SOLUTION BRIEF

Nokia Managed Security Services

Secure the telco future, today

NOKIA

Telecom systems, with their intricate web of interconnected components, pose a high complexity, requiring deep domain expertise to identify vulnerabilities woven into this complex ecosystem. The rapid evolution of telecom technologies adds to the challenge, expanding the attack surface and demanding a comprehensive understanding to mitigate associated risks effectively.
Nokia Managed Security Services (MSS) protects against all applicable telecom-centric cyber-threats following a risk-based approach in compliance to respective security standards and regulations.

A new world of threats

In the realm of telecommunications, businesses face a myriad of challenges in the cybersecurity landscape.
Traditional security models are rapidly becoming inadequate against the sophistication of modern-day threats. Existing security solutions are designed largely for enterprises and lack the features needed for telecom security.
Regulatory and compliance standards are tightening, leading to increased liabilities for non-compliance.
A significant hurdle lies in the scarcity of diverse security skill sets needed to cover the expansive security spectrum effectively.
Companies also grapple with the balancing act their security strategies.
Additionally, the lack of real-time awareness, security intelligence, and robust analytics and automation capabilities further compound the complexities faced in safeguarding telecom infrastructure from cyber threats.

Telecom-centric security solutions

Adoption of new technologies introduces new security challenges

Attacker shift

Cyber criminals are better organized and financially motivated

Threat shift

Major deterioration in threat landscape making traditional security measures ineffective

Compliance mandates

Regulatory fines, e.g., GPDR can cost billions for large global companies

Skills shortage

By 2025, there will be 3.5 million unfulfilled cybersecurity positions

Too many tools

Organizations are using many vendors with different tools

Nokia Managed Security Services Approach

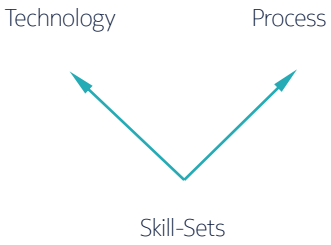
Security Approach

KEY: Automation, continuous monitoring and orchestration automation

1

Secure-by-design principle

1. Defense-in-depth
2. Adaptive and continuous security
3. Zero-trust



2

Identity & access management

Dramatic increase in the number & type of accesses. It's not only about User but Systems as well. Complete visibility on privileged identities and actions performed.

3

Vulnerability management

Closing all vulnerabilities may not be in your hands, but effective management of vulnerabilities certainly is! This needs domain expertise!

