NOKIA

Threat Intelligence Report 2024

What's next for telecom: Emerging trends and technologies

Main findings

Attacks on the telecom sector

- In North America, attacks often involved advanced techniques such as ransomware and were sometimes suspected to be state sponsored, focusing on data theft and service disruption.
- Incidents in East Asia frequently involved inadvertent exposures by companies themselves, leading to significant data leaks.
- Western Europe experienced a mix of cyber espionage and financially motivated breaches, indicating a diverse threat landscape.

DDoS attacks

- DDoS traffic continues to grow at a rate higher than any other type of network traffic, increasing 166% between June 2023 and June 2024. In many networks, the frequency of these events has grown from one or two a day to well over 100 per day.
- Botnets remain a major driver in the DDoS attack landscape, accounting for about 60% of traffic monitored by Nokia Deepfield.
- Carpet-bombing attacks, which attack multiple targets using a range of target IP addresses, are becoming larger in scope. In 2024, 13% of carpet-bombing DDoS attacks targeted 256 destination IP addresses or more, and 2.8% of attacks targeted 1,024 IPs or more.
- AI, automation and the use of residential proxies were prominent elements in DDoS attacks. In 2024, we observed greater DDoS attack sophistication driven by AI and automation, and significant abuse of residential proxies in large-scale DDoS attacks.

Emerging technology and threats

- Threat actors are increasingly using generative AI to mount sophisticated attacks faster and on a larger scale. Communications service providers (CSPs) are also using generative AI to accelerate response times and improve effectiveness against emerging threats.
- Quantum computing will pose a significant risk to critical networks and enterprises in the future. The National Institute of Standards and Technology (NIST) announced the formal publication of its first set of post-quantum cryptography (PQC) algorithms marking a major milestone in quantum-safe security.

About this report

Nokia has been producing threat intelligence reports for many years. The 2024 edition is the most comprehensive report to date, including a greater emphasis on cybersecurity trends and emerging technologies that will impact the telecom industry.

The report is based on analyses of:

- Real data by threat intelligence experts at Nokia's Cyber Security Center in France
- Security events and trends observed by Nokia Managed Security Services (MSS) security operational teams across the globe
- Distributed denial of service (DDoS) traffic and attacks by the Nokia Deepfield Emergency Response Team (ERT)
- Cybersecurity regulation trends by Nokia's Advanced Consulting Services, Cybersecurity Consulting team
- Quantum security by Nokia's quantum-safe networks security experts and Nokia Bell Labs
- Communications service provider (CSP) assessments of their own cybersecurity postures and top priorities by TM Forum

Telecom sector attack trends

Inside the latest attack trends in telecom

From 2022 to 2024, Nokia's threat intelligence experts at the Cyber Security Center in France have identified a notable pattern of cyberattacks targeting the telecom sector across various regions involving diverse threat actors and motives.

Attacks spanned the globe, with incidents reported in the US, UK, Germany, Ukraine and China. Impacts included significant service interruptions, theft of sensitive data, and potential unauthorized access to major online platforms.

Discovery and response

Nokia's threat intelligence experts have uncovered a concerning trend: cyberattacks are being discovered at different times, with some going undetected for months. For example, a November 2022 attack on a Tier 1 communications service provider (CSP) in Europe was not uncovered until January 2023. This delay in detection could have significantly worsened the impact of the attack, underscoring the critical need for faster threat identification.

Impact on services

The telecom industry is the backbone of our daily communications and vital infrastructure. An attack on the industry can have far-reaching consequences, disrupting services, jeopardizing security and undermining operational logistics.

For example, in February 2022, European CSP faced a sophisticated social engineering attack on its 4G/5G network that led to widespread service disruption. This attack affected 4.7 million mobile customers over 48 hours, significantly impacting the company's infrastructure and service delivery.

Trends and recommendations

Ransomware attacks on industrial organizations reached new levels of sophistication and scale in 2023. The threat landscape is expansive, with hundreds of ransomware variants such as LockBit, ALPHV, Hunters International, Rhysida, and NoEscape. Each deploys its own set of complex and unique techniques. The challenge is greater than ever, as these evolving threats continue to target critical infrastructure.

