert triage	Prioritize by impact, confidence, scope, and business context instead of by tool severity alone.
SOC workflow	Collection, correlation, enrichment, escalation, and documentation matter as much as raw detection.
Baselines	You need known-good behavior to identify anomalies in logs, flows, auth, and endpoint events.
KPIs and metrics	MTTD, MTTR, false positives, and dwell time connect technical work to operational performance.

2. Vulnerability management

Scanning vs validation	Findings must be verified, prioritized, and tracked rather than accepted blindly.
CVSS + context	A high score matters, but asset value, exploitability, exposure, and compensating controls also matter.
Patch strategy	Emergency fixes, maintenance windows, rollback planning, and verification are all part of the answer.
Exposure reduction	Segmentation, hardening, removal of unused services, and compensating controls reduce risk even before patching.

3. Incident response

Lifecycle	Preparation, identification, containment, eradication, recovery, and lessons learned.
Containment choices	Isolation can be tactical and temporary; preserve evidence while reducing spread.
Chain of custody	Important when handling evidence, especially if escalation outside the SOC may follow.
Root cause	Do not stop at 'malware found'; identify entry path, scope, persistence, and control gaps.

4. Reporting and communication

Audience matters	Executives want risk and impact; analysts want IOCs, timelines, and technical detail.

Documentation	Tickets, timelines, evidence notes, and action logs should be clear enough for handoff and review.
Threat intel use	Enrich alerts with context, not just extra data volume.
Recommendations	The best remediation advice is prioritized, realistic, and tied to business risk.

5. Tools and data sources

SIEM	Central search, correlation, and reporting.
EDR/NDR	Endpoint and network visibility complement each other.
Flow + packet + logs	These answer different questions; do not treat them as interchangeable.
Detection engineering mindset	Tune use cases to reduce noise and improve actionability.