Network & Infrastructure

Applications

OT Protocols & Interfaces

4

Security configuration management

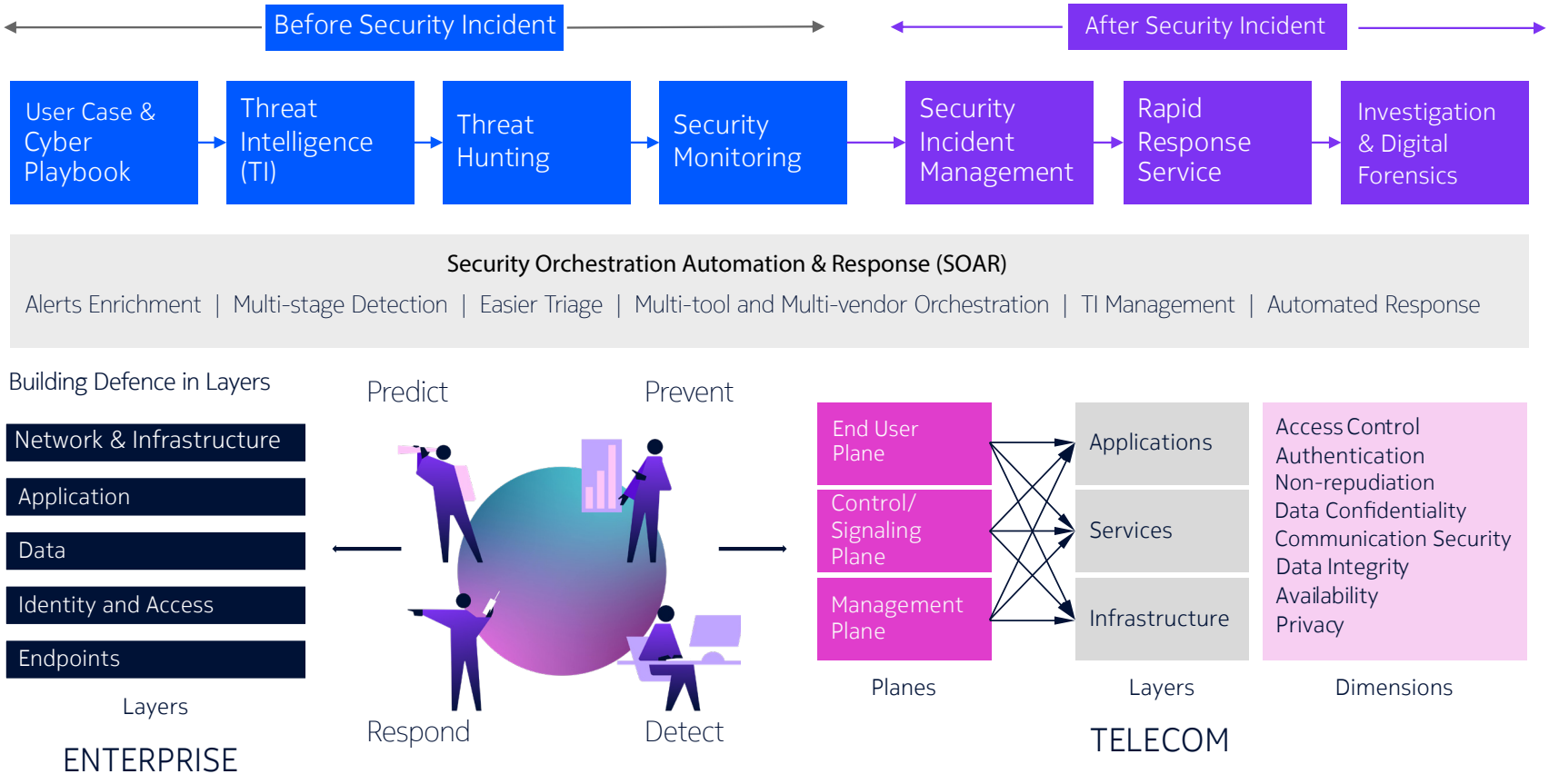
Ensure integrity of critical configurational parameters with complete visibility on the same – anywhere, anytime; prevent threat actors to induce any vulnerability through configuration manipulations.

Nokia Managed Security Services Approach

Security Approach

KEY: Automation, continuous monitoring and orchestration automation

5



An ecosystem of telecom-centric end-to-end adaptive security services

Managed Security Services Portfolio

Portfolio aligned with Defense-in-depth & Adaptive Security Architecture, and industry best practices (MITRE ATT&CK, Bhadra Telecom Framework, ITU-T x.805,..)

1 Security Operations Risk Assessment

- Operational readiness assessment
- Risk Index and Maturity
- Detailed Audits / Reports
- Security Blueprint / Roadmap

2 Security Infrastructure Management

- Network & Infrastructure Layer
- Application Layer
- Data Centric Layer
- Identity & Access Layer
- Monitoring & Governance Layer

