Appendix A

Mapping Course Content to CompTIA CySA+

Achieving CompTIA CySA+ certification requires candidates to pass Exam CS0-003. This table describes where the exam objectives for Exam CS0-003 are covered in this course.

1.0 Security Operations	
1.1 Explain the importance of system and network architecture concepts in security operations.	**Covered in**
Log ingestion	Lesson 3, Topic C
Time synchronization	
Logging levels	
Operating system (OS) concepts	Lesson 3, Topic A
Windows Registry	
System hardening	
File structure	
Configuration file locations	
System processes	
Hardware architecture	
Infrastructure concepts	Lesson 3, Topic A
Serverless	
Virtualization	
Containerization	
Network architecture	Lesson 3, Topic A
On-premises	
Cloud	
Hybrid	
Network segmentation	
Zero trust	
Secure access service edge (SASE)	
Software-defined networking (SDN)	
Identity and access management	Lesson 3, Topic B
Multifactor authentication (MFA)	
Single sign-on (SSO)	
Federation	
Privileged access management (PAM)	
Passwordless	
Cloud access security broker (CASB)	

1.1 Explain the importance of system and network architecture concepts in security operations.	Covered in
Encryption	Lesson 3, Topic C
Public key infrastructure (PKI)	
Secure sockets layer (SSL) inspection	
Sensitive data protection	Lesson 3, Topic C
Data loss prevention (DLP)	
Personally identifiable information (PII)	
Cardholder data (CHD)	

1.2 Given a scenario, analyze indicators of potentially malicious activity.	Covered in
Network-related	Lesson 11, Topic A
Bandwidth consumption	
Beaconing	
Irregular peer-to-peer communication	
Rogue devices on the network	
Scans/sweeps	
Unusual traffic spikes	
Activity on unexpected ports	
Host-related	Lesson 11, Topic B
Processor consumption	
Memory consumption	
Drive capacity consumption	
Unauthorized software	
Malicious processes	
Unauthorized changes	
Unauthorized privileges	
Data exfiltration	
Abnormal OS process behavior	
File system changes or anomalies	
Registry changes or anomalies	
Unauthorized scheduled tasks	
Application-related	Lesson 13, Topic B
Anomalous activity	
Introduction of new accounts	
Unexpected output	
Unexpected outbound communication	
Service interruption	
Application logs	
Other	Lesson 13, Topic B
Social engineering attacks	Lesson 11, Topic C
Obfuscated links	

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.	Covered in
Tools	Lesson 10, Topic A
Packet capture	
Wireshark	
tcpdump	
Log analysis/correlation	
Security information and event management (SIEM)	
Security orchestration, automation, and response (SOAR)	
Endpoint security	
Endpoint detection and response (EDR)	
Domain name service (DNS) and Internet Protocol (IP) reputation	
WHOIS	
AbuseIPDB	
File analysis	
Strings	
VirusTotal	
Sandboxing	
Joe Sandbox	
Cuckoo Sandbox	
Common techniques	Lesson 10, Topic C
Pattern recognition	Lesson 13, Topic B
Command and control	Lesson 10, Topic C
Interpreting suspicious commands	
Email analysis	
Header	
Impersonation	
DomainKeys Identified Mail (DKIM)	
Domain-based Message Authentication, Reporting, and Conformance (DMARC)	
Sender Policy Framework (SPF)	
Embedded links	
File analysis	
Hashing	
User behavior analysis	
Abnormal account activity	
Impossible travel	

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.	Covered in
Programming languages/scripting	Lesson 13, Topic A
JavaScript Object Notation (JSON)	
Extensible Markup Language (XML)	
Python	
PowerShell	
Shell script	
Regular expressions	

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.	Covered in
Threat actors	Lesson 2, Topic A
Advanced persistent threat (APT)	
Hacktivists	
Organized crime	
Nation-state	
Script kiddie	
Insider threat	
Intentional	
Unintentional	
Supply chain	
Tactics, techniques, and procedures (TTP)	Lesson 2, Topic B
Confidence levels	
Timeliness	
Relevancy	
Accuracy	
Collection methods and sources	Lesson 2, Topic B
Open source	
Social media	
Blogs/forums	
Government bulletins	
Computer emergency response team (CERT)	
Cybersecurity incident response team (CSIRT)	
Deep/dark web	
Closed source	
Paid feeds	
Information sharing organizations	
Internal sources	

