Securing the Future of Telecom with Nokia

Developments in telco cybersecurity

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. Leading in critical network security transformations, we play a key role in establishing security standards with five standardization bodies. With 15+ years of in-house security experience and 200+ telecoms-specific use cases, we support 500+ customers worldwide.

Technology is changing at a breakneck pace and CSPs are on a treadmill of adapting to these unprecedented shifts. This has brought to fore a vast array of new forms of attacks, security vulnerabilities and bad actors that are causing significant impairments and damage to CSPs worldwide.

Telecoms networks enable mission critical infrastructures & services and have disproportionate influence well on lives & communities at large. Interruptions and breaches are unacceptable and, to compound the pressure, regulators are starting to tighten security control mandates, reporting and oftentimes impose stippling penalties for lapses.

In this paper, we aim to elaborate on the reasons why telecom networks demand a unique approach to security. We also showcase Nokia's commitment to CSPs with a marketleading pedigree and share our comprehensive assortment of purpose-built security solutions, security consulting and services.

Developments in Telecom Security landscape

1. Telco security vs IT security

When exploring generic IT security vendors, there are various incidents from common threats like phishing and weak passwords to more severe issues such as data theft, compromised databases, and banking trojans. These attacks can lead to service disruptions and the exposure of user data including PII and credit card information. As we dive into the specialized domain of telco security vendors, the incidents are more severe with heavy consequences for end customers. These include eavesdropping on subscriber data/ network data, signaling storm towards RAN/ Core to cross technology attacks on roaming interface (SS7/ GTP), and compromised telco workloads/ network functions.

The fallout of these attacks can lead to network failures and country-wide communication outages.

This loss of connectivity can hinder access to emergency services and financial transactions. It's a stark contrast between IT security attacks which typically involve data theft and service disruptions, and telco network security breaches which can have the potential for life-and-death impact. Nokia's telco-centric security solutions are designed to protect both operational technology (OT) such as telecommunications networks as well as information technology (IT) systems from evolving cyber threats in the 5G and Industry 4.0 era.

Explore more

IT Security	Telecom Network Security
Components	
Industry agnostics such as laptops, Mobile Devices, Intra-net, IT applications and data center	Purpose-built networks such as Core, RAN, Transport, Ac-cess Network, OSS/ BSS
Infrastructure and protocols	
Standard protocols like TCP/IP and TLS	Multi-vendor legacy technologies mixed with the latest cloud-based SBA and telco protocols like SS7, Diameter, GTP
Skill sets	
Skills in endpoint security [mobile, desktop servers], app security, firewalls, and secure gateways.	Expertise in telco network topology, communication proto-cols, attack scenarios for SBA, NE integrations to collect telemetry data and take actions.
Tools and technology	
Homogenous security tools like IT SIEM, IAM, EDR, and laptop antivirus.	Specialized tools like telco XDR, mission-critical EDR, telco PAM, cloud-native architecture
Regulatory landscape	
Governed by standards like HIPAA, PCI, and GDPR	Abides by 3GPP, GSMA, and country-specific regulations such as TSA in the UK, NIS2 in Europe

2. GenAI - Driving fundamental changes to the threat landscape

In the next decade, we can expect AI to play an even more significant role in both defending against and perpetrating cyber threats. Generative AI, or GenAI, has been making waves in the cybersecurity industry. This technology is reshaping how organizations detect and respond to threats.

One of the significant advantages of GenAI is to expedite security incident forensics which speeds up cyber threat resolution time and quality. It will also help identify sophisticated attack techniques that traditional security tools might miss. Additionally, it empowers cybersecurity teams to proactively defend their networks and streamline their operations. However, it's crucial to recognize that malicious actors are also harnessing the same technology for multi-stage attacks which makes it essential for CSPs to establish a zero-trust architecture resistant to GenAI.