3 Security Governance Risk & Compliance

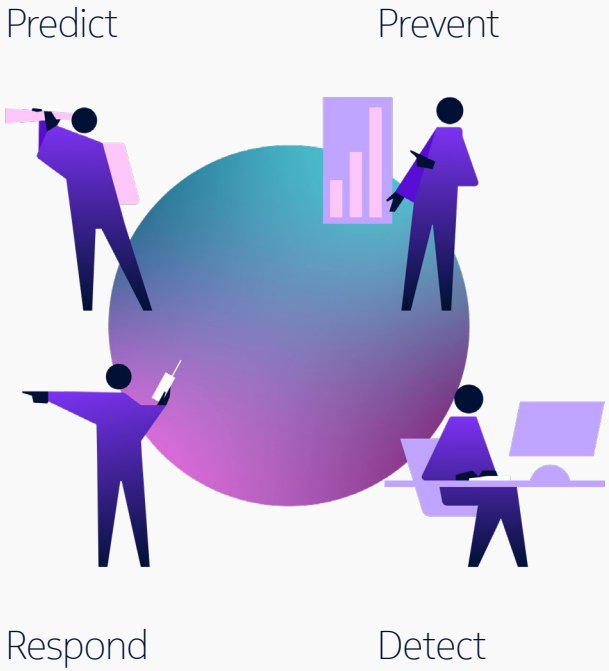
- Security Controls Governance & Automation
- Vulnerability Management
- Security Configuration Management
- Application Security Management

4 Managed Detection & Response

- Security Operations Centre (SOC)
- Detection use cases
- Threat Intelligence
- Proactive Threat Hunting
- Telecom Security Incident Response
- Response Automation
- Digital Forensics & Investigations

Continuous Visibility & Validation

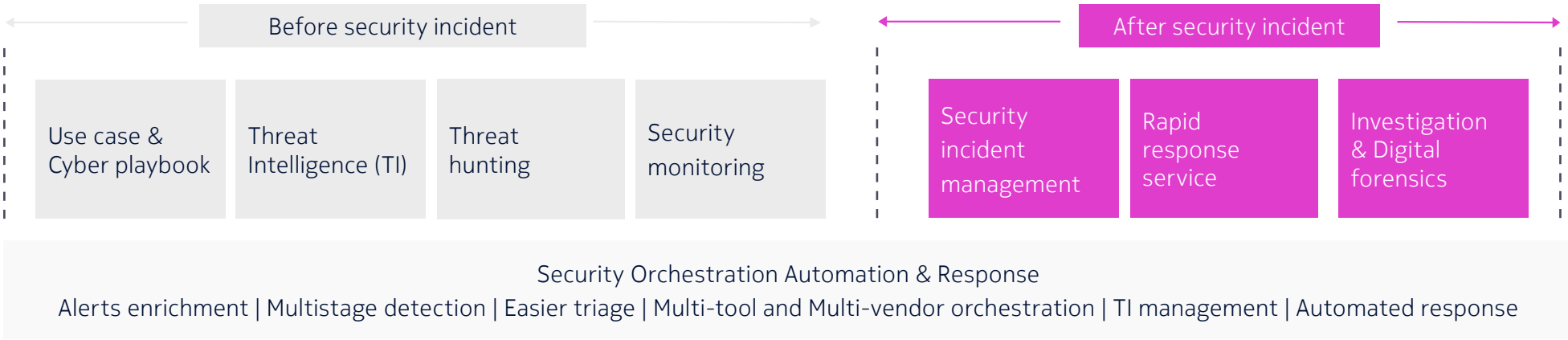
Users, System, Activity, Payload, Network.



ITU-T x.805 / MITRE ATT&CK Framework

Better detection and response

Nokia MSS related to cyber-attacks detection and response can be divided into those employed before a security incident and those used once an attack is executed. Together they provide a complete spectrum of defence for telecom companies facing a wide range of both known and unknown threats.



Before security incident

- **Use-case and Response plan:** This helps telecom companies identify telecom-specific threats or use cases and form a response plan to counter them.
- **Threat Intelligence:** The Nokia threat intelligence service keeps operators up to date on current global threats.
- **Threat hunting:** Our deep analytics and machine learning capabilities identify unknown or hidden threats that could evade existing security methods.
- **Security monitoring:** Nokia's unique use-case-based methodology monitors security alerts and events in real-time.

After security incident

- **Security incident management:** This service speeds up the management of the lifecycle of a security incident, using effective and faster incident analysis, communication, workaround, response, root-cause analysis and corrective measures.
- **Rapid response service:** Nokia's rapid security response service integrates machine intelligence with human expertise, to effectively contain, mitigate or eliminate the identified threats.
- **Investigation and Digital forensics:** Domain experts and forensics capabilities aid an effective response to cybercrimes, from the initial triage to investigations and corrective measures.

