ELYSIUM® ACADEMY
Milestone of Cognizance

Since 2007

PROFESSIONAL

VERSION 24

COMPTIA – CYBERSECURITY ANALYST+ (CS0-003)

ELYSIUM ACADEMY

COMPTIA – CYBERSECURITY ANALYST+ (CS0-003)

SR. CODE
EAPL/PROF/PRTC21

COURSE CODE
EAPCA

SUB CATEGORY
CYBER SECURITY & NETWORKING

TOTAL DURATION	THEORY TAKEN	PRACTICAL TAKEN
90 HOURS	20 HOURS	70 HOURS

COURSE DESCRIPTION

The goal of the Vision Training Systems-led CompTIA training certification course is to teach students how to use behavioural analytics to networks and devices in order to avoid, detect, and mitigate cybersecurity threats through ongoing security monitoring. After completing the CS0-002 exam, an IT professional can obtain the CompTIA CySA+ certification, which attests to their proficiency in proactively defending and continually enhancing an organization's security.

COURSE GOALS

The course is designed for Tier II security analysts, intermediate and mid-career cybersecurity experts, students holding a DoD IAT Level II or CSSP position, holders of the CompTIA Network+ or CompTIA Security+ certifications looking to advance, and anyone else looking to broaden their skill set and knowledge.

FUTURE SCOPE

The field is evergreen. As technology advances rapidly, there is an undeniable need for cyber security. As you begin to study and work, you will be able to gain an understanding of the upcoming trends and how to apply them in the field.

01
CHAPTER

12.5 HRS

14 HRS

SECURITY OPERATIONS

01.System and Network Architecture Concepts

a.Log ingestion

b.Operating system (OS) concepts

c.Infrastructure concepts

d.Network architecture

e. Identity and access management

f. Encryption

g. Sensitive data protection

02.Potentially Malicious Activity

a.Network-related

b.Host-related

c.Application-related

d.Other

03.Determine Malicious Activity

a. Tools

b. Common techniques

c. Programming languages/scripting

04.Threat-Intelligence and Threat-Hunting Concepts

a. Threat actors

b. Tactics, techniques, and procedures (TTP)

c. Confidence levels

d. Collection methods and sources

e. Threat intelligence sharing

f. Threat hunting

05.Efficiency and Process Improvement

a. Standardize processes

b. Streamline operations

c. Technology and tool integration

d. Single pane of glass

02 CHAPTER

VULNERABILITY MANAGEMENT

12.5 HRS

15 HRS

01.Implement Vulnerability Scanning Methods

a. Asset discovery

b. Special considerations

c. Internal vs. external scanning

d. Agent vs. agentless

e. Credentialed vs. non-credentialed

f. Passive vs. active

g. Static vs. dynamic

h. Critical infrastructure

i. Security baseline scanning

j. Industry frameworks

02.Vulnerability Assessment Tools

a. Tools

- Network scanning & Mapping
- Web application scanners
- Vulnerability scanners
- Debuggers
- Multipurpose
- Cloud infrastructure assessment tools

O3. Prioritize Vulnerabilities

a. Common Vulnerability Scoring System (CVSS) interpretation

b.Validation

c. Context awareness

d. Exploitability/weaponization

e. Asset value

f. Zero-day

O4.Software Vulnerabilities

a. Cross-site scripting

b. Overflow vulnerabilities

c. Data poisoning

d. Broken access control

e. Cryptographic failures

f. Injection flaws

g. Cross-site request forgery

h. Directory traversal

i. Insecure design

j. Security misconfiguration

k. End-of-life or outdated components

l. Identification and authentication failures

m.Server-side request forgery

n. Remote code execution

o. Privilege escalation

p. Local file inclusion (LFI)/remote file inclusion (RFI)

05.Vulnerability Response, Handling, and management

a. Compensating control

b. Control types

c. Patching and configuration management

d. Maintenance windows

e. Exceptions

f. Risk management principles

g.licies, governance, and service level objectives (SLOs)

h. Prioritization and escalation

i. Attack surface management

j. Secure coding best practices

k.Secure software development life cycle (SDLC)

l. Threat modeling

03 CHAPTER

INCIDENT RESPONSE AND MANAGEMENT

09 HRS

12 HRS

01.Attack Methodology Frameworks

a.Cyber kill chains

b.Diamond Model of Intrusion Analysis

c.MITRE ATT&CK

d.Open Source Security Testing Methodology Manual (OSS TMM)

e.OWASP Testing Guide

02.Perform Incident Response Activities

a. Detection and analysis

b. Containment, eradication, and recovery

03. Incident Management Life Cycle

a. Preparation

b. Post-incident activity

04
CHAPTER

REPORTING AND COMMUNICATION

06 HRS

09 HRS

01.Vulnerability Management Reporting and Communication

a. Vulnerability management reporting

b. Compliance reports

c. Action plans

d. Inhibitors to remediation

e. Metrics and key performance indicators (KPIs)

f. Stakeholder identification and communication

02.Incident Response Reporting and Communication

a.Stakeholder identification and communication

b.Incident declaration and escalation

c.Incident response reporting

d.Communications

e.Root cause analysis

f.Lessons learned

g.Metrics and KPIs

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

Placement Assistance 100%

135+ Professional Courses

Practical Sessions 90%

67+ Global Pacts

Corporate Placements 65%

170+ IT Companies Tie-Up

ELYSIUM GROUP OF COMPANIES ELYSIUM ACADEMY PRIVATE LIMITED

AUTHORIZED INTERNATIONAL Partners

Microsoft

CompTIA

CISCO

aws

Google

SUSE

ROCHESTON

C++