COURSE OUTLINE

Course Name: CompTIA Cybersecurity Analyst+

DURATION	SKILLS LEVEL	DILIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
5 Days	Intermediate	Instructor-Led	60	Data & Analytics

Course Description:

The CompTIA CyberSecurity Analyst (CySA+) certification is an intermediate-level certification designed to demonstrate the knowledge and competencies of a security analyst or specialist with four years' experience in the field.

This course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents.

The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyse cybersecurity intelligence, and handle incidents as they occur.

This course will also prepare participants for the CompTIA CySA+ certification examination.

Prerequisites:

Before attending this course, students should have:

- Network+, Security+ or equivalent knowledge.
- Minimum 3-4 years of hands-on information security or related experience.
- While there is no formal prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has technical, hands-on focus.

Target Audience:

- This course is primarily designed for students who are seeking the CompTIA CySA+ certification and who want to prepare for the CompTIA CySA+ CS0-002 certification exam.
- The course more generally supports candidates working in or aiming for job roles such as security operations centre (SOC) analyst, vulnerability analyst, cybersecurity specialist, threat intelligence analyst, security engineer, and cybersecurity analyst.

Learning Objectives:

On completion of the course, delegates will be able to:

- Collect and use cybersecurity intelligence and threat data.
- Identify modern cybersecurity threat actor's types and tactics, techniques, and procedures.
- Analyses data collected from security and event logs and network packet captures.
- Respond to and investigate cybersecurity incidents using forensic analysis techniques.
- Assess information security risk in computing and network environments.
- Implement a vulnerability management program.
- Address security issues with an organization's network architecture.
- Understand the importance of data governance controls.
- Address security issues with an organization's software development life cycle.
- Address security issues with an organization's use of cloud and service-oriented architecture.

Course Outline:

Lesson 1: Explaining the Importance of Security Controls and Security Intelligence

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

Lesson 2: Utilizing Threat Data and Intelligence

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

Lesson 3: Analysing Security Monitoring Data

- • Topic 3A: Analyse Network Monitoring Output
- Topic 3B: Analyse Appliance Monitoring Output
- Topic 3C: Analyse Endpoint Monitoring Output
- Topic 3D: Analyse Email Monitoring Output

Lesson 4: Collecting and Querying Security Monitoring Data

- Topic 4A: Configure Log Review and SIEM Tools
- Topic 4B: Analyse and Query Logs and SIEM Data

Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques

- Topic 5A: Identify Digital Forensics Techniques
- Topic 5B: Analyse Network related IoCs
- Topic 5C: Analyse Host-related IoCs
- Topic 5D: Analyse Application Related IoCs
- Topic 5E: Analyse lateral Movement and Pivot IoCs

Lesson 6: Applying Incident Response Procedures

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

Lesson 7: Applying Risk Mitigation and Security Frameworks

- Topic 7A: Apply Risk Identification, Calculation, and Prioritization Processes
- Topic 7B: Explain Frameworks, Policies, and Procedure

Lesson 8: Performing Vulnerability Management

- Topic 8A: Analyse Output from Enumeration Tools
- Topic 8B: Configure Infrastructure Vulnerability Scanning Parameters
- Topic 8C: Analyse Output from Infrastructure Vulnerability Scanners
- Topic 8D: Mitigate Vulnerability Issues
- Lesson 9 Applying Security Solutions for Infrastructure Management
- Topic 9A: Apply Identity and Access Management Security Solutions
- Topic 9B: Apply Network Architecture and Segmentation Security Solutions
- Topic 9C: Explain Hardware Assurance Best Practices
- Topic 9D: Explain Vulnerabilities Associated with Specialized Technology

Lesson 10: Understanding Data Privacy and Protection

- Topic 10A: Identify Non-Technical Data and Privacy Controls
- Topic 10B: Identify Technical Data and Privacy Controls

Lesson 11: Applying Security Solutions for Software Assurance

- Topic 11A: Mitigate Software Vulnerabilities and Attacks
- Topic 11B: Mitigate Web Application Vulnerabilities and Attacks
- Topic 11C: Analyse Output from Application Assessments

Lesson 12: Applying Security Solutions for Cloud and Automation

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

Associated Exam and Certifications:

This course will prepare students to take the **CompTIA Cybersecurity Analyst+ CS0-002 exam**.

Successfully passing this exam will result in the attainment of the **CompTIA Cybersecurity Certification.**

After completing this course students will receive a Netcampus course attendance certification.

The CompTIA Cybersecurity certification forms part of the of CompTIA CE Program and is valid for three (3) years from the day of your successful completion of the exam and there is requirement to renew the certification every 3 years.

Exams and Certifications

Notes and Annotations

What is Next