Managed Security Services
Managed Security Services to fight cyber-threats

Today’s telecom companies face an increasing volume and variety of cyber threats. To combat these risks, Nokia offers its Managed Security Service (MSS), an end-to-end security solution that helps prevent, detect, respond to and recover from attacks. It continuously manages an operator’s security infrastructure to protect against all applicable cyber-threats and meet all security standards and regulations.
A new world of threats

Telecom companies are experiencing a new world of cyber-threats, one where there is no longer a firm border between the safe and the unsafe. With network boundaries dissolving and networks themselves made up of several technologies from different vendors, intruders have more chances to gain access and cause damage using advanced malware. Such attacks may be from inside or outside the network, making any part of the network vulnerable, including the radio and core networks.

Conventional controls to prevent attacks have become ineffective and the focus has shifted to detection and response. However, existing security solutions are designed largely for enterprises and lack the features needed for telecom security.

Increased threat actors

Nation states, hacktivists, terrorists, cyber criminals, insider threats, competition

Highly sophisticated attacks

Advanced persistent threats, military-grade malware, refined zero day attacks, spear phishing attacks, ransomware, rootkits, exploits

Adoption of disruptive technologies

Cloud/virtualization, mobility, big data, digitization/IP-fication, collaboration, Internet of Things

Business challenges

- Conventional security models becoming obsolete against modern day threats
- Regulatory/compliance more stringent, increased liabilities
- Shift from prevention only to advanced monitoring, detection & response capabilities
- Lack of diverse security skill-sets to cover the wide security spectrum
- Economies of scale, predictable costs
- Lack of real-time awareness/security intelligence, analytics & automation capabilities
Managed Security Services
Nokia’s MSS approach

Ad-Hoc
- Un-managed
- Event driven
- Reactive
- Unmeasured
- Lack of effective threat detection and response capabilities

Repeatable
- Defined
- Managed

Continuous improvement – Security risk index and Maturity model

AS-IS assessment

Manage and Operate (TO-BE state)

Design correction (Processes & technology)

Optimized
- Managed
- Business driven
- Proactive
- Measured
- Advanced threat detection and response capabilities
Managed Security Services

Security Risk Assessment (SRI)

Security Infrastructure Management Services
- Device administration and lifecycle management
- Health, availability and performance monitoring
- Patch and version management
- Incident management
- Change management
- Configuration management
- Rule/case management
- Operations and security reporting
- Troubleshooting support

Security Governance, Risk & Compliance Management Services
- Security process lifecycle management
- Security audit & compliance management
- Security risk management
- Business resiliency management
- Third party security governance
- Data protection / Privacy governance

Security Monitoring & Response Services
- Threat intelligence services
- Managed threat hunting
- Security event monitoring services
- Security incident management services
- Security response services
- Investigation and digital forensics

Transformation Security (Cloud, Virtualization, SDN/VNF, IoT, Analytics, etc.)
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, work-around, 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.
Nokia value proposition

1. Pool of MultiVendor 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
Telecom specific cyber attack use case library

- **PRX/IPX**: Denial of Service, Traffic interception
- **Telecom/IT Apps**: Exploit injection, Information disclosure, Mediation and billing attacks, Billing system flooding for prepaid abuse, IN attacks (Intelligent Network), Web attacks
- **RAN**: Passive listening, Cloning, Outage, IMSI-catcher/Fake BTS, Subscribers DDoS, etc.
- **SS7**: SS7 entry point abuse, Hostile SS7 location request, Femto-cell based signaling attacks, SS7 MSU bill artificial inflation, VoIP originated SS7 injection
- **OSS/BSS/IT**: Data leakage, Service interruption, Total compromise
- **Cloud Core**: 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
- **Subscriber**: Malware, Privacy, Charge bypass

Telecom: Fixed and mobile (2G/3G/4G/5G)
Nokia Security Intelligence & Operation Centers (SIOC)

- 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

Existing
- Romania/Timisoara
- India/Chennai

Planned
- USA/Dallas
<table>
<thead>
<tr>
<th>Global presence</th>
<th>Security project world wide</th>
<th>Certifications held by our security experts</th>
<th>Active role in security standardization bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>500+</td>
<td>350+</td>
<td>10+</td>
</tr>
<tr>
<td>Commercial LTE</td>
<td>Open interface and vendor</td>
<td>Dedicated security service team since</td>
<td>Firewall installed on operator networks</td>
</tr>
<tr>
<td>Network Secures</td>
<td>agnostic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No1.</td>
<td>2004</td>
<td>4000+</td>
</tr>
</tbody>
</table>

**Wide-ranging benefits**

- Access to Nokia’s wide security portfolio to meet a wide range of security needs
- Enhance cybersecurity solutions with tailored telecom security use cases
- Gain continuous visibility of your readiness and improve security posture facing cyber-threats and comply with regulations
- Build effective detection and response mechanisms against modern day cyber-threats
- Sustained security program with continuous visibility and predictable outcome
- Secure safe adoption of disruptive technologies such as cloud, big data and Internet of Things (IoT)
About Nokia
Nokia is a global leader in the technologies that connect people and things. Powered by the innovation of Bell Labs and Nokia Technologies, the company is at the forefront of creating and licensing the technologies that are increasingly at the heart of our connected lives.

With state-of-the-art software, hardware and services for any type of network, Nokia is uniquely positioned to help communication service providers, governments, and large enterprises deliver on the promise of 5G, the Cloud and the Internet of Things. http://nokia.com

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.

© 2019 Nokia