Watch GenAI integrated in Cybersecurity Dome

3. Ransomware on the rise

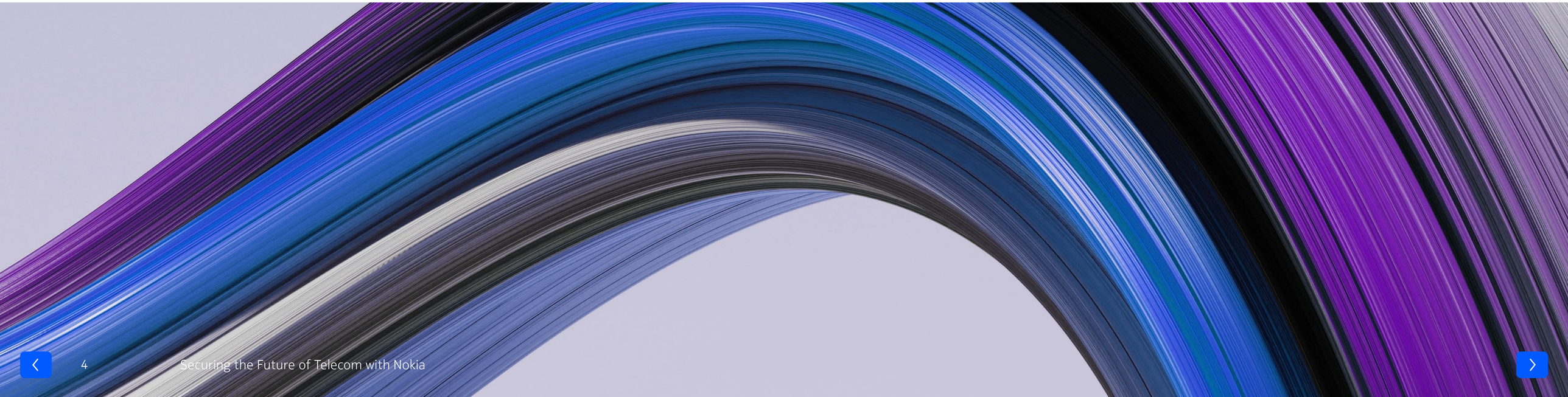
Malicious actors are using more sophisticated and targeted ransomware attacks against the telecom industry, leveraging zero-day vulnerabilities and the long cyber-criminal tradition of exploiting weak passwords to gain access to networks. In a recent GlobalData survey, more than two-thirds of CSPs cited ransomware as an area that needs substantial improvement for their security capabilities in telecommunications. To combat this, CSPs must implement multi-factor authentication and regularly back up their data to mitigate the impacts of a successful ransomware attack.

