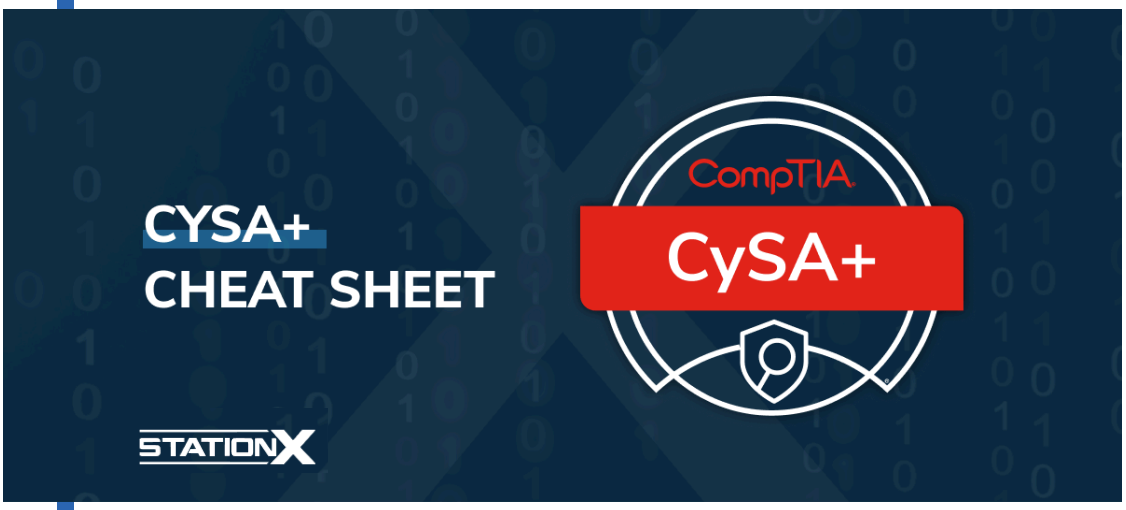
CySA+ Cheat Sheet



STATIONX
THE CYBER SECURITY COMPANY

About CompTIA CySA+

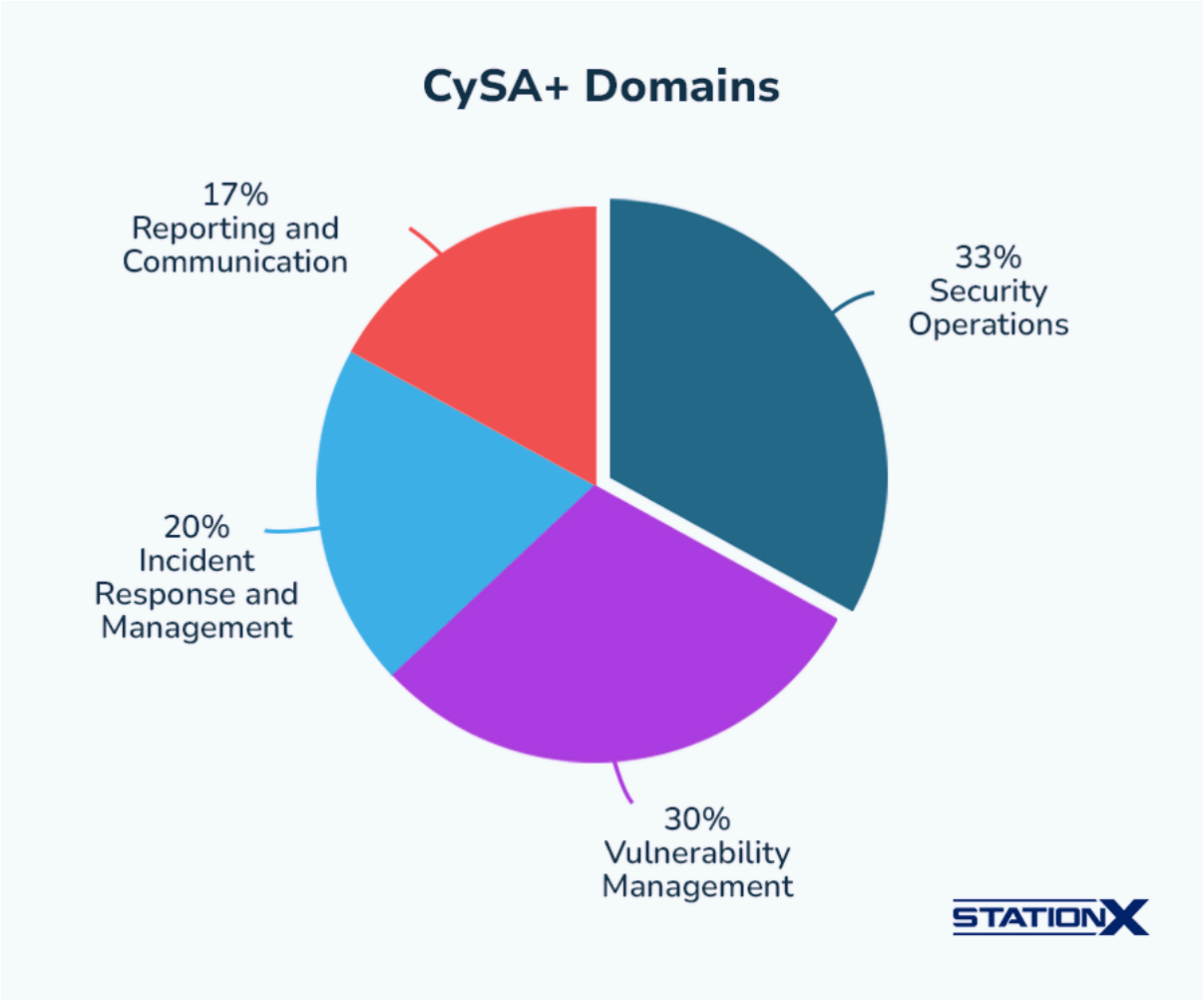
CompTIA CySA+ | CompTIA Cybersecurity Analyst (CySA+)

