



NOKIA

How an Asian mobile network operator
gained full visibility into the security
posture of its 4G and 5G networks

Advanced Consulting Services
Security

Case study

Background

Cyber threats are increasingly persistent, complex, and sophisticated. At the same time, the security regulations that communications service providers (CSP) must comply with are more stringent than ever before. If CSPs are to meet those demands and deliver the best possible services to customers, they need much greater visibility into the security posture of their networks and the potential risks they face — but many lack the in-house expertise or resources to generate the insights required to do so.

Using an established security framework proven for telco operators, Nokia Consulting Services identified key security gaps, risks, and vulnerabilities for our customer. We provided recommendations on how the customer can evolve its 4G and 5G security posture to meet high-quality standards.

Business benefits



Complete visibility into 4G and 5G security controls



In-depth assessment of key security gaps and vulnerabilities



Demonstrated compliance to best-in-class telecom security requirements



Comprehensive action plan for security improvements



The customer challenge

Our customer is a large mobile network operator in Asia, providing service to millions of mobile subscribers. Like other CSPs in the region, it sets a high standard for itself, striving to provide the most secure and reliable service possible to all of its customers. That goal will become even more important as they expand into 5G and offer services to more enterprise customers.

5G is technically more complex to manage and protect than 4G. Because it is so open and interconnected with other systems, the attack surface is greatly expanded, exposing CSPs and their customers to more pervasive and sophisticated attacks from a vast range of malicious actors. There are also more security regulations, standards,

and frameworks to comply with than ever before — NIST, 3GPP, ETSI, ISO, CIS, CSA and others — all of which are placing increasingly stringent requirements on how CSPs need to protect their networks and data.

To win new business in its target markets, this operator needed to achieve Tier 4 certification for both its existing 4G infrastructure and planned 5G expansion according to the NIST cybersecurity framework. But like many other CSPs, our customer didn't have the in-house resources or expertise to properly assess whether it could meet the NIST requirements or what improvements would have to be made to its security posture to get there.

Our customer required comprehensive world-class risk assessment to help guide its decisions, as it looked to improve the security readiness of its planned 5G network



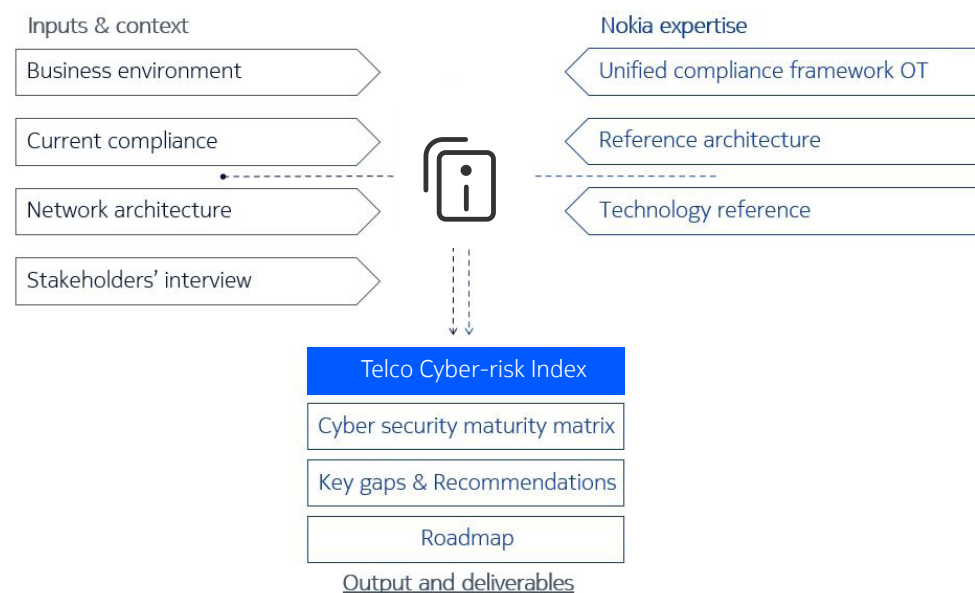
How Nokia helped

Drawing on its unique combination of cybersecurity and 4G/5G networking expertise, Nokia Security Consulting Services conducted a comprehensive, end-to-end assessment of the security posture and readiness of our customer's existing 4G network and its planned 5G expansion.

Using the NIST cybersecurity framework as a guide, Nokia started with document reviews and interviews with key customer team members to better understand the CSP's current security profile, including its business drivers and compliance mandates. Nokia then performed a thorough gap analysis to identify areas where the customer's network could be vulnerable to threats.

Potential security gaps were classified into nine main categories covering critical security control domains:

- Risk management
- General security concepts (e.g., firewalls, zero-trust communications)
- Network hardening
- Privileged access management and role-based access control
- Supply chain and software trustworthiness
- Roaming security
- DDoS/malware
- Personal identifiable information
- Security monitoring and incident detections



Nokia identified 27 security gaps in total and provided in-depth actions plans and roadmaps to address each one.

Instead of looking at each gap and vulnerability in isolation, Nokia's experts can see how they interconnect and affect each other — and their broader implications across all aspects of customer's infrastructure. (Consider this analogy: Rather just plastering over a series of holes in a wall, Nokia looks to see if those holes contributed to underlying structural damage that would require the entire wall to be rebuilt.) Such comprehensive analysis allows Nokia to propose more holistic solutions to meet its customers' security requirements.

Building better outcomes

Through the security assessment conducted on its 4G and 5G environments, the network operator was able to get clear visibility into:

- Its current maturity level across the critical security control domains — and what that means for its customers
- Quantified targets for improvement to better protect its 4G and 5G networks
- The required improvement path to get from where it is today to its desired future state as a certified NIST Tier 4 operator

With Nokia's action plans and roadmaps in hand, our customer can address the gaps in its security posture, with minimal impacts or

disruptions to its network operations or the service received by its customers. And unlike other security consultants, Nokia's work doesn't end with the assessment: as an industry-leading network vendor, Nokia plans to work closely with the customer to implement the solutions required to improve the CSP's overall security posture.

The network operator now has all the quantified and qualified inputs needed to bring a best-in-class security framework to its 4G and 5G infrastructure — all in line with its risk appetite and strategic business objectives. In doing so, they will be able to offer solid security assurance to their customers, expand into new 5G markets and reinforce trust with their existing customer base.



Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID:212904 (January)

nokia.com

NOKIA

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2023 Nokia