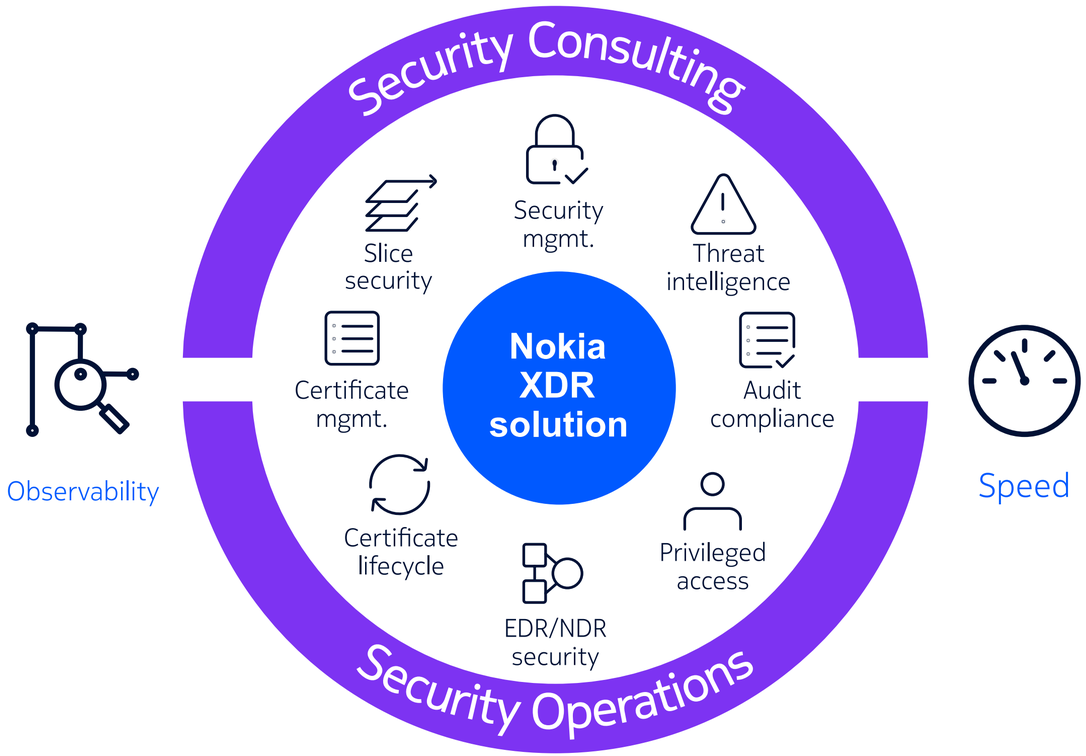
Learn more: Threat Intelligence Report

4. Regulatory changes in telecom worldwide

Compliance is a driving force behind cybersecurity operations adding complexity to the cybersecurity landscape. New regulations like Europe's Network and Information Systems Directive 2 (NIS 2), the UK Telecommunications Security Act (TSA), and other data protection laws are remodeling and strengthening compliance and reporting requirements. Organizations must adapt to the high expectations for reporting security incidents to regulators to avoid hefty fines and reputational damage.

Learn more: NIS2 directive





Nokia Security Products and Services

Nokia XDR Security:

Nokia XDR Security is a cloud-native Extended Detection and Response (XDR) platform suite, built as a use-case driven solution for flexibility and ease of integration. It solves the need for real-time threat detection and response and has demonstrated 70% increased effectiveness at rapidly blocking threats in Security Operations Centers or preventing them before they materialize.

1. NetGuard Cybersecurity Dome

NetGuard Cybersecurity Dome is an awardwinning XDR security orchestration platform suite with pre-built 5G use cases for telecommunication service providers and critical infrastructure enterprises. Built on extended detection and response (XDR) architecture, it offers visibility across various networks, cloud infrastructure, and endpoints.

2. NetGuard Endpoint Detection and Response (EDR):

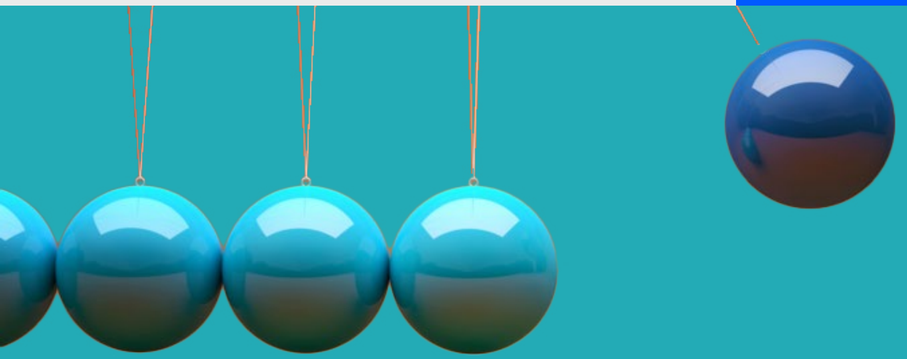
NetGuard EDR is an advanced security software designed to protect critical telecommunications infrastructure from cyber threats. It offers real-time monitoring of network function data and traffic for rapid threat detection and response.

3. NetGuard Identity Access Manager (IAM):

That XDR module is a Privileged Access Management (PAM) / Privileged Identity Management (PIM) application that secures physical or virtual network functions and resources. It acts as a centralized security gateway that allows you to control, monitor, and audit privileged access to all missioncritical network and IT systems through a single pane of glass.

4. NetGuard Audit Compliance Manager (ACM):

It automates the audit and analysis of all parameters in physical and virtual networks. It extracts real-time parameter settings from physical and virtual network functions and performs data integrity analysis by comparing the results to industry gold standards.



5. NetGuard Certificate Manager:

Based on a trusted certificate authority, the NetGuard Certificate Manager issues and manages digital certificates in a standardized and secure way. Its primary use is for 4G and 5G mobile networks where base stations and small cells are deployed in an unsecured area, and where a secured connection to the backbone network is required.

6. NetGuard Certificate Lifecycle Manager (NCLM):

Its for the certificate lifecycle management of digital identities. It automates the enrollment, renewal, and deployment of public keys and certificates in a centralized, secure and cost-effective way, preventing costly outages and vulnerabilities.