CompTIA's CySA+ certification stands for cyber security analyst and purposes to test one's understanding of **knowledge and tools cyber security analysts will use on the job.**

CySA+ is a **165-minute exam** comprised of a maximum of **85 multiple-choice and performance-based questions.** You'll need a score of at least **750/900 to pass the exam.**

The exam is categorized into four knowledge domains, weighted as follows:

- Security Operations (33%)
- Vulnerability Management (30%)
- Incident Response and Management (20%)
- Reporting and Communication (17%)



CySA+ Cheat Sheet Exam Domains

This cheat sheet details the most crucial information found in each domain. Each domain is broken up into subdomains.

Security Operations

The largest portion of the exam tests your understanding of cyber security tools and your ability to assess, defend, and harden asset security.

System & Network Architecture

Concept	Elaboration
System hardening	Tools, techniques, and best practices used to shore up the protection of IT assets.

Cloud	• Public cloud - Off-premises cloud environments where infrastructure is not owned by the end user. • Hybrid - using a combination of cloud-based and on-premises computing • On-premises - otherwise known as private cloud, on-premises cloud computing is located in a company's brick-and-mortar building and has its own dedicated resources.
Zero trust	No implicit trust. Every interaction must be validated.
Virtualization	Allows for the hardware resources of a computer to be divvied up into multiple virtual computers, called virtual machines (VMs).
Containerization	Software deployment process that bundles an application's code with the requisite libraries and files needed to run on any infrastructure.
PKI	Public key infrastructure
SSO	Single sign-on
MFA	Multi-factor authentication
Federation	Arrangement between companies allowing for user to sign on
DLP	Data loss prevention system
PII	Personal identifiable information

Tools & Techniques

Concept	Elaboration
Wireshark	Open-source packet capture analysis tool
tcpdump	CLI Packet analyzer tool
SIEM	Security information and event management
SOAR	Security, orchestration, automation, and

	response
EDR	Endpoint detection and response
VirusTotal	Free website used for file and url malware analysis
Email analysis	• Header • Impersonation • DomainKeys Identified Mail (DKIM) • Sender Policy Framework (SPF)
Programming languages/scripting	• JSON • Python • PowerShell • Shell script • XML
Sandboxing	Running code in a safe environment to test code and prevent threats.