SOAR

It can improve the efficacy, efficiency and consistency of the security operations by using orchestration and automation of threat intelligence management, security event monitoring and incident response processes.

Mastering vulnerability management

Addressing vulnerabilities demands continuous strategy refinement, leveraging technology, and deepening domain expertise. Core elements include comprehensive insights through vulnerability assessment, strategic prioritization, and compensation controls.

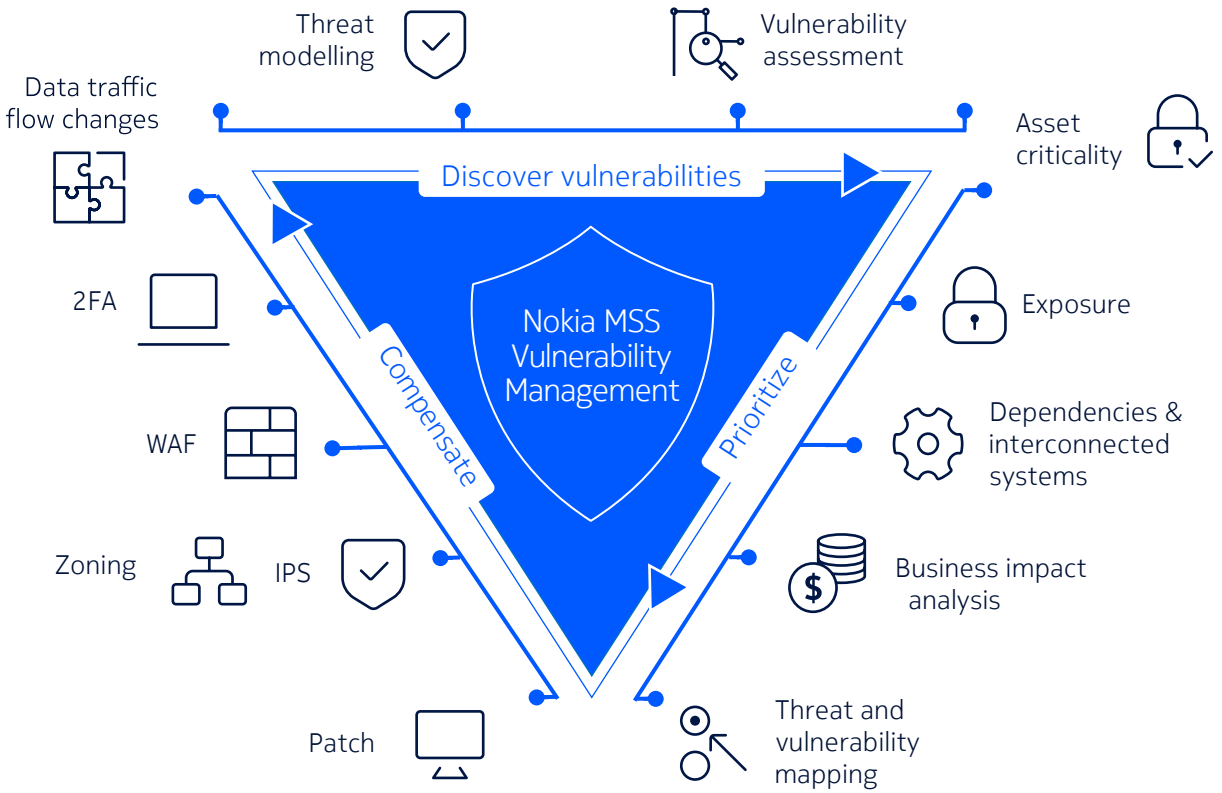
Embracing a risk-centric paradigm guides organizations in prioritizing efforts and aligning remediation with strategic objectives.

Our vulnerability management service provides the technologies, processes and operations to fully administer vulnerability management programs across the vulnerability lifecycle that fit the specific requirements and needs of telecom environments.

Vulnerability discovery: Optimized scanning configurations for maximum vulnerability discovery

Prioritization: Effective vulnerability management relies on strategic prioritization aligned with closure strategies.