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.	Covered in
Threat intelligence sharing	Lesson 2, Topic B
Bandwidth consumption	
Beaconing	
Irregular peer-to-peer communication	
Rogue devices on the network	
Scans/sweeps	
Unusual traffic spikes	
Activity on unexpected ports	
Threat hunting	Lesson 2, Topic C
Indicators of compromise (IoC)	
Collection	
Analysis	
Application	
Focus areas	
Configurations/misconfigurations	
Isolated networks	
Business-critical assets and processes	
Active defense	
Honeypot	

1.5 Explain the importance of efficiency and process improvement in security operations.	Covered in
Standardize processes	Lesson 4, Topic A
Identification of tasks suitable for automation	
Repeatable/do not require human interaction	
Team coordination to manage and facilitate automation	
Streamline operations	Lesson 4, Topic A
Automation and orchestration	
Security orchestration, automation, and response (SOAR)	
Orchestrating threat intelligence data	
Data enrichment	
Threat feed combination	
Minimize human engagement	
Technology and tool integration	Lesson 4, Topic B
Application programming interface (API)	
Webhooks	
Plugins	
Single pane of glass	Lesson 4, Topic B

2.0 Vulnerability Management	
2.1 Given a scenario, implement vulnerability scanning methods and concepts.	**Covered in**
Asset discovery	Lesson 5, Topic B
Map scans	
Device fingerprinting	
Special considerations	Lesson 5, Topic C
Scheduling	
Operations	
Performance	
Sensitivity levels	
Segmentation	
Regulatory requirements	Lesson 5, Topic B
Internal vs. external scanning	Lesson 5, Topic B
Agent vs. agentless	Lesson 5, Topic B
Credentialed vs. non-credentialed	Lesson 5, Topic B
Passive vs. active	Lesson 5, Topic B
Static vs. dynamic	Lesson 5, Topic B
Reverse engineering	
Fuzzing	
Critical infrastructure	Lesson 5, Topic C
Operational technology (OT)	
Industrial control systems (ICS)	
Supervisory control and data acquisition (SCADA)	
Security baseline scanning	Lesson 5, Topic B
Industry frameworks	Lesson 5, Topic B
Payment Card Industry Data Security Standard (PCI DSS)	
Center for Internet Security (CIS) benchmarks	
Open Web Application Security Project (OWASP)	
International Organization for Standardization (ISO) 27000 series	

2.2 Given a scenario, analyze output from vulnerability assessment tools.	**Covered in**
Tools	Lesson 11, Topic C
Network scanning and mapping	
Angry IP Scanner	
Maltego	
Web application scanners	Lesson 12, Topic A
Burp Suite	
Zed Attack Proxy (ZAP)	
Arachni	
Nikto	
Vulnerability scanners	Lesson 11, Topic C
Nessus	
OpenVAS	
Debuggers	Lesson 12, Topic A
Immunity debugger	
GNU debugger (GDB)	
Multipurpose	Lesson 11, Topic C
Nmap	
Metasploit framework (MSF)	
Recon-ng	
Cloud infrastructure assessment tools	Lesson 12, Topic B
ScoutSuite	
Prowler	
Pacu	

2.3 Given a scenario, analyze data to prioritize vulnerabilities.	**Covered in**
Common Vulnerability Scoring System (CVSS) interpretation	Lesson 6, Topic A
Attack vectors	
Attack complexity	
Privileges required	
User interaction	
Scope	Lesson 6, Topic B
Impact	
Confidentiality	
Integrity	
Availability	

2.3 Given a scenario, analyze data to prioritize vulnerabilities.	Covered in
Validation	Lesson 6, Topic B
True/false positives	
True/false negatives	
Context awareness	Lesson 6, Topic B
Internal	
External	
Isolated	
Exploitability/weaponization	Lesson 6, Topic B
Asset value	Lesson 6, Topic B
Zero-day	Lesson 6, Topic B

2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.	Covered in
Cross-site scripting	Lesson 14, Topic B
Reflected	
Persistent	
Overflow vulnerabilities	Lesson 14, Topic B
Buffer	
Integer	
Heap	
Stack	
Data poisoning	Lesson 14, Topic B
Broken access control	Lesson 14, Topic C
Cryptographic failures	Lesson 14, Topic C
Injection flaws	Lesson 14, Topic B
Cross-site request forgery	Lesson 14, Topic B
Directory traversal	Lesson 14, Topic B
Insecure design	Lesson 14, Topic C
Security misconfiguration	Lesson 14, Topic C
End-of-life or outdated components	Lesson 14, Topic C
Identification and authentication failures	Lesson 14, Topic C
Server-side request forgery	Lesson 14, Topic C
Remote code execution	Lesson 14, Topic C
Privilege escalation	Lesson 14, Topic C
Local file inclusion (LFI)/remote file inclusion (RFI)	Lesson 14, Topic B