Threat Intelligence & Threat Hunting

Concept	Elaboration
Threat actors	• Advanced persistent threat (APT) • Hacktivists • Organized crime • Nation-state • Script kiddie • Insider threat
TTP	Tactics, techniques, and procedures
Confidence levels	• Timeliness • Relevancy • Accuracy
Collection methods and sources	• Open source • Closed source
Threat intelligence sharing	• Incident response • Vulnerability management • Risk management • Security engineering • Detection and monitoring
Threat hunting	• Indicators of compromise (IOC) • Honeypot • Active defense • Configurations/misconfigurations

Vulnerability Management

The second largest knowledge domain will test your ability to identify, evaluate, and respond to security vulnerabilities.

Vulnerability Scanning & Assessment

Concept	Elaboration
Asset discovery	Map scans and device fingerprinting.
Internal scanning	Scanning internal devices for vulnerabilities.
External scanning	Assessing external threats to IT assets.
Credentialed scan	Using privileged credentials to scan systems.
Non-credentialed scan	Scanning of systems not using credentials.
Passive scanning	Scans for traffic on a network in a way that isn't likely to be detected by IDS or IPS.
Active scanning	Noisey type of scanning that targets specific ports and services to gather specific information.
Critical infrastructure	• Operational technology (OT) • Industrial control systems (ICS) • Supervisory control and data acquisition (SCADA)
Industry frameworks	• Payment Card Industry Data Security Standard (PCI DSS) • Center for Internet Security (CIS) benchmarks • Open Web App Security Project (OWASP) • International Organization for Standardization (ISO)

Data Analyzation

Concept	Elaboration
Network scanning and mapping	• Angry IP Scanner • Maltego

Web application scanners	• Burp Suite • Zed Attack Proxy (ZAP) • Arachni • Nikto
Vulnerability scanners	• Nessus • OpenVAS
Debuggers	• Immunity debuggers • GNU debuggers
Nmap	Popular CLI network mapping tool
Metasploit Framework (MSF)	Open-source penetration testing tool
Recon-ng	Open-source tool used for reconnaissance.
Cloud infrastructure assessment tools	• Scout Suite • Prowler • Pacu

Prioritizing Vulnerabilities

Concept	Elaboration
Common Vulnerability Scoring System Interpretation (CVSS)	• Attack vectors • Attack complexity • Privileges required • User interaction • Scope
Impact	• Confidentiality - was private information gained access to • Integrity - was data changed • Availability - can data still be accessed
Validation	• True/false positives • True/false negatives
Context awareness	• Internal • External • Isolated
Exploitability/weaponization	What was used to exploit the vulnerability in question.
Asset value	Combination of the value to the owner, maintenance cost, damage caused if lost, and penalties that would be incurred if it was lost.

Zero-day	An unknown vulnerability.

Software Vulnerabilities

Concept	Elaboration
Cross-site scripting	Injected malicious code into a website
Overflow vulnerabilities	• Buffer • Integer • Heap • Stack
Data poisoning	Adding malicious information to poison training data.
Cross-site request forgery	Tricking authenticated users into executing actions favorable to the hacker, such as transferring funds, changing passwords, or email addresses.
Directory traversal	Web vulnerability that allows hackers to easily access restricted directories.
Insecure design	Creating software that is inherently vulnerable.
End–of-life or outdated components	Inherently vulnerable systems that no longer receive security patches.
Privilege escalation	Gaining access to accounts you shouldn't be able to access.
Local file inclusion (LFI)	Including a file that has not been validated.

Vulnerability Response, Handling, and Management

Concept	Elaboration
Compensating control	Control put in place to satisfy a security measure deemed too difficult to implement.
Control types	• Managerial • Operational • Technical • Preventative • Detective

	• Responsive • Corrective
Patching and configuration management	• Testing • Implementation • Rollback - returns software to previous state • Validation
Risk management principles	• Accept • Transfer - using insurance to transfer risk • Avoid • Mitigate
SLOs	Service level objectives
Attack surface management	• Edge discovery - mapping edge network devices • Passive discovery • Security controls testing • Penetration testing and adversary emulation • Bug bounty - financially incentivizing ethical hackers to find bugs • Attack surface reduction
Secure coding best practices	• Input validation - ensuring only certain characters can be input. • Output encoding - ensuring data can safely be encoded into another format • Session management • Authentication - verifying the identity of a user • Data protection • Parameterized queries
SDLC	Secure software development life cycle
Threat modeling	Systematic way of finding threats and securing systems and data.