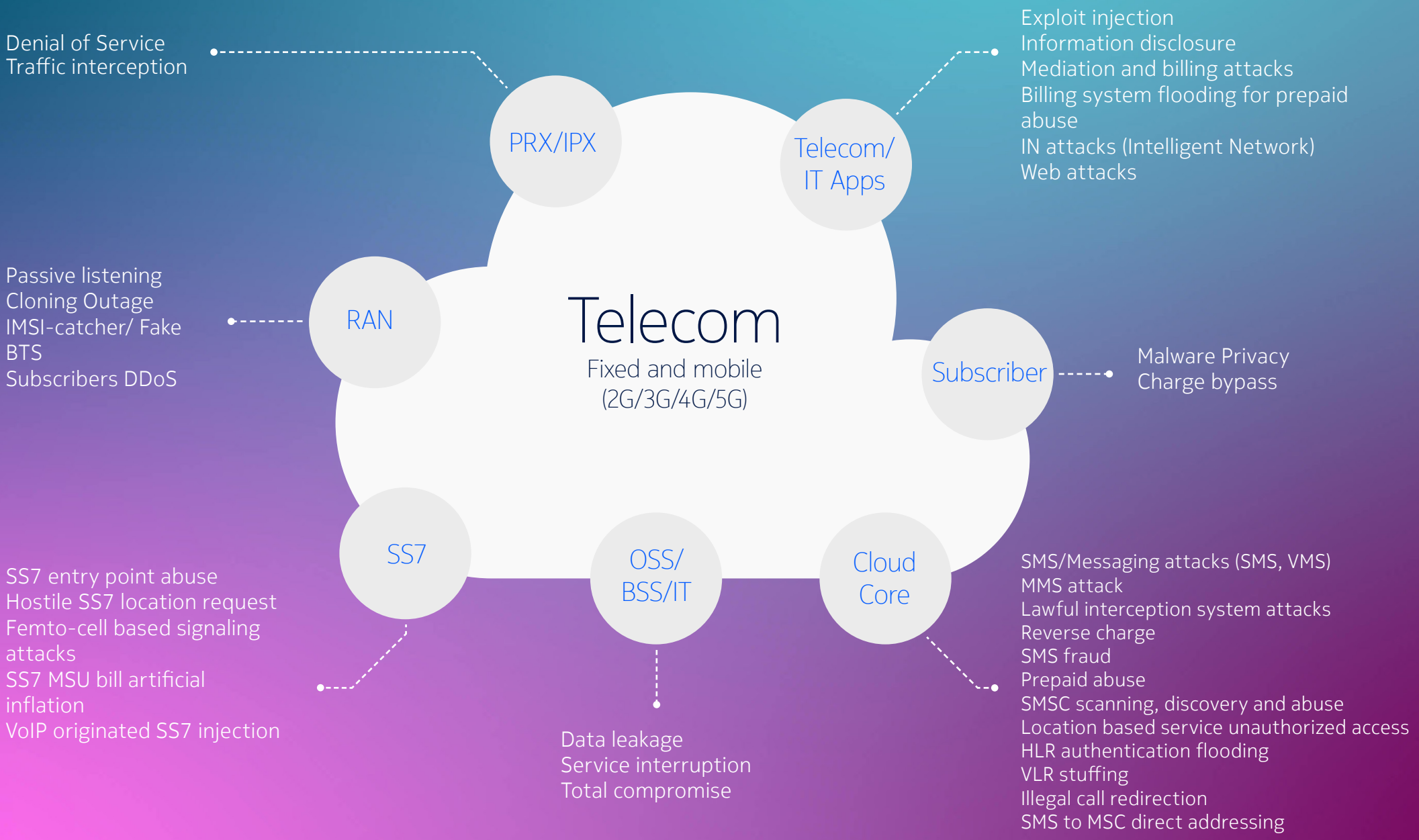
We eliminate false positives in network infrastructure to expedite the triaging of vulnerabilities.



Quantifying the associated risk enables organizations to prioritize closures based on well-informed risk assessment outcomes.