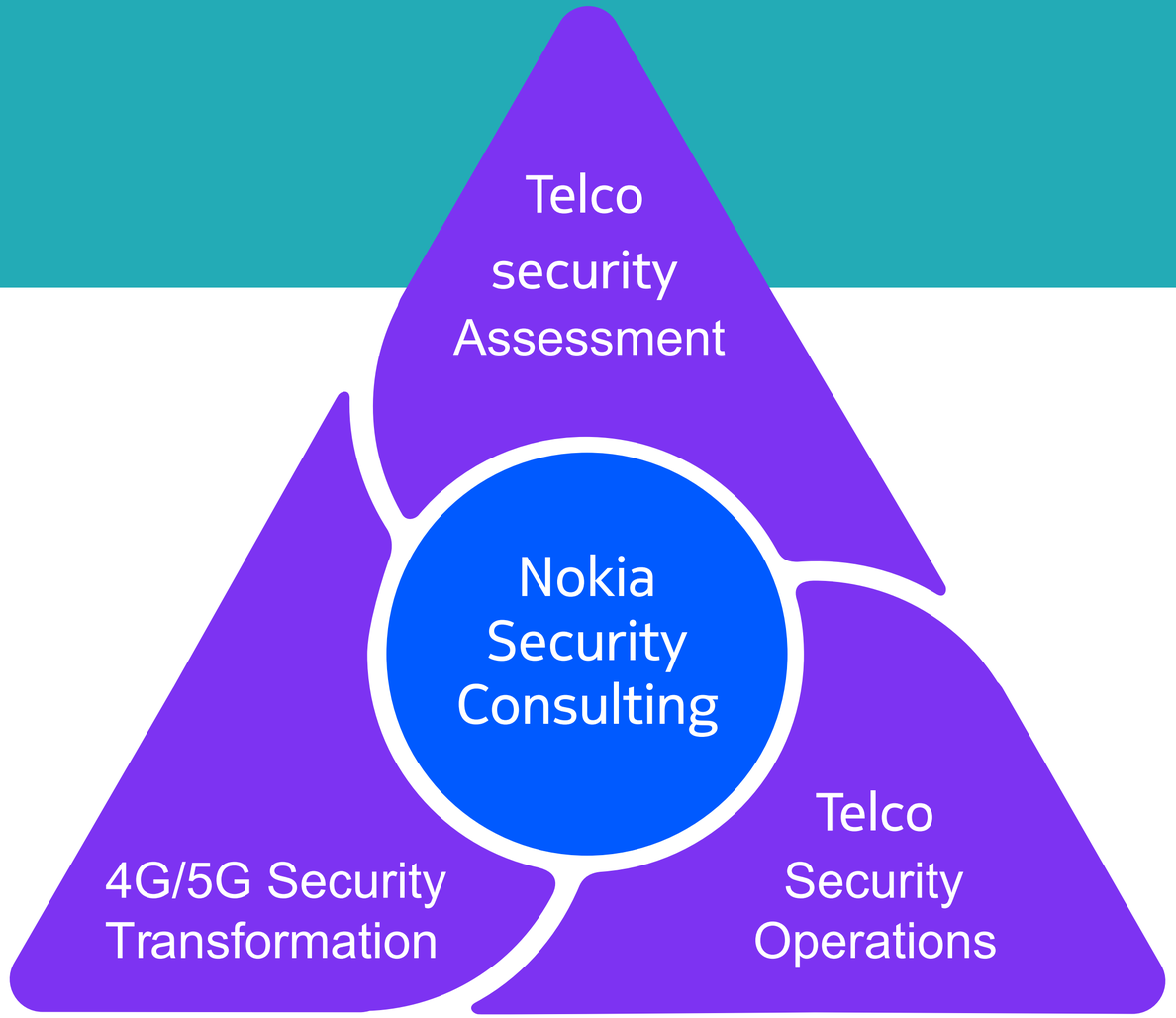
7. Cybersecurity Consulting:

Our cybersecurity consulting brings deep 5G security expertise and one of the world's only end-to-end 5G security assessment and insight capabilities to help you transform your 5G security operations and stay ahead of cybersecurity threats. Our clients can rely on the high level of expertise of our security auditors and a robust audit and assessment process.