Incident Response & Management

This domain will test your ability to prepare for, respond to, and manage the fallout of a cyber attack.

Attack Methodology Framework

Concept	Elaboration
Cyber kill chain	Lockheed Martin developed a framework for identifying and preventing cyber intrusions.
Diamond Model of Intrusion Analysis	Four-step model that identifies the adversary, capabilities, infrastructure, and victims
MITRE ATT&CK	The most in-depth attach methodology framework focusing on real-life tactics and techniques.
Open Source Security Testing Methodology Manual (OSS TMM)	Developed by ISECOM and used for security testing and analysis.
OWASP Testing Guide	In-depth guide for testing the cyber security of web apps.

Incident Respond Activities

Concept	Elaboration
IoC	Indicator of compromise
Evidence acquisitions	• Chain of custody • Validating data integrity • Preservation • Legal hold
Data and log analysis	Using a SIEM to collect, log, and understand data.
Containment, eradication, and recovery	• Scope • Impact • Isolation • Remediation - fixing vulnerabilities • Re-imaging - wiping or clearing a computer in an attempt to rid it of malware. • Compensating controls

Preparation & Post-Incident Handling

Concept	Elaboration
Incident response plan	A detailed incident response plan to be carried out after an incident.
Playbooks	Standardized steps to take after an incident has occurred.
Tabletop	Non-technical training exercise that prepares employees for how to respond to a cyber security incident.
Business continuity (BC)	Plan to ensure a business quickly recovers after an incident.
Post-incident activity	• Forensic analysis - analysis of data to understand how the attack took place. • Root cause analysis • Lessons learned - a detailed written report of lessons learned from the incident.

Reporting & Communication

17% of the questions you receive will pertain to the day-to-day tasks of a cyber security analyst that relate to reporting and communicating security information to co-workers, stakeholders, and those not well versed in the language of cyber security.

Vulnerability Management Reporting & Communication

Concept	Elaboration
Vulnerability management reporting	• Vulnerabilities • Affected hosts • Risk score • Mitigation • Recurrence • Prioritization
Action plans	• Configuring management • Patching • Compensating controls • Awareness, education, and training • Changing business requirements
Inhibitors to remediation	• Memorandum of understanding

	(MOU) • Service-level agreement (SLA) • Organizational governance • Business process interruption • Degrading functionality • Legacy systems • Proprietary systems
Metrics and key performance indicators (KPIs)	• Trends • Top 10 • Critical vulnerabilities and zero-days • Service level objectives (SLOs)

Incident Response Reporting & Communication

Concept	Elaboration
Stakeholder identification and communication	Identify stakeholders and communicate effectively
Incident declaration and escalation	Informing stakeholders and effectively escalating event.
Incident response reporting	• Executive summary • Who, what, when, where, and why • Recommendations • Timeline • Impact • Scope • Evidence
Communications	• Legal • Public relations • Media • Regulatory reporting • Law enforcement
Root cause analysis	Use forensics to understand the origin of attack.
Metrics and KPIs	• Mean time to detect • Mean time to respond • Mean time to remediate • Alert volume

Conclusion

This CompTIA CySA+ cheat sheet is a quick and easy-to-use guide that provides you with an understanding of what you will be tested on when you take CompTIA's CySA+ exam.

Not everything covered on this cheat sheet will be on the exam. However, it's important to grasp the aforementioned material as it's all fair game come test time. Take your time when studying for this exam, and be sure to use quality study material to prepare.

To prepare you for CompTIA CySA+ and a career in the cyber security industry, we invite you to join our Accelerator Program. When you join, you'll receive access to over 1,000 courses and labs, personalized study roadmaps, unlimited career mentorship, mastermind and study groups, and a growing community of supportive cyber security professionals.

CompTIA CySA+ (CS0-003) Complete Course