In 2023, LockBit ransomware became a major player in industrial cyberattacks. Operating as a ransomware-as-a-service (RaaS) provider, they execute highly aggressive extortion campaigns. LockBit's signature tactic involves StealBit, a custom-built data-stealing tool that extracts sensitive industrial information from compromised systems. The stolen data is then used as leverage, with threats to release it on the dark web if ransom demands are not met. This strategy not only heightens the pressure on victims but also introduces a secondary risk by potentially exposing the data to other malicious actors.

However, in 2024, a coordinated crackdown by law enforcement agencies – including the US Federal Bureau of Investigation (FBI), the UK's National Crime Agency (NCA) and Europol – delivered a significant blow to LockBit's operations. This joint effort led to the takedown of LockBit's website, the unmasking of its affiliate network, and the seizure of its cryptocurrency assets, marking a critical step in disrupting the group's activities.

Figure 1. A ransomware message from LockBit

Investing in cutting-edge cybersecurity and deploying rapid, decisive response strategies is no longer optional. It is now crucial. Enhanced detection capabilities are vital for accelerating incident response times and staying ahead of threats.

Global telecom sector attacks

Table 1 details cyberattacks from 2022 to 2024, including both the dates of the attacks and when they were discovered.

Table 1. Global telecom sector attacks, 2022-2024

Year	Country or area	Threat actor	Date of attack	Discovery date	Impact
2024	North America CSP	Unnamed (speculated as Black Basta)	February 2024	Not explicitly stated	Personal employee data exposed
2024	Latin America CSP	Trigona group	June 2022	February 2024	Significant service disruption, data encryption, risk of data leak
2023	North America CSP	Incident was attributed to an insider threat, "inadvertent disclosure," while the customer data exposure was linked to an external vendor	The discovery date is unknown, but the customer data was exposed by March 2023; the employee data breach occurred on or around September 21, 2023	The customer data exposure was resolved in January 2023, prior to being reported in March. The employee data breach was discovered on December 12, 2023.	The first incident exposed data of 7.5 million customers without revealing unencrypted personal data The second incident exposed personal details of 63,000 employees
2023	Europe CSP	Not specified	May 16, 2023	The incident was reported in June 2023	Limited to 7,500 customers; no evidence sensitive data was taken
2023	North America CSP	Seize	February 25, 2023	February 25, 2023	Risk to employee information
2023	Asia Pacific CSP	Unknown	November 8, 2023	November 8, 2023	Disruption to multiple services
2022	Europe CSP	KelvinSecurity (alleged)	First week of September 2022	Unspecified	Exposure of subscription details, identity documents and contact information
2022	Asia Pacific CSP	Unconfirmed; conflicting claims between CSP and an insider	Noticed on September 20, 2022	September 21, 2022	Exposure of names, birth dates, addresses and ID numbers

Insights by region

Following are key insights and trends from Nokia's Cyber Security Center in France, based on the latest regional analysis of cyberattacks.

Regional distribution

- North America stands out as the region with the highest number of attacks, highlighting its status as a major target, likely due to its concentration of technological infrastructure and large enterprises.
- Western Europe and East Asia also see significant activity, suggesting that areas with high economic output and advanced digital capabilities continue to attract cybercriminals.
- Regions like Central America and Eastern Europe report fewer incidents but are still notable for their specific vulnerabilities and types of attacks.

Nature of attacks

- In North America, attacks often involve advanced techniques such as ransomware and are sometimes suspected to be state sponsored, focusing on data theft and service disruption.
- East Asia's incidents frequently involve inadvertent exposures by companies themselves, leading to significant data leaks.
- Western Europe tends to experience a mix of cyber espionage and financially motivated breaches, indicating a diverse threat landscape.

Key threat actors and impacts

- In regions like South America, groups such as Trigona focus on service disruptions and data encryption, severely impacting business operations.
- Europe has seen prominent activity from groups like Killnet, which have launched attacks causing widespread service outages.

