Matrix-Shell

CASE STUDY

Securing a 5G RAN Environment

Strengthening Network Visibility, Device Trust, and Security Posture in a Live 5G RAN Environment

Executive Overview

A telecom operator engaged Matrix Shell Technologies to perform a security assessment of its 5G Radio Access Network (RAN) environment. The objective was simple: identify weaknesses before attackers could exploit them. During the assessment, our team uncovered critical security gaps that exposed internal network information and allowed unauthorized devices to interact with the network using manipulated identities.

By validating real-world attack scenarios and providing targeted remediation guidance, Matrix Shell helped the client strengthen network security, improve device authentication controls, and reduce the overall attack surface.

Challenge

As telecom networks evolve, maintaining visibility without exposing sensitive infrastructure becomes increasingly important.

During the assessment, two major security concerns were identified:

Internal Route Information Exposure

The network was unintentionally revealing internal IP addresses, network paths, and service information to external traffic.

This information could provide attackers with valuable insight into the network architecture, making targeted attacks significantly easier.

Weak Device Identity Validation

The network was also accepting altered or fake IMEI numbers during device registration.

Without proper validation, unauthorized devices could potentially gain access to network services while concealing their true identity.

Together, these issues increased security risk, reduced accountability, and created opportunities for unauthorized access or network abuse.

Objectives

Matrix Shell's assessment focused on:

- Identifying security weaknesses within the 5G RAN environment
- Validating real-world attack scenarios safely
- Evaluating routing and network exposure risks
- Assessing device authentication and identity controls
- Measuring potential business and operational impact
- Providing practical remediation recommendations

Solution

Matrix Shell conducted a comprehensive security assessment of the 5G RAN infrastructure using controlled testing methodologies and real-world attack simulations.

The engagement focused on validating how effectively the network protected critical infrastructure and authenticated connecting devices.

Key Areas Assessed

Infrastructure Exposure Analysis

- Network route validation
- Internal IP exposure testing
- Service and port enumeration
- Network segmentation review

Device Authentication Assessment

- IMEI validation testing
- Registration workflow analysis
- Identity spoofing validation
- Access control evaluation

The assessment provided clear visibility into how attackers could potentially gather intelligence or bypass security controls if weaknesses remained unaddressed.

Testing Process

Step 1

Environment Assessment

Matrix Shell reviewed the 5G RAN environment and identified potential attack paths within the authorized scope.

Step 2

Security Validation

Controlled testing was performed to validate whether identified weaknesses could be exploited in real-world scenarios.

Step 3

Impact Analysis

Each finding was analyzed to determine its potential impact on network security, operations, and service availability.

Step 4

Remediation Planning

The team provided prioritized recommendations to eliminate identified risks and strengthen security controls.

Step 5

Security Improvement Roadmap

A structured remediation roadmap was delivered to support long-term security enhancements across the RAN environment.

Results & Impact

Key Findings

Reduced Attack Surface

By addressing exposed services, routing disclosures, and identity validation weaknesses, the client gained a significantly more secure network posture.

Better Security Visibility

The assessment provided a clear understanding of potential risks, allowing security teams to prioritize remediation efforts more effectively.

Enhanced Operational Confidence

The client received actionable recommendations that supported both immediate risk reduction and long-term security improvements.

Critical Exposure Identified

Matrix Shell successfully identified and validated multiple high-risk security findings before they could be exploited by threat actors.

Improved Infrastructure Protection

The assessment highlighted areas where sensitive routing and network information required stronger protection, helping reduce reconnaissance opportunities for attackers.

Stronger Device Authentication

The findings enabled the client to strengthen device validation mechanisms and improve trust in network registration processes.

Conclusion

Telecom networks face increasingly sophisticated threats, making proactive security validation essential. Through a focused assessment of the 5G RAN environment, Matrix Shell Technologies identified critical security weaknesses related to infrastructure exposure and device identity validation.

By uncovering these risks early and delivering practical remediation guidance, Matrix Shell helped the client strengthen network security, improve trust in connected devices, and build a more resilient telecom infrastructure for the future.