CompTIA CySA+ Syllabus

Lesson 1: Explaining the Importance of Security Controls and Security Intelligence — 2 Hours - 2 Topics

- Topic 1A: Identify Security Control Types (Day 1)
- Topic 1B: Explain the Importance of Threat Data and Intelligence (Day 1)

Lesson 2: Utilizing Threat Data and Intelligence — 2 Hours - 3 Topics

- Topic 2A: Classify Threats and Threat Actor Types (Day 2)
- Topic 2B: Utilize Attack Frameworks and Indicator Management (Day 2)
- Topic 2C: Utilize Threat Modeling and Hunting Methodologies (Day 2)

Lesson 3: Analyze Network Monitoring Output — 2 Hours - 4 Topics

- Topic 3A: Analyze Network Monitoring Output (Day 3)
- Topic 3B: Analyze Appliance Monitoring Output (Day 3)
- Topic 3C: Analyze Endpoint Monitoring Output (Day 3)
- Topic 3D: Analyze Email Monitoring Output (Day 3)

Lesson 4: Collecting and Querying Security Monitoring Data — 2 Hours - 2 Topics

- Topic 4A: Configure Log Review and SIEM Tools (Day 4)
- Topic 4B: Analyze and Query Logs and SIEM Data (Day 4)

Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques — 2 Hours - 5 Topics

- Topic 5A: Identify Digital Forensics Techniques
- Topic 5B: Analyze Network-related IOCs (Day 5)
- Topic 5C: Analyze Host-related IOCs (Day 5)
- Topic 5D: Analyze Application-related IOCs (Day 5)
- Topic 5E: Analyze Lateral Movement and Pivot IOCs (Day 5)

Lesson 6: Applying Incident Response Procedures — 2 Hours - 3 Topics

- Topic 6A: Explain Incident Response Processes (Day 6)
- Topic 6B: Apply Detection and Containment Processes (Day 6)
- Topic 6C: Apply Eradication, Recovery, and Post-incident Processes (Day 6)

Lesson 7: Applying Risk Mitigation and Security Frameworks — 2 Hours - 2 Topics

- Topic 7A: Apply Risk Identification, Calculation, and Prioritization Processes (Day 7)
- Topic 7B: Explain Frameworks, Policies, and Procedures (Day 7)

Lesson 8: Performing Vulnerability Management — 2 Hours - 4 Topics

- Topic 8A: Analyze Output from Enumeration Tools (Day 8)
- Topic 8B: Configure Infrastructure Vulnerability Scanning Parameters (Day 8)
- Topic 8C: Analyze Output from Infrastructure Vulnerability Scanners (Day 8)
- Topic 8D: Mitigate Vulnerability Issues (Day 8)

Lesson 9: Managing Post-Installation Administrative Tasks — 2 Hours - 4 Topics

- **Topic 9A: Apply Identity and Access Management Security Solutions (Day 9)**
- **Topic 9B: Apply Network Architecture and Segmentation Security Solutions (Day 9)**
- **Topic 9C: Explain Hardware Assurance Best Practices (Day 9)**
- **Topic 9D: Explain Vulnerabilities Associated with Specialized Technology (Day 9)**

Lesson 10: Understanding Data Privacy and Protection — 2 Hours - 2 Topics

- **Topic 10A: Identify Non-Technical Data and Privacy Controls (Day 10)**
- **Topic 10B: Identify Technical Data and Privacy Controls (Day 10)**

Lesson 11: Applying Security Solutions for Software Assurance — 2 Hours - 3 Topics

- **Topic 11A: Mitigate Software Vulnerabilities and Attacks (Day 11)**
- **Topic 11B: Mitigate Web Application Vulnerabilities and Attacks (Day 11)**
- **Topic 11C: Analyze Output from Application Assessments (Day 11)**

Lesson 12: Applying Security Solutions for Cloud and Automation — 2 Hours - 4 Topics

- **Topic 12A: Identify Cloud Service and Deployment Model Vulnerabilities (Day 12)**
- **Topic 12B: Explain Service-Oriented Architecture (Day 12)**
- **Topic 12C: Analyze Output from Cloud Infrastructure Assessment Tools (Day 12)**
- **Topic 12D: Compare Automation Concepts and Technologies (Day 12)**