2.5 Explain concepts related to vulnerability response, handling, and management.	Covered in
Compensating control	Lesson 7, Topic B
Control types	Lesson 1, Topic B
Managerial	
Operational	
Technical	
Preventative	
Detective	
Responsive	
Corrective	
Patching and configuration management	Lesson 1, Topic C
Testing	
Implementation	
Rollback	
Validation	
Maintenance windows	Lesson 1, Topic C
Exceptions	Lesson 1, Topic A
Risk management principles	Lesson 1, Topic A
Accept	
Transfer	
Avoid	
Mitigate	
Policies, governance, and service-level objectives (SLOs)	Lesson 1, Topic A
Prioritization and escalation	Lesson 1, Topic B
Attack surface management	Lesson 1, Topic B
Edge discovery	
Passive discovery	
Security controls testing	
Penetration testing and adversary emulation	
Bug bounty	
Attack surface reduction	
Secure coding best practices	Lesson 14, Topic A
Input validation	
Output encoding	
Session management	
Authentication	
Data protection	
Parameterized queries	
Secure software development life cycle (SDLC)	Lesson 14, Topic A
Threat modeling	Lesson 1, Topic A

3.0 Incident Response and Management	
3.1 Explain concepts related to attack methodology frameworks.	**Covered in**
Cyber kill chain	Lesson 10, Topic B
Diamond Model of Intrusion Analysis	Lesson 10, Topic B
MITRE ATT&CK	Lesson 10, Topic B
Open Source Security Testing Methodology Manual (OSSTMM)	Lesson 10, Topic B
OWASP Testing Guide	Lesson 14, Topic A

3.2 Given a scenario, perform incident response activities.	**Covered in**
Detection and analysis	
IoC	Lesson 8, Topic B
Evidence acquisitions	
Chain of custody	
Validating data integrity	
Preservation	
Legal hold	
Data and log analysis	Lesson 8, Topic A
Containment, eradication, and recovery	Lesson 8, Topic B
Scope	
Impact	
Isolation	
Remediation	
Reimaging	
Compensating controls	

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.	**Covered in**
Preparation	Lesson 8, Topic A
Incident response plan	
Tools	
Playbooks	
Tabletop	
Training	
Business continuity (BC) / disaster recovery (DR)	
Post-incident activity	Lesson 8, Topic A
Forensic analysis	Lesson 2, Topic C
Root cause analysis	Lesson 9, Topic B
Lessons learned	Lesson 8, Topic A

4.0 Reporting and Communication	
4.1 Explain the importance of vulnerability management reporting and communication.	**Covered in**
Vulnerability management reporting	Lesson 7, Topic A
Vulnerabilities	
Affected hosts	
Risk score	
Mitigation	
Recurrence	
Prioritization	
Compliance reports	Lesson 7, Topic A
Action plans	Lesson 7, Topic B
Configuration management	
Patching	
Compensating controls	
Awareness, education, and training	
Changing business requirements	
Inhibitors to remediation	Lesson 7, Topic B
Adversary	
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)	Lesson 7, Topic A
Trends	
Top 10	
Critical vulnerabilities and zero-days	
SLOs	

4.2 Explain the importance of incident response reporting and communication.	**Covered in**
Stakeholder identification and communication	Lesson 9, Topic A
Incident declaration and escalation	Lesson 9, Topic A
Incident response reporting	Lesson 9, Topic A
Executive summary	Lesson 9, Topic B
Who, what, when, where, and why	Lesson 8, Topic A
Recommendations	Lesson 9, Topic B
Timeline	
Impact	
Scope	
Evidence	

4.2 Explain the importance of incident response reporting and communication.	Covered in
Communications	Lesson 9, Topic B
Legal	
Public relations	
Customer communication	
Media	
Regulatory reporting	
Law enforcement	
Root cause analysis	Lesson 9, Topic B
Lessons learned	Lesson 9, Topic B
Metrics and KPIs	Lesson 9, Topic B
Mean time to detect	
Mean time to respond	
Mean time to remediate	
Alert volume	