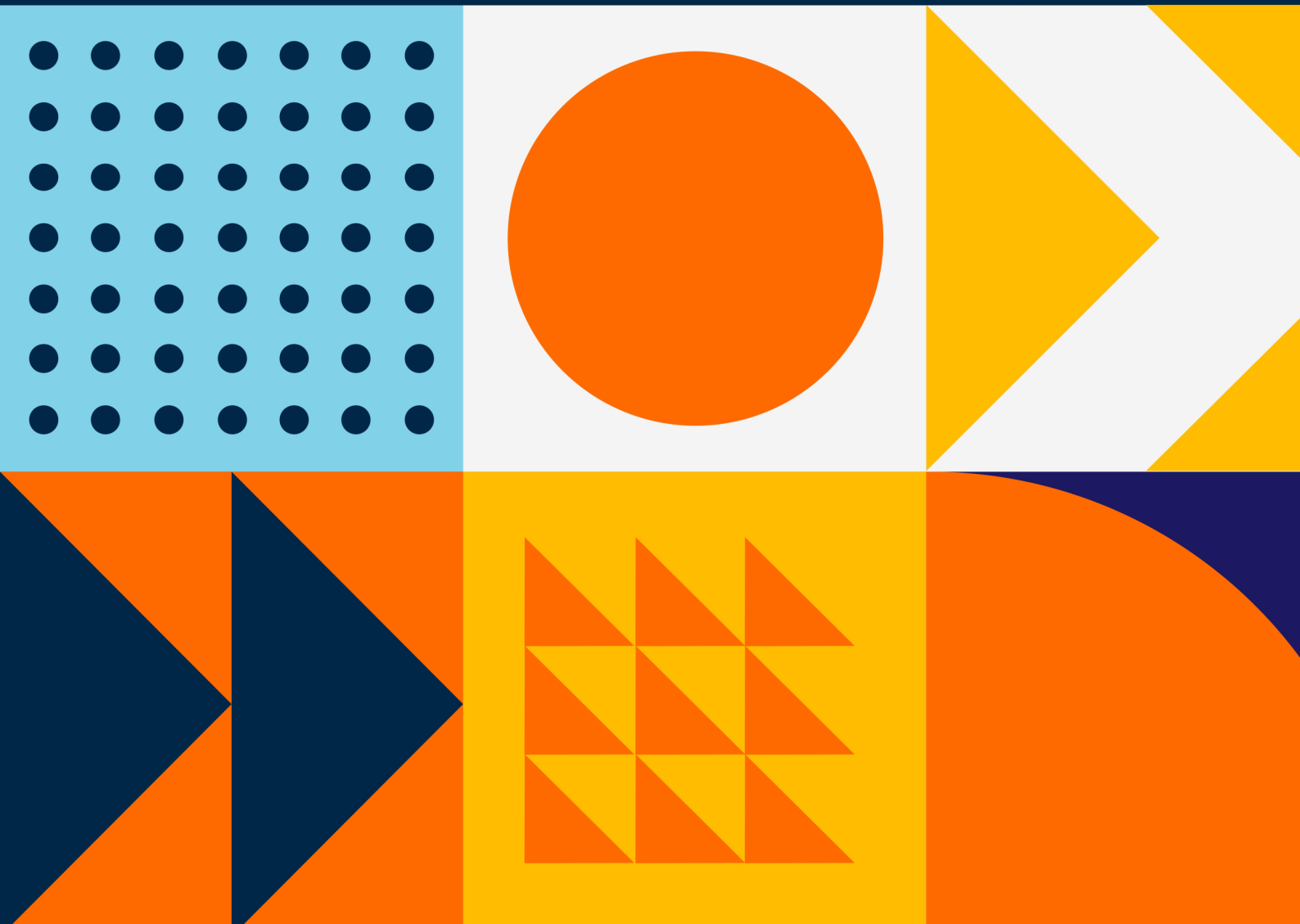




We do **IT**
to inspire.

Cyber Security:

**CompTIA Cybersecurity Analyst CySA+
Certification Training**





About Us

who we are.

Averest is one of the leading and fast-growing companies specialising in Information Technologies, Cyber Security, Cloud Computing, DevOps, Artificial Intelligence, Agile and Scrum, and Project Management, which is based in the United Kingdom and Turkey. Averest provides high-quality tech-accredited training and business solutions to its clients on these topics and more.



