BLACKBIRD FOR TRAINING

The 5G Network Security: Safeguarding Next-Gen Connectivity

9 – 20 November 2026
Kuala Lumpur (Malaysia)



The 5G Network Security: Safeguarding Next-Gen Connectivity

Ref: 321582_164435 **Date:** 9 – 20 November 2026 **Location:** Kuala Lumpur (Malaysia) **Fees:** 8800 GBP

Why This Course

The deployment of 5G networks is transforming connectivity, enabling ultra-low latency services, massive IoT ecosystems, and cloud-native infrastructures. However, this evolution also introduces a significantly expanded threat surface. Virtualization, network slicing, edge computing, and distributed architectures demand a new generation of security strategies.

This intensive two-week program delivers a comprehensive and technically grounded understanding of 5G network security. Participants will explore 5G architecture, built-in security mechanisms, emerging vulnerabilities, and advanced protection models. Through practical discussions and applied technical analysis, the course prepares professionals to design, secure, and manage resilient 5G environments aligned with global standards and evolving threats.

What You'll Learn and Practice

By attending this program, you will be able to:

- Understand 5G network architecture and its security implications.
- Identify, assess, and mitigate 5G-specific threats and vulnerabilities.
- Implement robust security controls across core, RAN, cloud, and edge environments.
- Apply advanced protection strategies for virtualized and software-defined infrastructures.
- Ensure compliance with global security standards and regulatory frameworks.

The Program Flow

Day 1: Introduction to 5G Security

- Overview of 5G technology and architecture
- The evolving 5G threat landscape
- Key differences between 4G and 5G security models
- International standards and governing bodies

Day 2: 5G Security Architecture

- Security components of the 5G core network
- Radio Access Network RAN security principles
- Securing network slicing environments
- Edge computing security challenges



Day 3: Authentication and Access Control

- 5G authentication frameworks and protocols
- Subscriber identity protection and privacy mechanisms
- Access and mobility management security
- Applying Zero Trust principles in 5G environments

Day 4: Encryption and Data Protection

- 5G encryption standards and cryptographic mechanisms
- Key management and secure key distribution
- Establishing secure communication channels
- Ensuring data integrity and confidentiality

Day 5: NFV and SDN Security

- Security considerations in virtualized network functions
- Software-Defined Networking SDN risks and controls
- Container and microservices security
- Securing orchestration and automation platforms

Day 6: Threat Detection and Mitigation

- Common 5G attack vectors and exploitation techniques
- Intrusion detection and prevention strategies
- Security Information and Event Management SIEM systems
- Threat intelligence integration and incident analysis

Day 7: IoT and Device Security in 5G

- Protecting large-scale IoT deployments
- Secure device authentication and lifecycle management
- Over-the-air OTA updates and patch governance
- Best practices for IoT risk reduction

Day 8: Cloud and Edge Security in 5G

- Multi-access Edge Computing MEC security models
- Cloud-native security controls
- API and microservices protection strategies
- Data privacy in distributed architectures



Day 9: Emerging Technologies and Future Trends

- Artificial intelligence and machine learning in threat detection
- Quantum-resistant cryptographic approaches
- Blockchain applications in telecom security
- Preparing for next-generation 6G security considerations

Day 10: Compliance, Regulations, and Best Practices

- Global 5G security regulations and industry standards
- Privacy and data protection requirements
- Conducting security audits and risk assessments
- Implementing best-practice security frameworks

Individual Impact

Participants will leave the program with:

- The capability to design and secure modern 5G architectures.
- Advanced skills in threat identification and mitigation.
- A practical understanding of virtualized and cloud-native security controls.
- Confidence in aligning 5G deployments with regulatory and compliance requirements.

Organizational Impact

Organizations will benefit from:

- Stronger protection of 5G infrastructure and services.
- Reduced exposure to evolving cyber threats.
- Improved compliance with international standards and data protection regulations.
- Enhanced readiness for emerging technologies and future network generations.

Training Methodology

- Expert-led technical sessions grounded in telecom security practice
- Architecture deep dives and threat modeling exercises
- Real-world attack scenario discussions
- Framework-based workshops for implementation planning

Beyond the Course

By the end of the two weeks, participants will be equipped to:



• Architect secure and resilient 5G networks.
• Integrate advanced cybersecurity technologies into telecom environments.
• Proactively address emerging risks and evolving threat landscapes.
• Support long-term security governance across next-generation network infrastructures.

