CompTIA Cybersecurity Analyst CySA+

Security concepts, tools, and best-practice frameworks

A practical, student-friendly outline covering compTIA CySA+ CS0-003 Basics, compTIA CySA+ CS0-003 Domain 1 - Security Operations, compTIA Cy...

MODULES
6

LESSONS
84

FORMAT
Self-paced

Module Breakdown

MODULE 1

CompTIA CySA+ CS0-003 Basics

1.1 Course Introduction
1.2 Instructor Introduction
1.3 What is CySA
1.4 Exam Objectives
1.5 Cybersecurity Pathway
1.6 DoD Baseline Certfication

MODULE 2

CompTIA CySA+ CS0-003 Domain 1 - Security Operations

2.1 Domain 1 - Security Operations Overview
2.2 System and Network Architecture Concepts in Security Operations
2.3 Log Files
2.4 Operating Systems
2.5 Infrastructure Concepts
2.6 Network Architecture
2.7 Software Defined Networking
2.8 Whiteboard Discussion - Network Architectures
2.9 Identity and Access Management IAM Basics
2.10 Demonstration - IAM
2.11 Encryption
2.12 Sensitive Data
2.13 1.2 Analyze Indicators of Potentially Malicious Activity
2.14 Network Attack
2.15 Host Attacks

Module Breakdown (continued)

MODULE 2

CompTIA CySA+ CS0-003 Domain 1 - Security Operations (continued)

2.16 Application Related Attacks
2.17 Social Attacks
2.18 Tools or Techniques to Determine Malicious Activity Overview
2.19 Tools and Toolsets For Identifying Malicious Activity
2.20 Common Techniques
2.21 Programming Concerns
2.22 Threat-Intelligence and Threat-Hunting Concepts Overview
2.23 Threat Actors
2.24 Tactics, Techniques and Procedures
2.25 Confidence Levels IOC
2.26 Collection Sources
2.27 Threat Intelligence
2.28 Cyber Response Teams
2.29 Security Operations
2.30 Standardized Processes and Operations

MODULE 2

CompTIA CySA+ CS0-003 Domain 1 - Security Operations (continued)

2.31 Security Operations Tools and Toolsets
2.32 Module 2 Review

MODULE 3

CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management

3.1 Domain 2 - Vulnerability Management Overview
3.2 Vulnerability Discovery and Scanning
3.3 Asset Discovery and Scanning
3.4 Industry Frameworks
3.5 Mitigating Attacks
3.6 CVSS and CVE
3.7 Common Vulnerability Scoring System (CVSS) interpretation
3.8 CVE Databases
3.9 Cross Site Scripting (XSS)
3.10 Vulnerability Response, Handling, and Management
3.11 Control Types (Defense in Depth, Zero Trust)
3.12 Patching and Configurations
3.13 Attack Surface Management
3.14 Risk Management Principles
3.15 Threat Modeling
3.16 Threat Models

MODULE 3

CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management (continued)

3.17 Secure Coding and Development (SDLC)
3.18 Module 3 Review

Module Breakdown (continued)

MODULE 4

CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management

4.1 Domain 3 - Incident Response and Management Overview
4.2 Attack Methodology Frameworks
4.3 Cyber Kill Chain
4.4 Frameworks to Know
4.5 Incident Response and Post Reponse
4.6 Detection and Analysis
4.7 Post Incident Activities
4.8 Containment, Eradication and Recovery
4.9 Module 4 Review

MODULE 5

CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication

5.1 Domain 4 - Reporting and Communication Overview
5.2 Reporting Vulnerabilities Overview
5.2.1 Vulnerability Reporting
5.3 Compliance Reports
5.4 Inhibitors to Remediation
5.5 Metrics and KPI's
5.6 Incident Response Reporting and Communications Overview
5.7 Incident Declaration
5.8 Communication with Stakeholders
5.9 Root Cause Analysis
5.10 Lessons Learned and Incident Closure
5.11 Module 5 Review

MODULE 6

CompTIA CySA+ CS0-003 - Course Closeout

6.1 Course Closeout Overview
6.2 Practice Questions
6.3 Exam Process
6.4 Continuing Education
6.5 Course Closeout