CyberSecurity Analyst (CySa+)

In this course, you'll learn how to analyse, monitor, and protect an organisation's infrastructure using threat-detection and threat-analysis tools.

course outline

IS THIS COURSE FOR YOU?

This course is designed for IT professionals seeking to develop their skills in cybersecurity analytics.

ABOUT THE COURSE

You'll learn the duties of cybersecurity analysts, who are the IT professionals responsible for monitoring and detecting security incidents in networks and information systems and for executing an appropriate response to such incidents.

You'll gain the skills and learn the tactics to identify various types of common threats, evaluate an organisation's security and manage its cybersecurity risks, collect and analyse security intelligence, and handle incidents as they occur.

This course offers a comprehensive approach to security aimed toward those who are on the front lines of defence.

This course will also help prepare you for the CompTIA CySa+ - Cybersecurity Analyst (CS0-003) certification exam.

AIMS AND OBJECTIVES

This course will prepare you for roles of greater responsibility in IT security, as well as for CompTIA's CySa+ certification exam.

PRE-REQUISITES

Network+ and Security+ or equivalent background with 3-4 years in information security or related experience.

CAREER PATH

This course and associated certification will stand you in good stead in roles that involve analysing, monitoring, and protecting an organisation's infrastructure.

COURSE CONTENT

Module 1 - Network Security Concepts
Module 2 - Managing Network Settings
Module 3 - Cloud Computing & Cybersecurity
Module 4 - Virtualisation & Container Security
Module 5 - Data Security Standards
Module 6 - Threat Intelligence
Module 7 - Managing Risk
Module 8 - Business Continuity
Module 9 - OS Process Management
Module 10 - Public Key Infrastructure
Module 11 - Authentication
Module 12 - Authorisation
Module 13 - Cryptography
Module 14 - Firewalls & Intrusion Detection
Module 15 - Hardening Techniques
Module 16 - Malware
Module 17 - Malicious Techniques & Procedures
Module 18 - Analysing Malicious Activity
Module 19 - Vulnerability & Penetration Testing
Module 20 - Secure Coding & Digital Forensics
Module 21 - Logging & Monitoring
Module 22 - Security & Network Monitoring

COURSE DURATION

50 hours. This will vary from individual to individual based on prior knowledge and ability.

Accredited cpd Centre

CPD POINTS: 50

CPD points awarded upon successful completion.

PITMAN TRAINING

Building careers for 180 years.

SPECIALISED TRAINING SINCE 1837