Explore more: NIS2 whitepaper

8. Managed Security Services:

Managed Security Services offers you the most complete portfolio of value-added telco security services tailored to protect both OT/5G networks and IT technology from the evolving cyber threats in the 5G and Industry 4.0 era. Our Managed Security Services portfolio is fully aligned with the 'Continuous & Defense-in-depth Adaptive Security Architecture', as well as references including MITRE ATT&CK, Nokia's Bhadra Telecom Framework, ITU-T x.805, etc.



How We address Telco Specific Security Challenges

Projects Worldwide

500+

Telco-Network Security and Services

Certifications

350+

Nokia's Commitment to Network Security for the 5G World:

Nokia has been incorporating advanced research from Nokia Bell Labs to create Network Slicing Security Solutions that ensure security and trustworthiness of the end-to-end network slices. These are the critical connectivity and service fabric for industrial applications in the 5G era.

This addresses the challenge of securing network slices against potential cyber threats.

Nokia XDR Security and Microsoft Partnership:

The partnership between Nokia and Microsoft brings together deep telco security expertise and experience in secure public cloud deployments. By leveraging the Nokia XDR security solution and their partnership with Microsoft, you are able to enrich cybersecurity orchestration. This addresses the challenge of securing cloud-based systems against cyber threats.

Comprehensive Use-case Library:

Nokia Managed Security Services protects against all applicable telecom-centric cyber-threats following a risk-based approach in compliance to respective security standards and regulations. Managed Security Services Portfolio aligned with Defense-in-depth & Adaptive Security Architecture, and industry best practices (MITRE ATT&CK, Bhadra Telecom Framework, ITU-T x.805,)

Augmenting Cyber-security Skills & Capabilities:

Our portfolio covers holistic capabilities covering holistic attack surface management (Hybrid Infra, network, applications, Endpoints and Identity), Security Governance & Risk (GRC), Managed Detection & Response, Vulnerability Management & threat research, Audit & Governance.

- Pool of multi-vendor telecom domain SMEs leveraged for security design and implementation activities.
- Library of baseline security and hardening parameters for Telecom Domain
- Use case library for telecom technologies based on ITU-T x.805 framework.
- Lab environment for telecom technologies for security testing and R&D
- Global SIOCs designed for round the clock monitoring, detection & response.

Telecom specific cyber attack use case library

Denial of Service
Traffic interception

Exploit injection
Information disclosure
Mediation and billing attacks
Billing system flooding for prepaid abuse
IN attacks (Intelligent Network)
Web attacks

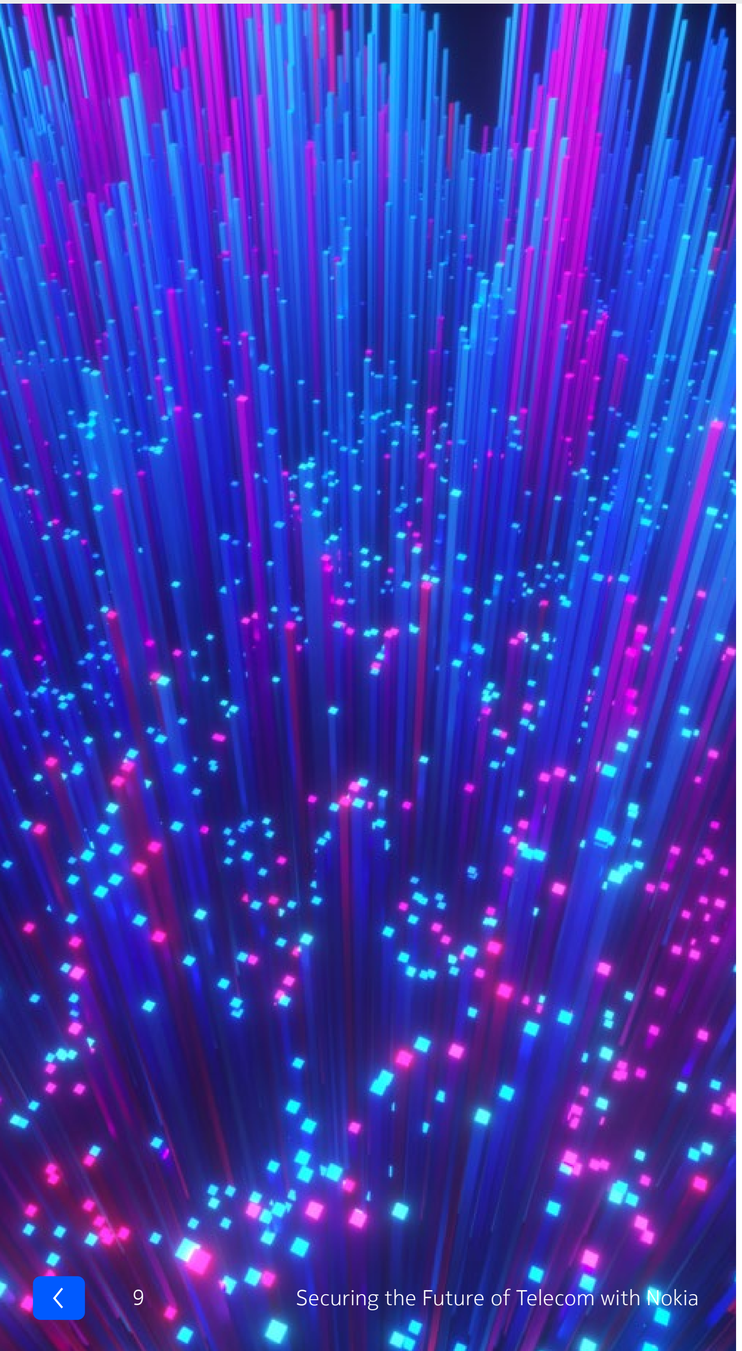
Passive listening
Cloning Outage
IMSI-catcher/ Fake BTS
Subscribers DDoS