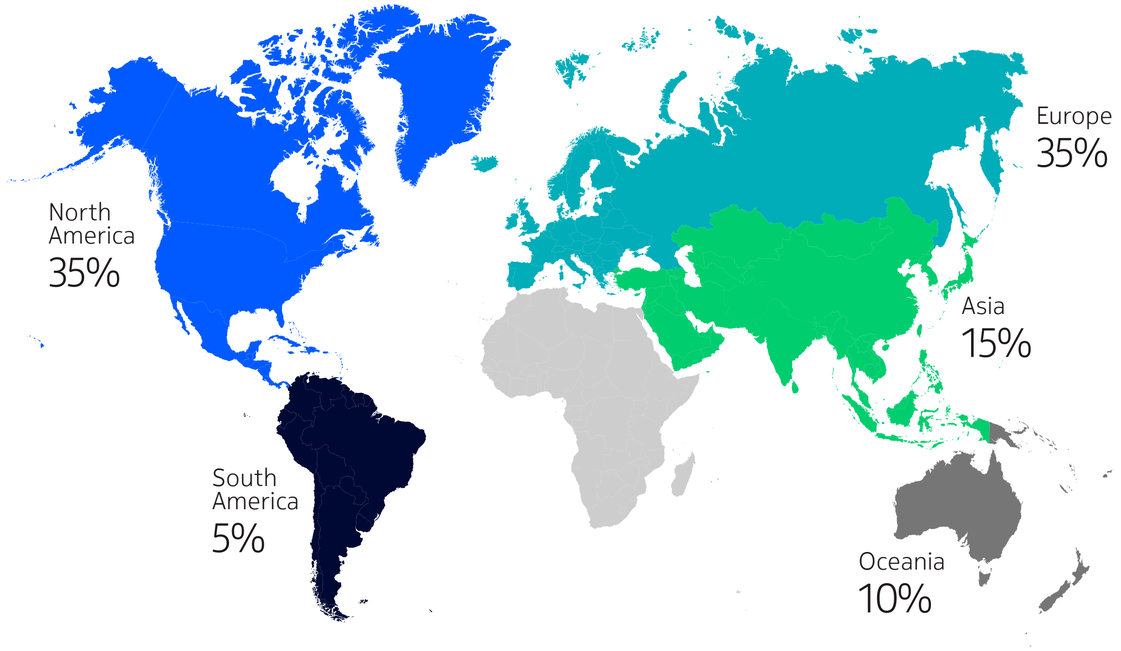
Trends and recommendations

The persistent focus on technologically advanced and economically significant regions highlights the ongoing risk for robust cyber-security defenses. The data also reveals a trend that threat actors are exploiting both technological vulnerabilities and human factors, suggesting that a comprehensive security strategy is essential.

To combat this, here are some key recommendations:

- Enhancing cybersecurity measures, including threat intelligence and rapid response capabilities, is crucial, especially in high-risk regions.
- Increased collaboration and information sharing among international security agencies and private sectors can help mitigate the impact of these attacks.
- Investing in cybersecurity education and awareness programs will be vital to defend against socially engineered attacks and inadvertent data exposures.

Figure 2. Distribution by region of cyberattacks against the telecom sector



Insights by country

Following are observations and emerging trends from our latest analysis of cyberattacks, broken down by country.

Countries most targeted

- The US was the most frequently targeted country, indicative of its large digital infrastructure and the high value of its corporate data.
- Ukraine also showed a significant number of attacks, likely due to geopolitical tensions and cyber warfare incidents in the region.
- The UK and Germany were also notable for experiencing cyberattacks, reflecting the broader trend of targeting economically significant and technologically advanced European countries.

