CONCEPT

5G Network Security: Core Architecture, Network Slicing and Private 5G

5G Network Security: Core Architecture, Network Slicing and Private 5G

Introduction:

5G network security fails when operators and enterprises treat a service-based core, shared slices and edge sites as a faster copy of 4G. Exposed APIs, weak inter-network signalling filters, poorly isolated slices and unverified vendor software open paths that perimeter firewalls never see. This Core Concept course trains engineers to map the 5G architecture from NR radio to the cloud-native core, apply the 3GPP security architecture, test and monitor network functions and slices, and secure private 5G deployments. Participants build a 5G Security Plan and Network Function Hardening Checklist in a lab environment.

Course Objectives:

- Map a 5G deployment across NR radio, transport, core network functions and reference points, distinguishing NSA and SA options and their security consequences
- Apply the TS 33.501 security architecture to authentication, subscriber identity concealment, key hierarchy and protection of the service-based interfaces
- Assess network slices and edge computing sites for isolation, resource separation and lifecycle security weaknesses
- Analyse signalling, roaming, API exposure and supply chain threats against a threat-to-asset map of the 5G system
- Configure test and monitoring procedures that verify network function hardening and detect abnormal signalling and slice behaviour
- Build a 5G Security Plan and Network Function Hardening Checklist for an operator or private 5G network

Target Audience:

- Telecom engineers who plan, integrate and operate 5G radio access and core networks
- Network engineers responsible for transport, routing and interconnection of 5G sites and data centres
- Security engineers who assess, harden and monitor mobile network infrastructure
- Engineers deploying private 5G networks for industrial campuses, ports, airports and utilities
- Cloud and platform engineers running virtualised and containerised 5G core network functions

Course Outline:

Day 1: 5G System Architecture and Deployment Options

- 5G NR Frequency Ranges FR1 and FR2 and gNB Functional Split into CU and DU
- Non-Standalone Versus Standalone Deployment and the Role of the X2 and Xn Interfaces
- TS 23.501 Service-Based Architecture and Control and User Plane Separation
- 5G Core Network Functions: AMF, SMF, UPF, UDM, NRF, NSSF, PCF and NEF
- Current-State Assessment of an Existing 4G to 5G Migration Path

Day 2: 3GPP Security Architecture and Authentication

- TS 33.501 Security Domains and the Role of AUSF, SEAF and UDM
- Primary Authentication with 5G-AKA and EAP-AKA' Message Flows
- SUPI Concealment Using SUCI and Home Network Public Key Handling
- 5G Key Hierarchy and NAS and AS Integrity and Confidentiality Protection
- Service-Based Interface Protection with TLS, OAuth 2.0 Token Authorisation and SEPP for Roaming

Day 3: Securing Slices, Edge Sites and the Cloud-Native Core

- Network Slice Selection with S-NSSAI and NSSF and Slice-Specific Authentication
- Inter-Slice Isolation Controls Across Radio, Transport and Core Resources
- Multi-Access Edge Computing Site Placement, Local Breakout and UPF Exposure
- NFV and Container Platform Hardening for Core Network Functions
- Network Exposure Function API Security and Third-Party Application Onboarding

Day 4: 5G Threat Landscape, Private Networks and Monitoring

- ENISA 5G Threat Taxonomy and Threat-to-Asset Mapping
- Signalling Attacks on N2, N11 and Roaming Interconnect Interfaces
- Supply Chain and Vendor Software Integrity Risks in Multi-Vendor 5G Builds
- Private 5G Network Design for Enterprise Campuses and Integration with IT Security Zones
- Security Monitoring of NRF Registrations, Signalling Anomalies and Slice Performance Counters

Day 5: 5G Security Lab and Final Deliverable

- Lab: Tracing a 5G Registration and Authentication Call Flow in a Test Core
- Lab: Testing Slice Isolation and NEF API Access Controls
- Mobile Operator Case: Hardening a Service-Based Core Against Signalling Abuse
- Manufacturing and Logistics Case: Securing a Private 5G Campus Network
- 5G Security Plan and Network Function Hardening Checklist Peer Review

Skills You Will Gain:

- 5G Core Architecture Mapping
- 3GPP Authentication Flow Analysis
- Network Slice Isolation Assessment
- Edge Computing Security Design
- Service-Based Interface Hardening
- 5G Signalling Threat Analysis
- Private 5G Security Architecture
- Mobile Core Security Monitoring

Why Attend This Course:

- Leave with a 5G Security Plan and Network Function Hardening Checklist ready to apply to an operator or private network
- Read 5G call flows and security logs with confidence because authentication, key derivation and slice selection are traced hands on
- Question vendor and integrator designs on slicing, edge exposure and API access before they reach production
- Compare 5G security practice with engineers from operators, utilities, ports, manufacturing and government networks

Conclusion:

A 5G network is only as secure as its weakest network function, interface or slice. This course moves from NR radio and deployment options, through the 3GPP security architecture and authentication procedures, to slicing, edge computing, cloud-native core hardening, signalling and supply chain threats, private 5G and monitoring. The final day applies these methods in lab exercises and operator and enterprise cases, producing a 5G Security Plan and Network Function Hardening Checklist that engineers can use to guide design reviews, tests and operations.