Malware Privacy
Charge bypass

SS7 entry point abuse
Hostile SS7 location request
Femto-cell based signaling attacks
SS7 MSU bill artificial inflation
VoIP originated SS7 injection

Data leakage
Service interruption
Total compromise

SMS/Messaging attacks (SMS, VMS)
MMS attack
Lawful interception system attacks
Reverse charge
SMS fraud
Prepaid abuse
SMSC scanning, discovery and abuse
Location based service unauthorized access HLR authentication flooding
VLR stuffing
Illegal call redirection
SMS to MSC direct addressing



Analyst Recognition

Industry analyst GigaOm has recognized Nokia for the second year in a row for our XDR security software and has upgraded our position to a fast-moving leader in the industry.

The GigaOM Radar Report for Extended Detection and Response (XDR) positions Nokia as a "Leader" in the XDR market. The report evaluates Nokia's XDR solution, which is part of the company's broader cybersecurity portfolio.

According to the report, Nokia's XDR solution stands out for its:

- **Broad Threat Coverage:** Nokia's XDR solution provides comprehensive threat coverage, including network, endpoint, and cloud security.
- **Integration and Automation:** Nokia's XDR solution integrates with various security tools and automates threat detection and response, reducing the workload of security analysts.
- **Machine Learning and AI:** Nokia's XDR solution leverages machine learning and AI to detect and respond to threats more effectively.
- **Scalability and Performance:** Nokia's XDR solution is designed to handle large volumes of data and provide real-time threat detection and response.
- **Customization and Flexibility:** Nokia's XDR solution is highly customizable and can be tailored to meet the specific needs of different organizations and industries.

The report also highlights Nokia's strong reputation in the cybersecurity industry and its commitment to innovation and research and development.

Overall, the GigaOM Radar Report for Extended Detection and Response (XDR) recognizes Nokia's XDR solution as a leading XDR platform, highlighting its comprehensive threat coverage, integration and automation, machine learning and AI, scalability and performance, customization and flexibility.