Why You Should Learn With Us?

We offer accredited Programs that are available for anyone wishing to acquire skills and gain professional certification to take their career to the next level.

- **100+ Premium Programs**

Choose the appropriate program, date and region for your occupation.

- **50+ World-Wide Accredited Certifications**

Get certified by global certification bodies and deepen your expertise.

- **500+ Expert Advisors**

Get together with professional trainers who are experts in their professions.

- **100.000+ Professionals Trained**

We help many of the world's leading companies to build their tech and digital capabilities.

Our partners.



To Explore More Please Visit [Our Website](#)

Program

CompTIA Cybersecurity Analyst CySA+ Certification Training

Overview

The CompTIA Cybersecurity Analyst (CySA+) training course will prepare you to successfully achieve this in-demand certification with hands-on, scenario-based training so you'll be ready to meet advanced persistent threats (APTs) head-on.

What You Will Learn?

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

Course Key Features

- One-on-one after course instructor coaching
- Earn 29 CompTIA CEUs
- Practice exam questions
- Exam voucher included

Program

CompTIA Cybersecurity Analyst CySA+ Certification Training

Eligibility

CompTIA Cybersecurity Analyst CySA+ Training is aimed at students seeking the CompTIA CySA+ certification who want to prepare for the CompTIA CySA+ CS0-002 certification exam. The system 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.

Program

CompTIA Cybersecurity Analyst CySA+ Certification Training

Program Outline

Explaining the Importance of Security Controls and Security Intelligence

- Identify Security Control Types
- Explain the Importance of Threat Data and Intelligence

Analyzing Security Monitoring Data

- Analyze Network Monitoring Output
- Analyze Appliance Monitoring Output
- Analyze Endpoint Monitoring Output
- Analyze Email Monitoring Output

Utilizing Digital Forensics and Indicator Analysis Techniques

- Identify Digital Forensics Techniques
- Analyze Network-related IoCs
- Analyze Host-related IoCs
- Analyze Application-Related IoCs
- Analyze Lateral Movement and Pivot IoCs

Utilizing Threat Data and Intelligence

- Classify Threats and Threat Actor Types
- Utilize Attack Frameworks and Indicator Management
- Utilize Threat Modeling and Hunting Methodologies

Collecting and Querying Security Monitoring Data

- Configure Log Review and SIEM Tools
- Analyze and Query Logs and SIEM Data

Applying Incident Response Procedures

- Explain Incident Response Processes
- Apply Detection and Containment Processes
- Apply Eradication, Recovery, and Post-Incident Processes

Program

CompTIA Cybersecurity Analyst CySA+ Certification Training

Applying Risk Mitigation and Security Frameworks

- Apply Risk Identification, Calculation, and Prioritization Processes
- Explain Frameworks, Policies, and Procedures

Applying Security Solutions for Infrastructure Management

- Apply Identity and Access Management Security Solutions
- Apply Network Architecture and Segmentation Security Solutions
- Explain Hardware Assurance Best Practices
- Explain Vulnerabilities Associated with Specialized Technology

Applying Security Solutions for Software Assurance

- Mitigate Software Vulnerabilities and Attacks
- Mitigate Web Application Vulnerabilities and Attacks
- Analyze Output from Application Assessments

Performing Vulnerability Management

- Analyze Output from Enumeration Tools
- Configure Infrastructure Vulnerability Scanning Parameters
- Analyze Output from Infrastructure Vulnerability Scanners
- Mitigate Vulnerability Issues

Understanding Data Privacy and Protection

- Identify Non-Technical Data and Privacy Controls
- Identify Technical Data and Privacy Controls

Applying Security Solutions for Cloud and Automation

- Identify Cloud Service and Deployment Model Vulnerabilities
- Explain Service-Oriented Architecture
- Analyze Output from Cloud Infrastructure Assessment Tools

Program

CompTIA Cybersecurity Analyst CySA+ Certification Training

- Compare Automation Concepts and Technologies

Program

CompTIA Cybersecurity Analyst CySA+ Certification Training

Program Schedule



LONDON

71-75 Shelton Street Covent Garden
London, United Kingdom WC2H 9JQ
+44 20 3967 83 79

ISTANBUL

Merkez Mah. Abide-i Hürriyet Cad. Blackout A Blok Kat:1
No:64 Sisli, Istanbul, Turkey 34381
+90 534 551 20 88
info@averesttraining.com