How Telecom Argentina took a proactive stand to validate the security of its mobile network

NOKIA | personal

The starting point

A network in constant motion

Telecom Argentina runs a nationwide mobile network that serves around **20 million mobile subscribers**. As the network evolved through regular software updates, new roaming arrangements and changing traffic patterns, different parts of the system began to interact in new ways. This is normal for a large telecom provider, but it also means some behaviors can change in ways routine operational monitoring doesn't immediately surface.

The team wanted a **clearer sense of how their network would hold up against the threats operators face today**. Nothing seemed amiss, but with so much ongoing change, it felt like the right moment to step back and validate their assumptions.

With that goal, Telecom Argentina decided to conduct a **comprehensive assessment of their security posture** with support from an external global telco cybersecurity expert.

That's when they turned to Nokia.

The goal

A clear picture of exposure

Telecom Argentina wanted to go beyond assumptions and gain a concrete understanding of how their environment would hold up against today's telecom specific threats. They wanted to see how the live network would behave when subjected to realistic attack techniques, from roaming and signaling abuse to cross domain probing.

Their aim was to **confirm that recent changes hadn't introduced unseen risks, verify where existing safeguards were performing as expected**, and **identify where targeted improvements would have the greatest impact.**

As Marcelo Januszewski, Lead Business Information Security Officer (BISO) at Telecom Argentina put it:

"We didn't need a theoretical picture. We wanted to see how the network behaves when someone really tries to test it."

The solution

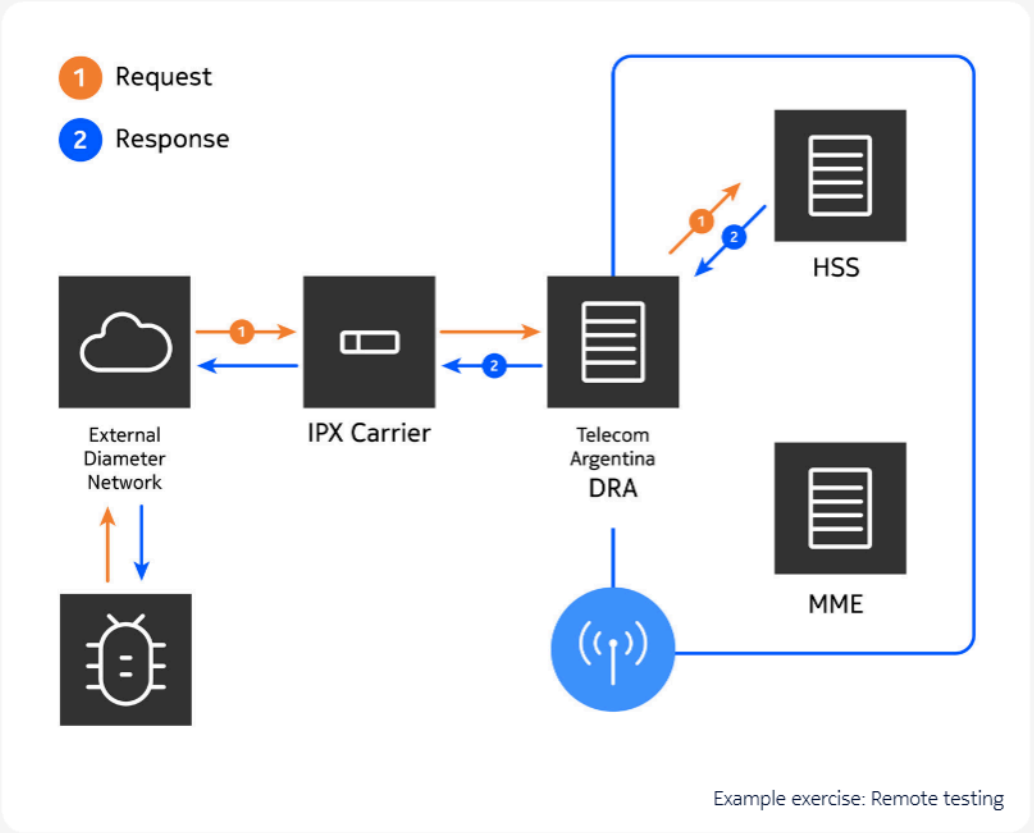
How Nokia and Telecom Argentina carried out the assessment

To understand the network's real exposure, Nokia and Telecom Argentina performed a validation of security controls using **telecom-specific attack techniques** that could realistically occur across roaming, core, transport, and radio domains. The goal was to uncover any gaps or risks that weren't visible to Telecom Argentina at the outset.

The work followed a gray-box methodology, giving Nokia enough context to run meaningful scenarios while still approaching the network the way an external attacker or untrusted partner might. Each exercise was designed to reveal how different parts of the network behaved under specific conditions and whether any weaknesses could be exposed through real-world methods.

The cyber-assessment covered **roaming and voice protocols, core network functions, transport and radio behavior, mobile infrastructure, and the operator's protection mechanisms**. Every assessment chapter produced clear evidence: what was attempted, how the network responded, where defenses held strong, and where improvements would reduce risk.

All point of improvements - including severity, impact, and recommended steps - were documented in a structured report, giving Telecom Argentina a clear picture of actual exposure and actionable next steps.



Example exercise: Remote testing

The outcome

What Telecom Argentina gained

The assessment gave Telecom Argentina a more accurate understanding of how its mobile network responds to real-world telecom threats. By **observing the live environment under conditions that mirror actual attacker techniques**, Telecom Argentina could see its network behave in ways that routine monitoring doesn't reveal.

Findings from each exercise were captured in both **technical and executive reports**, outlining improvement areas, associated risks, observed behavior, and recommended steps, all mapped to industry frameworks such as GSMA, MITRE, 3GPP, and CIS.

With this level of visibility, Telecom Argentina now has a far more complete picture of its attack surface and a precise understanding of where targeted improvements will have the greatest impact. This puts the company in a stronger position to:

- Maintain continuity of operations even in the face of emerging cyber threats
- Respond to and resolve security events more quickly and effectively
- Reinforce its reputation as a secure and reliable service provider
- Stay prepared for threats that attempt to compromise networks through signaling, roaming, or infrastructure weaknesses

Reflecting on the engagement, Marcelo Januszewski, Lead Business Information Security Officer (BISO) at Telecom Argentina noted:

"The work, experience and tools provided by Nokia gave us a level of visibility that we simply could not have achieved on our own. The assessment was realistic, pragmatic and immediately applicable. It strengthened our security and our confidence."

With this clarity, Telecom Argentina moves forward with a more confident and informed approach to security, and a stronger foundation for protecting its customers as the network continues to evolve.

Learn more about Nokia's
Advanced Cybersecurity Consulting Services

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 215319

nokia.com

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, we're advancing connectivity to secure a brighter world.