Explore more: HERE

Customers References

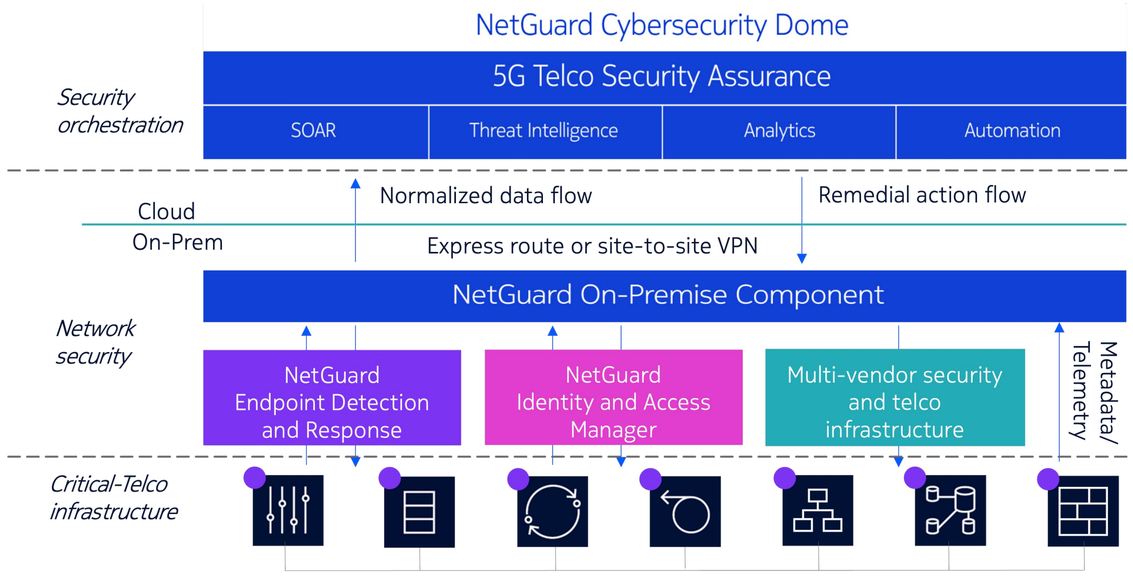
Claro Colombia's Success with NetGuard Cybersecurity

Claro Colombia, in partnership with Nokia, has successfully completed the first stage of Colombia's largest 5G deployment, which involved the construction of over 1,000 sites nationwide. A key part of this project was the implementation of Nokia's NetGuard Cybersecurity solutions.

Nokia provided a variety of software solutions, two key components of the XDR security solution provided were:

- **NetGuard Cybersecurity Dome:** An award-winning security orchestration software suite with pre-built 5G use cases. Built on extended detection and response (XDR) architecture, it offers visibility across various networks, cloud infrastructure, and endpoints.
- **NetGuard Endpoint Detection and Response (EDR/NDR:** A real-time threat detection and response solution to protect critical network functions on customer premises.
- **NetGuard Identity and Access Manager:** Monitor and control network access by privileged users, ensuring that only authorized individuals can access sensitive information. It aims to detect any potential threats from within the organization by keeping track of such high-level access.

These broad telco-centric XDR solution have helped Claro Colombia to improve its efficiency and response times to new and existing cyber threats, thereby enhancing the security of its 5G network. This successful implementation demonstrates how Nokia's security products can address specific security challenges in the telecommunications industry. LINK



Nokia and Bharti Airtel's Journey to a Safe 5G Deployment

Recognizing the transformative potential of 5G, both companies understood the critical need for robust security measures. They agreed that Nokia would lead the security assessment, leveraging its global expertise to ensure a secure implementation.

The first step was a comprehensive security assessment conducted by Nokia's team of experts. They began by identifying all potential security threats specific to 5G networks, including advanced persistent threats, identity theft, and data breaches. This phase was crucial for setting the baseline for the security architecture that would need to be robust yet flexible enough to adapt to evolving threats.

With the threats identified, Nokia security consulting introduced a systematic approach to develop the 5G security architecture. This approach was divided into several key phases:

Phase 1: Requirement Gathering - Nokia worked closely with Bharti Airtel to understand the specific security needs and expectations from the 5G network.

