CompTIA PLA CySA+

(Cyber Security Analyst)

Hybrid Delivery Overview

CompTIA CySA+

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring.

Content

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to detect and analyse indicators of malicious activity, understand threat intelligence and threat management, respond to attacks and vulnerabilities, perform incident response, and report and communicate related activity. To attain the CySA+ certification, learners will be required to pass a 165-minute online exam (maximum of 85 multiple choice and performance based questions)

The CySA+ exam verifies you have the knowledge and skills required to:

- Control Security Operations - Improve processes in security operations, identify and analyse malicious activity using the appropriate tools and techniques
- Implement Vulnerability Management - Implement and analyse vulnerability assessments, prioritise vulnerabilities and make recommendations on mitigating attacks and vulnerability response
- Lead Incident Response and Management - Perform incident response activities and understand the incident management lifecycle
- Manage Reporting and Communication -Apply communication best practices in vulnerability management and incident response as it relates to stakeholders, action plans, escalation and metrics

Hybrid Delivery (Online Tutor Led and E-Learning Self Study):

- Induction session delivered remotely via Microsoft Teams.
- Live Tutor led knowledge and skills workshops via Microsoft Teams.
- Approximately 29 hours of directed learning.
- A minimum of 57 ½ hours self-study and practice
- **Examination:** Tutor led exam revision and preparation followed by exam.
- **E-Learning:** Supported by self-study e-learning and practice labs.

Pre-course Requirements

Prospective learners should have a minimum of four years of experience hands on experience as an incident response analyst or security operations centre (SOC) analyst and preferably have achieved the CompTIA Network+, Security+ or a similar qualification

Delivery Schedule – Week 1 – 15

Week 1 – Module 1: Understanding Vulnerability Response, Handling and Management	
Monday	**Self-Directed Study** Lesson 0 Course Introduction (60 mins) **Live Evening Sessions** Introduction / Welcome (60 mins)
Tuesday	**Self-Directed Study** Lesson 01A Understanding Cybersecurity Leadership (60 mins)
Wednesday	**Self-Directed Study** Lesson 01B Exploring Control Types and Methods (60 mins)
Thursday	**Self-Directed Study** Lesson 01C Explaining Patch Management Concepts (60 mins) **Live Evening Sessions** Information Security Concepts (60 mins)
Friday	**Self-Directed Study** Lesson 01D Module Quiz (30 mins)
Week 2 – **Module 2: Exploring Threat Intelligence** **Module 3 - System and Network Architecture**	
Monday	**Self-Directed Study** Lesson 02A Exploring Threat Actor Concepts (60 mins)
Tuesday	**Self-Directed Study** Lesson 03A Identifying Active Threats (60 mins)
Wednesday	**Self-Directed Study** Lesson 03B Exploring Threat-Hunting Concepts (60 mins)
Thursday	**Self-Directed Study**

	Lesson 03C Maintaining Operational Visibility (60 mins)
Friday	**Self-Directed Study** Lesson 03D Module Quiz (30 mins)
Week 3 – Module 4: Understanding Process Improvement in Security Operations	
Monday	**Self-Directed Study** Lesson 04A Exploring Leadership and Security Operations (60 mins)
Tuesday	**Self-Directed Study** LAB – Packet Analysis (60 mins)
Wednesday	**Self-Directed Study** Lesson 04B Understanding Technology for Security Operations (60 mins)
Thursday	**Self-Directed Study** LAB – Simple Packet Analysis (60 mins) **Live Evening Sessions** Module 1/2/3 Review? Q&A (60 mins) NIST Cyber Security Framework (60 mins)
Friday	**Self-Directed Study** Lesson 04D Module Quiz (30 mins)
Week 4 – Module 5: Implementing Vulnerability Scanning Methods	
Monday	**Self-Directed Study** Lesson 05A Explaining Compliance Requirements (60 mins)
Tuesday	**Self-Directed Study** Lesson 05B Understanding Vulnerability Scanning Methods (60 mins)
Wednesday	**Self-Directed Study** Lesson 05C Exploring Special Considerations in Vulnerability Scanning (60 mins)
Thursday	**Self-Directed Study**

	Lesson 05D Module Quiz (60 mins) **Live Evening Sessions** Computer Forensics and Legal Compliance: UK (120 mins) Threat Concepts / Social Engineering Insider Threats (120 mins)
Week 5 – BREAK	
Week 6 – Module 5: Performing Vulnerability Analysis	
Monday	**Self-Directed Study** Evaluation Quiz (60 mins)
Tuesday	**Self-Directed Study** Lesson 06A Understanding Vulnerability Scoring Concepts (60 mins)
Wednesday	**Self-Directed Study** Vulnerability Assessment Scoring (60 mins)
Thursday	**Self-Directed Study** Lesson 06B Exploring Vulnerability Context Considerations (60 mins) **Live Evening Sessions** Module 4/5 Review / Q&A / Quiz Review (60 mins) Vulnerability Assessment (60 mins)
Friday	**Self-Directed Study** Lesson 06C Module Quiz (60 mins)
Week 7 - Module 7: Communicating Vulnerability Information **Module 8: Explaining Incident Response Activities**	
Monday	**Self-Directed Study** Lesson 07A Explaining Effective Communication Concepts (60 mins)
Tuesday	**Self-Directed Study** Lesson 07B Understanding Vulnerability Reporting Outcomes and Action Plans (60 mins)
Wednesday	**Self-Directed Study**