Compensation: Diverse alternatives, including IPS, WAF, and robust authentication, are needed to reduce the attack surface. Additionally, integrating security controls like enhanced monitoring and analytics (UEBA, NBA) is essential, making compensating controls a crucial part of any comprehensive vulnerability management strategy.

Telecom specific cyber attack use case library



Nokia security intelligence and operations center (SIOC)

Our security intelligence and operations centers (SIOCs) are designed to monitor, analyze and respond to threats targeting an organization's information systems and assets. Acting as a central point for security operations, they coordinate the detection, investigation and mitigation of cyberattacks and other incidents. Key services include:

- Telecom domain experts
- Simulated R&D lab environment for developing security use cases around telecom technologies
- Standardized processes & tools framework
- Multi-vendor & multi-technology environment
- Compliance with ISO 27001 / NIST practices
- 24x7 SOC monitoring and incident response
- Purpose-built security solutions for telco networks–public and private

Presence

- Romania/Timisoara
- India/Chennai
- USA/Dallas

MSS GDC delivery capability
Facts & figures from Tier-1/2 CSPs

Volume

+400 million Subscribers

+75K integrated devices – SIEM

+53K EDR integrated nodes

+300 unique MBSS hardened nodes

+400 telco application assessed

+144 5G (SA) use cases

+180 Telecom penetration use cases 2G/4G/5G

+450K of total SOC inventory assets

Performance

+360K handled notable events

+3.5K triaged security incidents

+23 critical security Incidents

+2K AppSec vulnerabilities

+1426K infra vulnerabilities

+3.5K unique vulnerabilities.

100% uptime of SIEM

100% response SLA for security incidents

People & skills

+100 skilled security resources

+40 telco security experts

- Security consulting
- Network & Infrastructure
- Application security
- Identity & Access
- Managed Detection & Response
- Security Governance
- Risk & Compliance Management
- Security operations
- Security engineering
- 2G-5G & Fixed Line SMEs
- Radio
- Transmission
- Core
- Interconnect

Competency

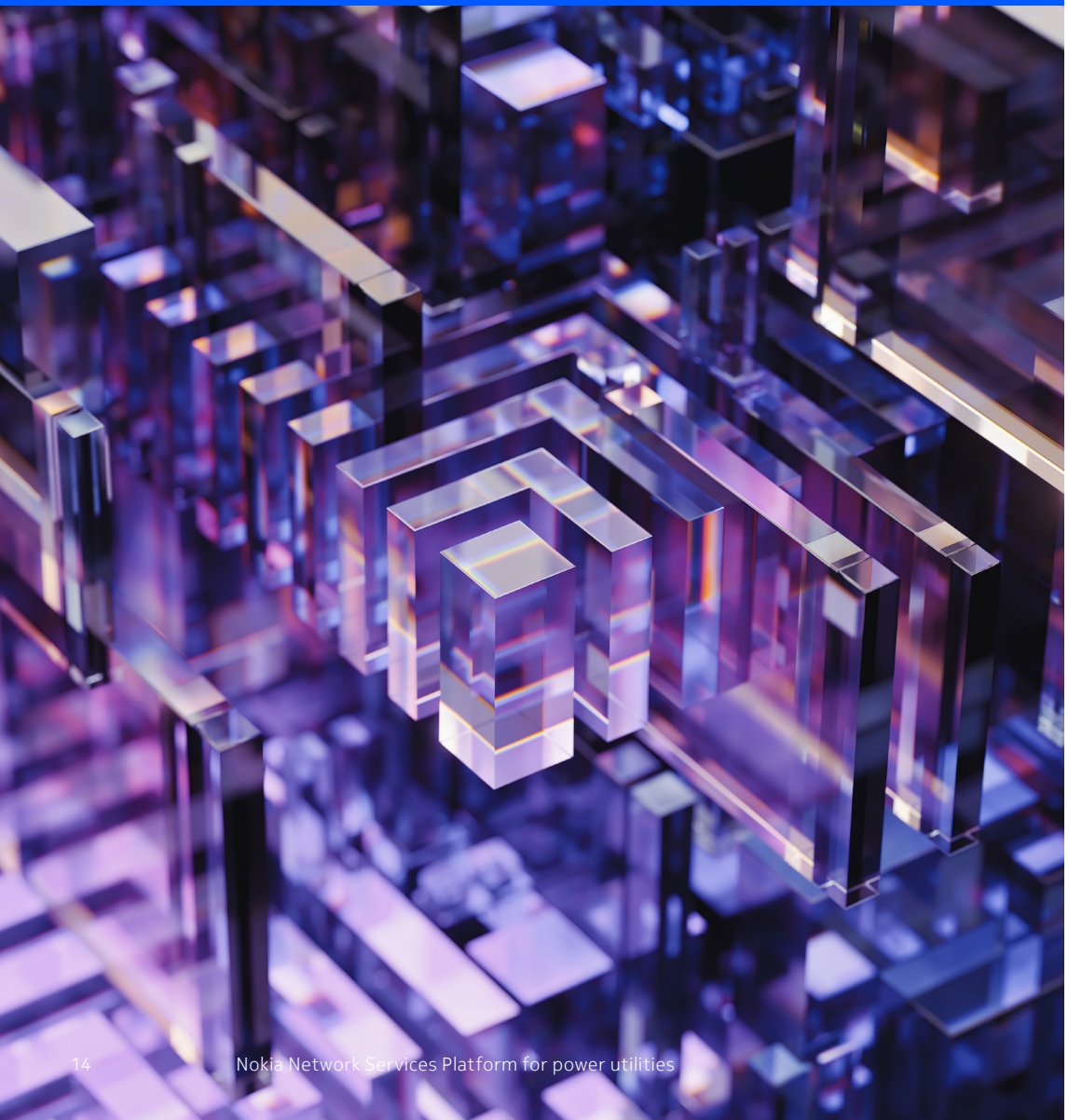
- Splunk Certified
- Qualys Certified
- CEH Certified
- CCNA , CCNP, CISSP, CISM
- Telecom Security
- TDR – Threat Detection & Response
- NCYD
- Telecom domain expertise (2G-5G, FL)
- Bell Lab e2e 5G security

Nokia value proposition to telecom cybersecurity

1. Pool of Multi-vendor telecom domain SMEs leveraged for security design and implementation activities
2. Library of baseline security and hardening parameters for Telecom Domain
3. Use case library for different telecom technologies based on ITU-T x.805 framework
4. Lab environment for telecom technologies for security testing and R&D (India and France)
5. Global SIOCs designed for monitoring telecom infrastructure (India and Romania)
6. Inhouse security products and product line focused on Telecom Security
7. Blueprinted security products and solutions addressing telecom security needs

Industrialized and efficient delivery

Our approach emphasizes automation, analytics, scalability, predictability, and skillset management.
Through streamlined processes and advanced technologies, and advanced technologies, we ensure swift, reliable, and cost-effective service delivery, tailored to meet your unique needs and challenges.



Securing the telco future, today

Telecom-centric security solutions

Our services are crafted to meet the unique demands of 2G, 3G, 4G/LTE, 5G, fixed lines, and Telco-heavy IT/ Enterprise scenarios. Aligned with the latest global best practices and industry standards, we ensure your network stays secure and resilient

Layered security solutions

Our approach to cybersecurity encompasses a multi-layered strategy from robust network and infrastructure security to the protection of critical applications, telecom protocols & interfaces, data-centric security measures, and stringent identity and access management. These integrated layers ensure comprehensive protection for your telecom infrastructure.

Comprehensive portfolio

We offer a range of services including consulting and risk assessment, security infrastructure management, security governance risk and compliance management, and managed detection and response services to safeguard your business in today's dynamic threat landscape.

Monetization

CSPs can now 'white-label' Nokia's services to offer innovative solutions to their enterprise customers, paving the way for fresh business models and generating additional revenue streams for operators.

High intense automation

Scalability

Analytics

Predicability

Skillset Management

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

CID: 214945

nokia.com

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, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. 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.