

KOENIG SOLUTIONS • COURSE OUTLINE

CompTIA Cybersecurity Analyst (CySA+)

Learn to monitor, detect, analyse and respond to cybersecurity threats using SIEM, vulnerability management and incident response practices.

5 Days

8 HOURS A DAY

23

MODULES

66

TOPICS

COURSE OVERVIEW

This course covers core security concepts, the modern threat landscape and threat intelligence fundamentals, followed by security monitoring, log management, SIEM and alert triage. It then addresses vulnerability management, scanning, scoring and malware analysis, before moving into incident detection, classification, digital forensics and recovery. The final modules cover security architecture, automation and orchestration, risk management and compliance, and threat hunting.

WHO THIS COURSE IS FOR

Security Operations Analysts

SOC Analysts

Incident Responders

Vulnerability Analysts

Threat Intelligence Analysts

Security Engineers

LEARNING OBJECTIVES

- Describe the SOC analyst role and SOC workflows
- Explain core security concepts including CIA triad and AAA
- Identify modern threats, malware types and attack vectors
- Interpret indicators of compromise and indicators of attack
- Analyse log sources and SIEM correlation rules and alerts
- Apply CVSS scoring to assess vulnerability risk and severity
- Plan incident response activities from detection to recovery
- Assess risk, compliance frameworks and threat hunting techniques

23 Modules, 66 Topics

DAY 1 Cybersecurity Foundations & Threat Landscape

Build core understanding of security concepts and modern threats

1.1

Introduction to CySA+ (CS0-004)

TOPICS

Exam objectives overview · Security Operations Analyst role · SOC structure and workflows

1.2

Core Security Concepts Refresher

TOPICS

- CIA triad & security principles
- Authentication, authorization, accounting (AAA)
- **Security controls:** preventive, detective, corrective

1.3

Threat Landscape

TOPICS

- Modern cyber threats (APT, ransomware, phishing)
- Malware types and behaviors
- Attack vectors and kill chain

1.4

Threat Intelligence Fundamentals

TOPICS

- Threat intelligence lifecycle
- Indicators of Compromise (IoC)
- Indicators of Attack (IoA)
- Threat intelligence sources (OSINT, dark web, internal logs)

Understand log sources, SIEM, and monitoring tools

2.1**Security Monitoring Concepts****TOPICS**

Continuous monitoring principles · SOC monitoring objectives

2.2**Log Management****TOPICS**

- Types of logs (network, endpoint, application, firewall)
- Log formats (syslog, JSON, Windows Event Logs)

2.3**SIEM Fundamentals****TOPICS**

SIEM architecture and components · Correlation rules · Dashboards and alerting

2.4**Data Sources & Sensors****TOPICS**

- IDS vs IPS
- EDR/XDR tools
- Network traffic analysis tools (Wireshark basics)

2.5**Alert Triage Basics****TOPICS**

Alert prioritization · False positives vs false negatives · Basic incident categorization

Identify, assess, and prioritize vulnerabilities

3.1**Vulnerability Management Lifecycle****TOPICS**

■ Discovery → Assessment → Remediation → Verification

3.2**Vulnerability Scanning Tools****TOPICS**

Authenticated vs unauthenticated scans · Tools overview (Nessus, OpenVAS concepts)

3.3**Vulnerability Scoring****TOPICS**

CVSS scoring system · Risk vs severity vs impact

3.4**Attack Surface Analysis****TOPICS**

Asset inventory · Exposure assessment

3.5**Malware & Behavioral Analysis Basics****TOPICS**

Static vs dynamic analysis · Sandbox environments · Fileless malware overview

Handle security incidents from detection to containment

4.1**Incident Response Lifecycle****TOPICS**

Preparation · Detection & Analysis · Containment · Eradication · Recovery · Lessons learned

4.2**Incident Classification & Handling****TOPICS**

Incident severity levels · Escalation procedures · Communication flow in SOC

4.3**Digital Forensics Basics****TOPICS**

Evidence collection principles · Chain of custody · Volatile vs non-volatile data

4.4**Response Tools & Techniques****TOPICS**

Endpoint isolation · Network containment strategies · IOC-based investigation

4.5

Recovery & Post-Incident Activities

TOPICS

System restoration · Root cause analysis · Reporting

DAY 5

Security Architecture, Automation & Exam Preparation

Integrate knowledge and prepare for exam success

5.1

Security Architecture Concepts

TOPICS

Network segmentation · Zero Trust model · Defense in depth

5.2

Automation & Orchestration

TOPICS

SOAR concepts · Playbooks and workflows · Security automation use cases

5.3

Risk Management & Compliance

TOPICS

Risk types (inherent, residual) · Policies, procedures, and governance · Compliance frameworks overview

5.4

Threat Hunting Basics

TOPICS

Hypothesis-driven hunting · Behavioral analytics · MITRE ATT&CK framework overview

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com