GTC International Consulting Limited
Riverbank House
1 Putney Bridge Approach
Fulham, London, SW6 3BQ
T: +44(0)2037055710
E:enquiries@thegtcgroup.com
W: www.thegtcgroup.com

Networking Security & Secure Architecture

COURSE OVERVIEW

The course delivers a detailed and practical exploration of how to design, implement, and maintain resilient network infrastructures that safeguard against modern cyber threats. It emphasizes the principles of secure architecture, network segmentation, access control, encryption, and secure communication protocols, while also addressing emerging trends such as zero-trust models, cloud-based networking, and software-defined networks (SDNs). Participants will gain insights into common vulnerabilities, attack vectors, and defense mechanisms, alongside exposure to global standards and best practices for securing enterprise networks.

WHO SHOULD ATTEND?

This course is designed for network administrators, system architects, cybersecurity engineers, IT managers, consultants and security analysts responsible for designing or managing secure infrastructures. It is also valuable for individuals pursuing careers in cybersecurity, professionals transitioning into network security roles, and business leaders who need a strong understanding of how secure architectures protect organizational assets and ensure compliance with global standards.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Explain the core principles of networking security and secure architectural design.
- Identify and mitigate common network vulnerabilities and attack techniques.
- Apply secure design practices including segmentation, access control, and encryption.
- Implement secure communication protocols and authentication mechanisms.
- Integrate zero-trust principles and cloud-native architectures for modern enterprises.
- Align network security strategies with international standards and compliance frameworks.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- The comprehensive study of network security fundamentals and secure architecture principles.
- The coverage of secure communication protocols (SSL/TLS, IPSec, HTTPS, VPNs).
- The implementation of network segmentation, firewalls, and intrusion detection/prevention systems.
- Deep dive into zero-trust architecture and secure cloud networking.
- Case studies on network breaches and defense strategies.
- Alignment with global standards such as ISO 27001, NIST, and CIS benchmarks.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.
1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded.