COURSE SYLLABUS

CompTIA CySA+ Exam Preparation Course (Self-Paced)

Build the CySA+ skills to recognize malicious activity, manage vulnerabilities, and respond to incidents like a SOC analyst.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/cysa-plus-exam-preparation-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Security Operations Architecture Concepts

- Lessons:
  - Logging Fundamentals: Ingestion, Configuration, and Retention
  - Operating System Hardening and File Structure Concepts
  - Modern Infrastructure Architecture: Cloud, Virtualization, and Containers
  - Network Architecture and Zero Trust Concepts: ZTNA, SASE, IAM, and PAM
  - Data Protection, Encryption, and Critical Infrastructure: OT, ICS, and SCADA
- Applied activity: Given a simplified network diagram and a log ingestion pipeline description, learners identify where Zero Trust controls, encryption, and log retention policies should be applied.

Module 2: Recognizing Indicators of Malicious Activity

- Lessons:
  - Network and Host Indicators of Compromise
  - Living Off the Land Binaries, Scripts, and File System Changes
  - Application and Cloud Indicators of Malicious Activity
  - Identity-Based and Social Engineering Indicators: Impossible Travel, Business Email Compromise, and Typosquatting
- Applied activity: Given a set of annotated screenshots, a process list, a firewall log excerpt, and an email header, learners classify each artifact by indicator category and justify the classification.

Module 3: Tools for Detecting Malicious Activity

- Lessons:
  - Packet and Log Analysis Tools: Wireshark, tcpdump, Snort, Suricata, Zeek, and SIEM
  - Threat Intelligence Platforms and Endpoint Tools: OTX, MISP, OpenCTI, EDR/XDR, and MDM
  - Reputation, File, and Sandbox Analysis: WHOIS, AbuseIPDB, VirusTotal, YARA, and Sandboxing
  - Pattern Recognition and Email Analysis: Regular Expressions, Suspicious Commands, MXToolbox, and UEBA

- File Formats and Scripting for Analysts: JSON, XML, YAML, EVTX, Python, PowerShell, and Shell Script

- Applied activity: Given a screenshot of Wireshark packet capture output and a corresponding EVTX log excerpt, learners identify the matching indicator and describe which additional tool they would use next and why.

Module 4: Threat Intelligence and Threat Hunting Concepts

- Lessons:
  - Threat Actors, TTPs, and the Pyramid of Pain
  - MITRE ATT&CK and Attribution Confidence
  - Threat Intelligence Collection and Sharing: OSINT and Closed-Source Sources
  - Indicators of Compromise: Atomic and Behavioral Types
  - Threat Modeling with STRIDE, Threat Mapping, and Cyber Deception
- Applied activity: Given a short threat report excerpt, learners map the described activity to MITRE ATT&CK tactics and rate the source's confidence level using timeliness, relevance, and accuracy criteria.

Module 5: Process Improvement, Automation, and AI in Security Operations

- Lessons:
  - Standardizing and Streamlining Security Operations: Playbooks and Runbooks
  - Automation and Orchestration: SOAR and Infrastructure as Code
  - Alert Tuning, Dashboards, and Tool Integration
  - AI Risks and Governance in Security Operations
  - Practical AI Use Cases for Analysts
- Applied activity: Given a sample SOAR playbook description and an AI chatbot transcript, learners identify one process-improvement opportunity and one AI governance risk, and recommend a mitigation for each.

Module 6: Vulnerability Scanning Methods

- Lessons:
  - Asset Inventory and Scan Planning Considerations
  - Scan Types: Internal versus External, Agent versus Agentless, Credentialed versus Non-Credentialed
  - Passive and Active Discovery: Mapping Scans and Device Fingerprinting
  - Security Baseline Scanning: PCI DSS, CIS Benchmarks, and ISO/IEC 27000
- Applied activity: Given a scenario describing a regulated environment with cardholder data present and a segmented network, learners choose the appropriate scan type, schedule, and baseline standard, and justify each choice.

