Advanced 5G Core Network Security and Cyber Defense Training Course



26 - 30 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #TEL4517_145867

Course Introduction / Overview:

The transition to 5G represents a monumental leap in telecommunications, enabling unprecedented connectivity and innovation across industries. However, this evolution from centralized hardware to a distributed, software-defined, and cloud-native architecture introduces a complex and expanded threat landscape. This course provides a comprehensive exploration of the 5G core network's security architecture and the sophisticated cyber defense mechanisms required to protect it. We delve into the intricacies of the Service-Based Architecture (SBA), Network Function Virtualization (NFV), and Software-Defined Networking (SDN) that form the backbone of 5G. As discussed by leading experts like Dr. Anand R. Prasad in works such as "Security in Next Generation Mobile Networks," securing this new ecosystem requires a proactive and multi-layered approach. BIG BEN Training Center has designed this program to move beyond theoretical knowledge, equipping participants with practical skills to identify vulnerabilities, analyze threats, and implement robust security controls. This training covers everything from 3GPP security standards and identity management to advanced topics like network slicing security, MEC protection, and developing a resilient incident response strategy for the 5G era.

Target Audience / This training course is suitable for:

- Telecommunications Engineers and Architects.
- Cybersecurity Analysts and Consultants.
- Network Security Engineers.
- Security Operations Center (SOC) personnel.
- IT Professionals involved in 5G deployment.
- Government and Military Communications Specialists.
- System Integrators and Network Administrators.
- Technical Managers overseeing network infrastructure.

Target Sectors and Industries:

- Telecommunication Service Providers.
- Managed Security Service Providers (MSSPs).
- Internet of Things (IoT) and Smart City Solution Providers.
- Critical Infrastructure sectors (Energy, Utilities, Transportation).
- Government, Defense, and Public Safety Agencies.
- Automotive and Autonomous Vehicle Technology.
- Healthcare and Remote Medicine Providers.
- Financial Services and Banking.

Target Organizations Departments:

- Network Operations and Engineering.
- Cybersecurity and Information Security.
- Security Operations Center (SOC).
- Information Technology (IT) and Infrastructure.
- Research and Development (R&D).
- Risk Management and Compliance.
- Incident Response and Digital Forensics.
- Technical Strategy and Planning.

Course Offerings:

By the end of this course, the participants will have able to:

- Analyze the 5G security architecture and its key components based on 3GPP standards.
- Identify and mitigate vulnerabilities within the 5G core network functions (AMF, SMF, UPF).
- Implement robust security controls for network slicing and Multi-access Edge Computing (MEC).
- Secure the Service-Based Architecture (SBA) and its API-driven communications.
- Master subscriber identity management techniques, including SUPI/SUCI privacy protection.
- Develop and apply 5G-specific threat intelligence and intrusion detection strategies.
- Design a comprehensive cyber defense framework using a zero-trust security model.
- Formulate an effective incident response and recovery plan for 5G network security breaches.
- Evaluate the security implications of integrating 5G with IoT and cloud-native technologies.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster deep understanding and practical skill acquisition through an immersive and interactive learning environment. This course moves beyond traditional lectures by integrating a dynamic blend of expert-led instruction, real-world case study analysis, and collaborative group workshops. Participants will engage in detailed discussions on recent 5G security incidents and architectural vulnerabilities, allowing them to connect theoretical concepts to practical challenges. The curriculum incorporates hands-on simulated lab sessions where attendees can apply security principles to configure and defend virtualized 5G network components. Team-based exercises will challenge participants to develop cyber defense strategies and incident response plans for various threat scenarios. This active learning approach, facilitated by experienced instructors, ensures that every participant not only grasps the complex material but also builds the confidence to apply these critical skills directly within their professional roles. Continuous feedback and Q&A sessions are integral to the process, creating a supportive atmosphere for mastering 5G security.

Course Agenda (Course Units):

Unit One: Foundations of 5G Architecture and Security Landscape

- Introduction to 5G technology and its evolution from 4G.
- Deep dive into the 5G System Architecture (5GS) and Service-Based Architecture (SBA).
- Understanding Network Function Virtualization (NFV) and Software-Defined Networking (SDN) in 5G.
- The expanded 5G threat landscape and new attack vectors.
- Overview of 3GPP security standards for 5G (Release 15, 16, and 17).
- Key security principles: confidentiality, integrity, and availability in the 5G context.
- Authentication and Key Agreement (AKA) protocol enhancements in 5G.

Unit Two: Securing the 5G Core Network

- Security architecture of the 5G Core (5GC) network functions.
- Securing the Access and Mobility Management Function (AMF).
- Protecting the Session Management Function (SMF) and User Plane Function (UPF).
- Subscriber identity management: SUPI, SUCI, and privacy considerations.
- Security protocols for the user plane (GTP-U) and control plane (PFCP).
- Inter-network security with roaming partners and the Security Edge Protection Proxy (SEPP).
- Securing network repositories and data storage (UDR, UDM).

Unit Three: Advanced 5G Security Domains

- The concept of Network Slicing and its security implications.
- Implementing security isolation and controls for network slices.
- Securing Multi-access Edge Computing (MEC) environments.
- Protecting applications and data at the network edge.
- Security for the Service-Based Architecture (SBA) and API protection.
- Implementing OAuth 2.0 and TLS for secure service communication.
- Security challenges in cloud-native 5G deployments and container security.

Unit Four: 5G Cyber Defense and Threat Mitigation

- Developing a 5G-specific threat intelligence program.
- Intrusion Detection and Prevention Systems (IDS/IPS) for the 5G environment.
- Security monitoring, logging, and analytics in the 5G core.
- Implementing a Zero-Trust Security model in a 5G network.
- Security Orchestration, Automation, and Response (SOAR) for 5G security operations.
- Denial of Service (DoS/DDoS) attack vectors and mitigation techniques in 5G.
- Proactive vulnerability management and penetration testing for 5G infrastructure.

Unit Five: Incident Response and Future Security Trends

- Developing a 5G Security Incident Response Plan (SIRP).
- Digital forensics and investigation techniques for virtualized network functions.
- Coordination with law enforcement and regulatory bodies.
- The impact of Quantum Computing on 5G cryptography and future-proofing strategies.
- The role of Artificial Intelligence (AI) and Machine Learning (ML) in 5G security.
- Securing massive IoT deployments on 5G networks.
- Course review, final assessment, and strategic roadmap development.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As 5G networks become increasingly decentralized with MEC and network slicing, how can traditional, centralized security models evolve to provide effective, real-time threat mitigation without compromising performance and latency goals?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by offering a holistic, end-to-end perspective on 5G security that bridges the gap between architectural theory and practical cyber defense. While many courses focus narrowly on 3GPP standards or specific network functions, this program integrates these elements into a comprehensive security framework. We emphasize the operational realities of securing a distributed, software-defined network, dedicating significant time to advanced domains like network slicing, MEC security, and the protection of the API-driven Service-Based Architecture. The curriculum is uniquely structured to build skills progressively, from foundational principles to sophisticated defense strategies like implementing a zero-trust model and leveraging SOAR within a 5G context. A key differentiator is our focus on proactive defense and incident response, equipping participants not just to build secure networks, but to actively monitor, hunt for threats, and respond effectively to breaches in a virtualized environment. By examining real-world threat scenarios and future challenges like quantum computing, the course prepares professionals for the long-term evolution of 5G security, making it an unparalleled strategic investment in professional development.