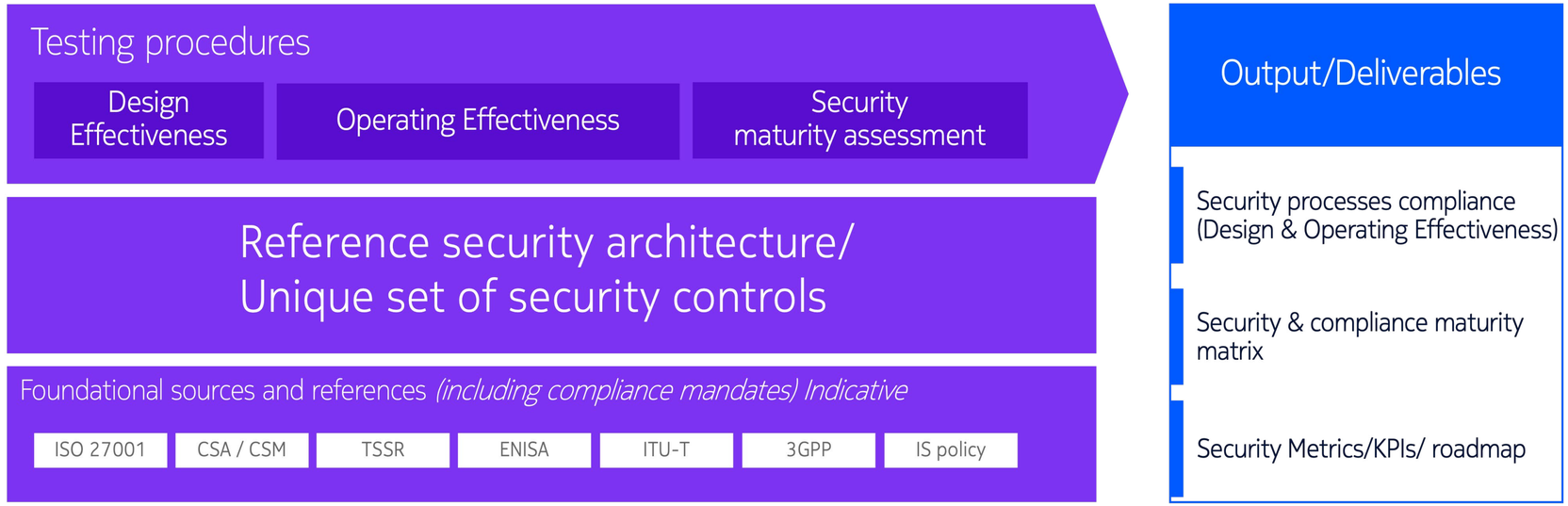
Phase 2: Designing the Architecture - Using the information gathered, Nokia designed a multi-layered security architecture that included encryption, intrusion detection systems, and AI-driven threat analysis.

Phase 3: Implementation and Deployment - The security systems were integrated into Bharti Airtel's 5G infrastructure, with continuous monitoring setups to manage and mitigate any real-time threats.

Understanding that technology alone is not enough, Nokia provided comprehensive training to Bharti Airtel's team. This training ensured that the staff were well-versed in the new security protocols and could manage the day-to-day security operations effectively. Additionally, Nokia established a joint task force that could swiftly address any security issues that arose.

With the security architecture in place and the teams trained, Bharti Airtel launched its 5G services. The launch was met with positive feedback, with customers expressing confidence in the security of their data. Nokia continued to support Bharti Airtel by providing ongoing security updates and advanced threat detection capabilities.

The successful deployment of a secure 5G network by Bharti Airtel, guided by Nokia's expertise, set a new standard in the industry. It showcased how systematic planning and advanced security measures could pave the way for safe and efficient 5G services. Other telecom operators looked to this partnership as a model for their own 5G security strategies.



Integration with 5G FiGHT and MITRE

Nokia's security solutions can be further enhanced by integrating with the 5G FiGHT framework developed by MITRE. The FiGHT (5G Hierarchy of Threats) framework is a knowledge base of adversary Tactics and Techniques for 5G systems. It provides organizations with the ability to assess the confidentiality, integrity, and availability of 5G networks and the applications using them.

By integrating Nokia's security solutions with the 5G FiGHT framework, organizations can gain a more comprehensive understanding of potential threats to their 5G networks. This can help to develop more robust security strategies and measures, thereby enhancing the overall security of their 5G networks.

Benefits of Integration

The integration of Nokia's security solutions with the 5G FiGHT framework can offer several benefits:

1. Enhanced Threat Detection: The FiGHT framework can help organizations to identify potential threats to their 5G networks more quickly and accurately.

2. Improved Security Strategies: By providing a comprehensive overview of potential threats, the FiGHT framework can help organizations to develop more effective security strategies.

3. Greater Network Resilience: By helping to identify and mitigate potential threats, the FiGHT framework can enhance the resilience of 5G networks.

In conclusion, the integration of Nokia's security solutions with the 5G FiGHT framework can significantly enhance the security of 5G networks.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214130

nokia.com

About Nokia

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

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.