Module 7: Analyzing Vulnerability Assessment Tool Output

- Lessons:
  - Network Scanning and Mapping Tool Output: Angry IP Scanner, Masscan, and Nmap
  - Multipurpose Reconnaissance Tools: Metasploit Framework, Maltego, and Recon-ng
  - Web Application Scanner Output: Burp Suite, ZAP, and Nikto
  - Vulnerability and Cloud Assessment Tool Output: Nessus, Nuclei, OpenVAS, ScoutSuite, Prowler, Trivy, and Checkov
  - Breach and Attack Simulation Output: Atomic Red Team and Caldera
- Applied activity: Given annotated screenshots of an Nmap scan and a Nessus findings report for the same host, learners reconcile the two outputs and identify which findings require follow-up first.

Module 8: Prioritizing and Mitigating Vulnerabilities

- Lessons:
  - Prioritization Criteria: Exploitability, Asset Value, and Impact

- Scoring Methods: CVSS and EPSS
- Context Awareness and False Positive and Negative Analysis
- Mitigation Strategies and Validating Remediation

- Applied activity: Given a short list of scored vulnerabilities with CVSS, EPSS, and asset criticality noted, learners rank them for remediation and justify the ranking, then propose a compensating control for one item that cannot be patched immediately.

Module 9: Controls, Risk, and Vulnerability Management Governance

- Lessons:
  - Control Types and Control Functions
  - Risk Concepts and Risk Management Strategies
  - Policies, Governance, and Service-Level Objectives
  - Application Security: SAST, DAST, and SAMM
  - Third-Party and Supply Chain Risk: SCA and SBOM
- Applied activity: Given a described application vulnerability found late in development, learners classify the control gap, recommend a risk management strategy, and identify whether SAST or DAST would have caught it earlier.

Module 10: Attack Methodology Frameworks

- Lessons:
  - The Cyber Kill Chain
  - The Diamond Model of Intrusion Analysis
  - Applying MITRE ATT&CK to Incident Analysis
- Applied activity: Given a short narrative of an attack, learners map the events to Cyber Kill Chain stages and to the Diamond Model's core features.

Module 11: The Incident Response Process

- Lessons:
  - Preparation and Detection
  - Analysis and Containment
  - Eradication and Recovery
  - Post-Incident Activities
- Applied activity: Given a timeline of an incident, learners label each described action with the correct incident response phase.

Module 12: Incident Response Planning, Roles, and Evidence Handling

- Lessons:
  - Developing Incident Response and Communication Plans
  - Playbooks, Roles, and Training: Tabletop and Simulation Exercises
  - Log Collection, Correlation, and Enrichment
  - Triage: Timeline, Severity, and Prioritization
  - Evidence Gathering: Chain of Custody, Preservation, and Legal Hold
- Applied activity: Given a set of raw, unordered log entries from different systems, learners correlate them into a timeline, assign a severity rating, and describe the chain-of-custody steps needed to preserve the evidence.

Module 13: Containment, Eradication, Recovery, and Root Cause Analysis

- Lessons:
  - Isolating Affected Targets and Escalation
  - Remediation, Verification, and Release from Isolation

- Performing Restoration
- Root Cause Analysis and Corrective Action Development

- Applied activity: Given a described incident that recurs after an initial fix, learners perform a root cause analysis, identify the true underlying cause, and propose a corrective action distinct from the original fix.

Module 14: Vulnerability Management Reporting and Communication

- Lessons:
  - Vulnerability Scan Reports, Compliance Findings, and Risk Scorecards
  - Action Plans, Escalation, and Dependencies
  - Inhibitors to Remediation: Legacy Systems, Contracts, and Business Impact
  - Stakeholder Identification and Communication
  - Metrics, KPIs, Trends, and Service-Level Agreements
- Applied activity: Given a mock vulnerability scorecard and a remediation delay caused by a legacy system, learners draft a short stakeholder communication that explains the inhibitor, the risk, and the proposed action plan.

Module 15: Security Operations and Incident Response Reporting and Communication

- Lessons:
  - Incident Declaration, Escalation, and Shift Handover
  - Executive Summaries and Internal Threat Intelligence Reporting
  - Stakeholder Communication: Legal, Public Relations, Regulators, Law Enforcement, and Customers
  - Post-Incident Reporting: After Action Reports and Lessons Learned
  - Security Operations Metrics and KPIs: Mean Time to Detect, Respond, and Remediate
- Applied activity: Given a completed incident timeline, learners draft a one-paragraph executive summary, identify which three stakeholders must be notified and why, and calculate a mean-time-to-respond figure from provided timestamps.