Nature of attacks

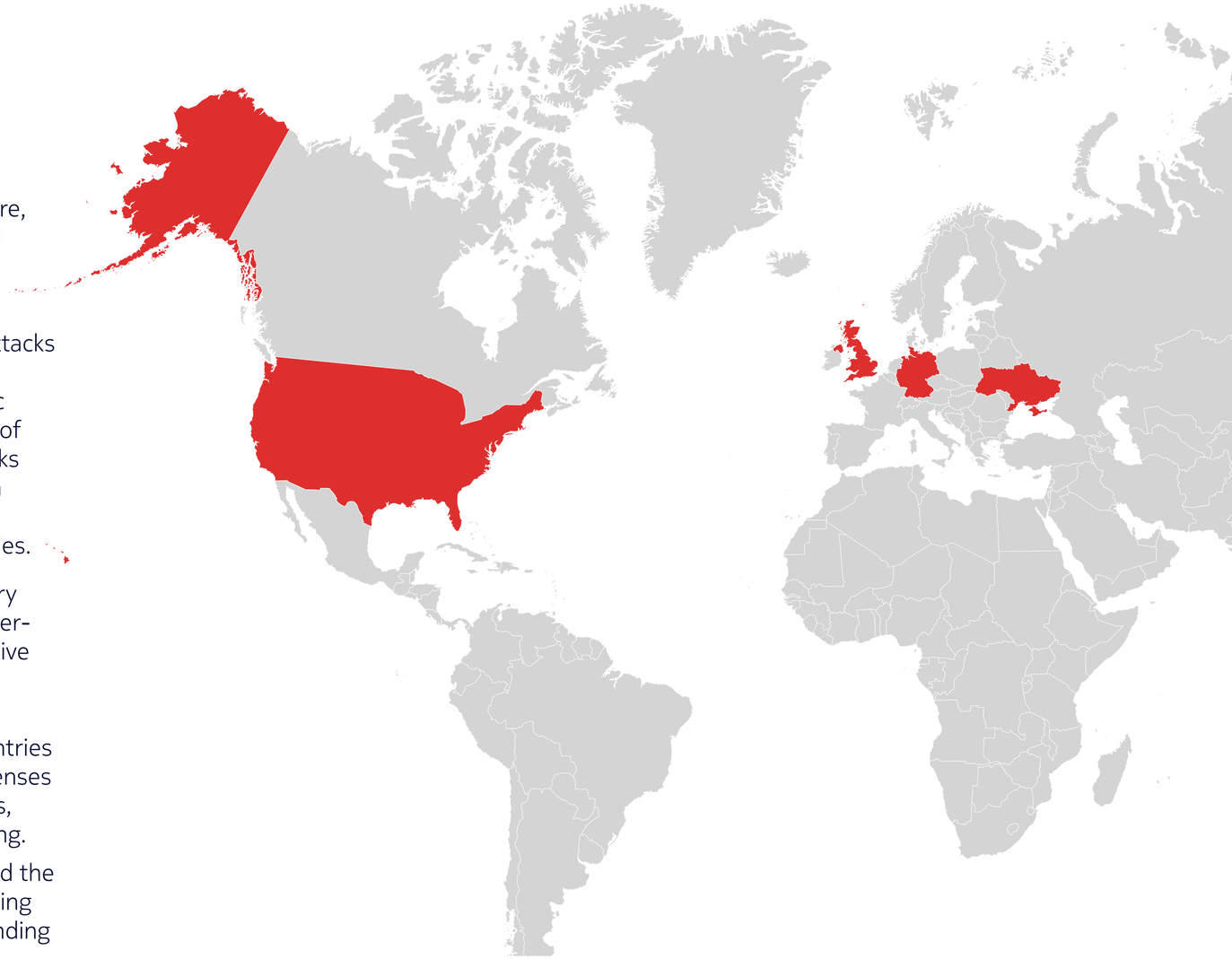
- In the US, attacks included both ransomware and insider threats targeting a range of sectors, from telecom to government. The variety of attacks reflects the broad. spectrum of valuable assets and sensitive information held by entities in the country.
- In Ukraine, the attacks were more focused on telecommunications and critical infrastructure, possibly due to ongoing conflicts and the strategic importance of disrupting these services.
- Attacks in the UK and Germany often involved data breaches and ransomware, aimed at extracting financial gains and disrupting services.

Trends and recommendations

We are seeing a clear trend where cyberattacks are increasingly aimed at nations with substantial global influence and economic power, particularly those at the forefront of technological advancements. These attacks are becoming more sophisticated, using a blend of techniques to exploit everything from human errors to system vulnerabilities.

The distribution of cyberattacks by country underscores the need for heightened cyber-security awareness and enhanced protective measures, particularly in nations that play significant roles in the global economy.

- Nations and organizations in these countries need to bolster their cybersecurity defenses through advanced security technologies, regular audits and continuous monitoring.
- Collaboration between governments and the private sector is also crucial for developing more resilient infrastructure and responding promptly to cyber incidents.