	Lesson 08A Exploring Incident Response Planning (60 mins)
Thursday	**Self-Directed Study** Lesson 08B Performing Incident Response Activities (60 mins) **Live Evening Sessions** Incident Response Overview / NIST Computer Security Handling (120 mins)
Friday	**Self-Directed Study** Lesson 08C Module Quiz (30 mins)
Week 8 – Module 9 - Demonstrating Incident Response Communication	
Monday	**Self-Directed Study** Lesson 09A Understanding Incident Response Communication (60 mins)
Tuesday	**Self-Directed Study** LAB - Impact of Cyber Attack (60 mins)
Wednesday	**Self-Directed Study** Lesson 09B Analysing Incident Response Activities (60 mins)
Thursday	**Self-Directed Study** LAB – Cloud Computing Attacks (60 mins) **Live Evening Sessions** Module 6/7/8 Review / Q&A (60 mins) Access Control Terminologies and Principles (60 mins)
Friday	**Self-Directed Study** Lesson 09C Module Quiz (30 mins)
Week 9 – Module 10: Applying Tools to Identify Malicious Activity	
Monday	**Self-Directed Study** Lesson 10A Identifying Malicious Activity (60 Mins)
Tuesday	**Self-Directed Study** Lesson 10B Explaining Attack Methodology Frameworks (60 mins)

Wednesday	**Self-Directed Study** Lesson 10C Explaining Techniques for Identifying Malicious Activity (60 mins)
Thursday	**Self-Directed Study** Lesson 10D Module Quiz (30 mins) **Live Evening Sessions** Cyber Kill Chain Methodology / IoT Hacking Methodology (120 mins)
Week 10 – BREAK	
Week 11 – Analysing Potentially Malicious Activity	
Monday	**Self-Directed Study** Evaluation Quiz (60 mins)
Tuesday	**Self-Directed Study** Lesson 11A Exploring Network Attack Indicators (60 mins)
Wednesday	**Self-Directed Study** Lesson 11B Exploring Host Attack Indicators (60 mins)
Thursday	**Self-Directed Study** Lesson 11C Exploring Vulnerability Assessment Tools (60 mins) **Live Evening Sessions** Module 8/9/10 Review/ Q&A/ Quiz Review (60 mins) Wireless Hacking Methodology (60 mins)
Friday	**Self-Directed Study** Lesson 11D Module Quiz (30 mins)
Week 12 – Module 12: Understanding Application Vulnerability Assessments	
Monday	**Self-Directed Study** Lesson 12A Digital Forensics (60 mins)
Tuesday	**Self-Directed Study** LAB - Information Security Laws and Regulations (60 mins)

Wednesday	**Self-Directed Study** Lesson 12B Alerting and Monitoring Tools (60 mins)
Thursday	**Self-Directed Study** LAB - Fundamentals of Forensics (60 mins) **Live Evening Sessions** Incident Response Overview / NIST Computer Security Handling (120 mins)
Friday	**Self-Directed Study** Lesson 12C Module Quiz (30 mins)
Week 13 – Module 13: Exploring Scripting Tools and Analysis Concepts	
Monday	**Self-Directed Study** Lesson 13 A Physical and Network Attack Indicators (60mins)
Tuesday	**Self-Directed Study** LAB - Capturing Network Traffic (60 Mins)
Wednesday	**Self-Directed Study** Lesson 13B Policies, Standards and Procedures (60 mins)
Thursday	**Self-Directed Study** LAB - Windows Log Analysis (60 mins) **Live Evening Sessions** Module 11/12 Review / Q&A (60 mins) Impact of a Cyber Attack (60 mins)
Friday	**Self-Directed Study** Lesson 13C Module Quiz (30 mins)
Week 14 – Module 14: Understanding Application Security and Attack Mitigation Best Practices	
Monday	**Self-Directed Study** Lesson 14A Explore Secure Software Development Practices (60 mins)
Tuesday	**Self-Directed Study**

	Level 14B Recommending Controls to Mitigate Successful Application Attacks (60 mins)
Wednesday	**Self-Directed Study** Level 14C Implementing Controls to Prevent Attacks (60 mins)
Thursday	**Self-Directed Study** LAB – Directory Traversal (60 mins) **Live Evening Sessions** SQL Injection/ SQL Injection Countermeasures (120 mins)
Friday	**Self-Directed Study** Lesson 14D Module Quiz (30 mins)
Week 15 – EXAM WEEK	
Monday	**Self-Directed Study** Practice Test (60 mins)
Tuesday	**Self-Directed Study** Mock Test (120 mins)
Wednesday	**Self-Directed Study** Practice Test (60 mins)
Thursday	**Self-Directed Study** Practice Test (60 mins) **Live Sessions** Module 13/14 Review/Q&A (120 mins) CySa+ Course Review (120 mins) Open Q&A (60 mins)
Friday	**CompTIA Exam**