CompTIA CySA+ CS0-003

Quick Exam Refresher

*This is your **condensed, high-impact review** designed for **quick recall** and confidence-building right before the exam — not deep instruction.*

Domains at a Glance

Each domain is weighted differently on the exam, with **Security Operations** carrying the most weight:

- Domain 1: **Security Operations (33%)**
- Domain 2: **Vulnerability Management (30%)**
- Domain 3: **Incident Response and Management (20%)**
- Domain 4: **Reporting and Communication (17%)**

Quick Reminder: How the Exam Works

- **Number of Questions**: Up to 85
- **Format**: Multiple choice + Performance-Based Questions (PBQs)
- **Time Limit**: 165 minutes
- **Passing Score**: 750 / 900 (approx. 83%)
- **Test Provider**: Pearson VUE (in-person or online)
- **Recommended Prerequisites**: Network+, Security+, or equivalent knowledge.

Remember — You Don’t Need to Be Perfect to Pass

The CySA+ passing score is around **83%**, which means you can miss **up to 14 questions** and still pass.

Domain 1: Security Operations (33%)

System & Network Architecture

- Understand OS components (processes, logs, memory, services)
- Monitor endpoints, servers, domain controllers, and network infrastructure
- Use baseline behavior to detect anomalies

Log Management

- Centralize logs with a SIEM (e.g., Splunk, QRadar)
- Normalize, parse, and store for correlation and alerting
- Use Event IDs (e.g., 4625 for failed login in Windows)

SIEM, EDR, and Detection Tools

- SIEM: real-time alerts, rule-based correlation, dashboards
- EDR/XDR: monitors endpoints, kills malicious processes
- IDS/IPS: detects (and blocks if IPS) suspicious network traffic

Indicators of Compromise (IOC)

- Suspicious hashes, IPs, unusual login times, unauthorized software
- DNS anomalies, encoded PowerShell, registry changes

MITRE ATT&CK / Kill Chain

- ATT&CK: Tactics (e.g., Persistence, Privilege Escalation) and Techniques (e.g., Create Account, Mimikatz)
- Kill Chain: Recon → Weaponize → Deliver → Exploit → Install → C2 → Actions

Threat Intelligence

- Strategic (big picture), Tactical (IOCs), Operational (campaigns), Technical (hashes, domains)
- Sources: OSINT, commercial feeds, ISACs

Threat Hunting

- Proactive analysis using hypotheses
- IOC-based, TTP-based, or anomaly-based
- Uses tools like SIEM queries, EDR logs, and network captures

SOC Efficiency

- Streamline alerts, integrate tooling, automate responses, track metrics.

Domain 2: Vulnerability Management (30%)

Vulnerability Scanning

- Credentialed vs. Non-credentialed
- Internal vs. External; Active vs. Passive
- Agent-based vs. Agentless

Tools

- Nessus, OpenVAS, Qualys, InsightVM
- SAST (code scan), DAST (runtime app test), SCA (3rd-party lib check)

Interpreting Results

- CVE: unique vuln ID (e.g., CVE-2021-34527)
- CVSS: severity score (0–10), Critical ≥9
- Validate findings to eliminate false positives

Risk Prioritization

- Risk = Likelihood × Impact
- Consider exposure, asset value, threat intel, exploitability

Remediation Options

- Patch (ideal), reconfigure, isolate
- Compensating controls if patching isn't feasible (e.g., firewall, monitoring)

Common Vulnerabilities

- Misconfigs, weak crypto (e.g., TLS 1.0), XSS, SQLi, open S3 buckets
- Zero-day = unknown and unpatched

Secure Configuration

- Use CIS Benchmarks, hardening guides, baseline images
- Regularly scan for drift or misconfigurations

Attack Surface Management

- Minimize exposure (e.g., close unused ports)
- Use discovery tools (Nmap, asset inventory)
- Include shadow IT and cloud assets

Domain 3: Incident Response and Management (20%)

Incident Response Lifecycle (NIST / PICERL)

1. **Preparation** – IR plan, playbooks, tools, team training
2. **Detection & Analysis** – Validate alerts, classify incident type/severity
3. **Containment** – Quarantine infected hosts, block malicious IPs
4. **Eradication** – Remove malware, fix root cause (e.g., patch vuln)
5. **Recovery** – Restore systems, monitor post-recovery
6. **Lessons Learned** – Postmortem review, update playbooks

Incident Types

- Malware, phishing, insider threat, DDoS, data breach, privilege misuse

Roles and Responsibilities

- SOC Analyst, IR Lead, Forensic Analyst, PR/Legal, Executives
- Escalation paths and stakeholder coordination are critical

Evidence Handling

- Chain of Custody: document who touched what, when, and how
- Order of Volatility: RAM → Process list → Disk → Logs → Backups
- Imaging: use forensic tools to clone before analyzing

Attack Methodologies

- **MITRE ATT&CK**: use for mapping attacker behavior
- **Diamond Model**: Adversary, Infrastructure, Capability, Victim
- **Kill Chain**: visualize attack progression

Detection Tools

- SIEM: event correlation
- IDS/IPS: packet analysis
- EDR: endpoint telemetry

Reporting

- Include timeline, systems affected, actions taken, root cause, IOCs
- Submit to management, legal, and regulators if needed

Domain 4: Reporting and Communication (17%)

Report Types

- Executive: summaries, trends, business risk
- Technical: detailed CVEs, affected assets, fix instructions
- Compliance: maps to frameworks (e.g., PCI, HIPAA, NIST)

Remediation Planning

- Assign ownership, deadlines, remediation steps
- Track status via tickets or dashboards

Metrics / KPIs

- Vulnerability KPIs: patch SLAs, recurring issues
- IR KPIs: MTTD, MTTC, MTTR, detection sources (internal vs external)

Inhibitors to Remediation

- Technical: patch breaks app
- Operational: limited downtime
- Resource: no staff/time/tools
- Communication: unclear ownership

Stakeholder Communication

- Technical: specific, actionable
- Executives: high-level impact/risk
- Legal/compliance: breach reporting timelines

During Incidents

- Use war room or secure chat
- Avoid compromised channels
- Escalate as per policy
- Only authorized personnel communicate externally

Post-Incident

- Reports include timeline, affected systems, response, lessons
- Feed findings back into detection logic, training, and procedures

MITRE ATT&CK Tactics and Examples

Tactic	Description	Common Techniques
Initial Access	How attackers gain entry	Phishing, Exploit Public-Facing App, Drive-by
Execution	Run malicious code	PowerShell, Macros, Command-Line Interface
Persistence	Maintain access	Startup scripts, Registry Run Keys, New Services
Privilege Escalation	Gain higher-level access	Exploiting SUID, Bypassing UAC, Token Manipulation
Defense Evasion	Avoid detection	Obfuscation, Disabling AV, Masquerading
Credential Access	Steal user credentials	Keylogging, LSASS dump, Brute Force
Discovery	Understand the environment	Network scans, AD queries, File/System enumeration
Lateral Movement	Move between systems	Pass-the-Hash, RDP, SMB shares
Collection	Gather target data	Screen capture, Email scraping, Clipboard logging
Command & Control	Communicate with compromised systems	DNS Tunneling, Web Traffic, Custom Protocols
Exfiltration	Steal data	HTTPS uploads, Cloud sync, Removable media
Impact	Disrupt operations or destroy data	Ransomware, Data Wipe, DDoS