Understanding the telco security landscape

In cybersecurity, there are two distinct worlds: conventional IT security and telecom network security. Both are important but differ significantly in their scope, focus, features, and challenges.

The telecom sector is characterized by vast and complex network infrastructure that is essential to providing uninterrupted communication services. With the advent of 5G and the Internet of Things (IoT), CSPs must manage an ever-increasing number of connected devices and a higher volume of data traffic. This expansion of the threat surface requires a specialized approach to security.

For CSPs, there is a need for both information technology (IT) and telecom network security, but they often converge under a single leadership umbrella. In a 2023 global survey by TM Forum of 40 telco operators at the director level or above, 71% of respondents said their organization has a single Chief Information Security Officer (CISO) or Chief Security Officer (CSO) across both enterprise IT and network domains.

To safeguard their organizations and protect critical data assets, it is critical that CSPs understand the differences between IT and telecom network security.

Anatomy of breaches in IT and telecom network security

IT security incidents range from common threats like phishing and weak passwords to more severe issues such as data theft, compromised databases and banking trojans. These attacks can disrupt services and expose user data, including personally identifiable information (PII) and credit card details.

In the specialized field of telecommunications network security, incidents are far more severe and can have significant consequences for end customers. Threats include eavesdropping on subscriber or network data, signaling storms targeting the radio access network (RAN)/core and cross-technology attacks on roaming interfaces (SS7/GTP), and compromised CSP workloads and network functions. These attacks can result in network failures and country-wide communication outages that hinder access to emergency services and financial transactions.

The stakes are much higher when it comes to CSP network security breaches. While IT security attacks often result in data theft and service disruptions, breaches in CSP networks can have life-or-death consequences.

Table 2. IT security versus telecom network security

IT security	Telecom network security
Components	
Industry agnostic such as laptops, mobile devices, intranet, IT applications and data centers	Purpose-built networks such as core, RAN, transport, access 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 and GTP
Skill sets	
Skills in endpoint security (mobile, desktop servers), app security, firewalls and secure gateways	Expertise in telecom network topology, communication protocols, 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

SPOTLIGHT: How IT and telecom network security solutions differ

Many CSPs are unaware of the distinctions between telecom-specific and generic security solutions. Despite sharing similar names, these solutions have fundamentally different approaches to network security. For example, generic endpoint detection and response (EDR) systems are tailored to enterprise environments, protecting workstations, end-user devices, and IT data centers. In contrast, telecom-specialized EDR systems have agents running on critical infrastructure to protect against telecom-specific attacks while maintaining the functionality of network elements. These specialized solutions are engineered to have minimal impact on the workloads, ensuring network performance is not affected.

In July 2024, a defective update to EDR software triggered a global IT outage that led to widespread disruptions. Airports were forced to ground flights, financial institutions faced ATM outages, and hospitals had to cancel procedures due to system failures. This event underscored the importance of having a telecom-specific security solution to ensure security agents on telecom endpoints do not interfere with critical functions, and to prioritize network functionality and uptime.

The critical role of a tailored database in building a cyberattack knowledge base

Intelligence is the key to success in cybersecurity. Having the right information at the right time requires the deployment of sensors to collect data, analyze it, and produce actionable intelligence.

Automation supported by recent machine learning and large language model techniques is critical to drawing insights from the massive amounts of data that businesses manage today. Even still, the quality of the information these systems output depends on the quality of the information provided as input.

The most effective approach involves using recognized and robust standards combined with data centralization and management solutions that leverage the latest developments. This includes threat intelligence expressions such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) ontology, playbook automation, and AI integration capabilities.

Threat intelligence platforms are highly customizable, allowing users to add multiple threat intelligence sources. They also include widgets that retrieve and display specific information relevant to the telecom sector. Automation playbooks also make it possible to pre-analyze data and draw insights quickly. The following figures demonstrate a sample of the capabilities threat intelligence platforms have to identify threats faster.

Figure 3 shows an example of a customized dashboard for an open-source threat intelligence platform.

Figure 3. Customized OpenCTI threat intelligence platform dashboard used to track cyber telecom attacks and collect cyber operational data

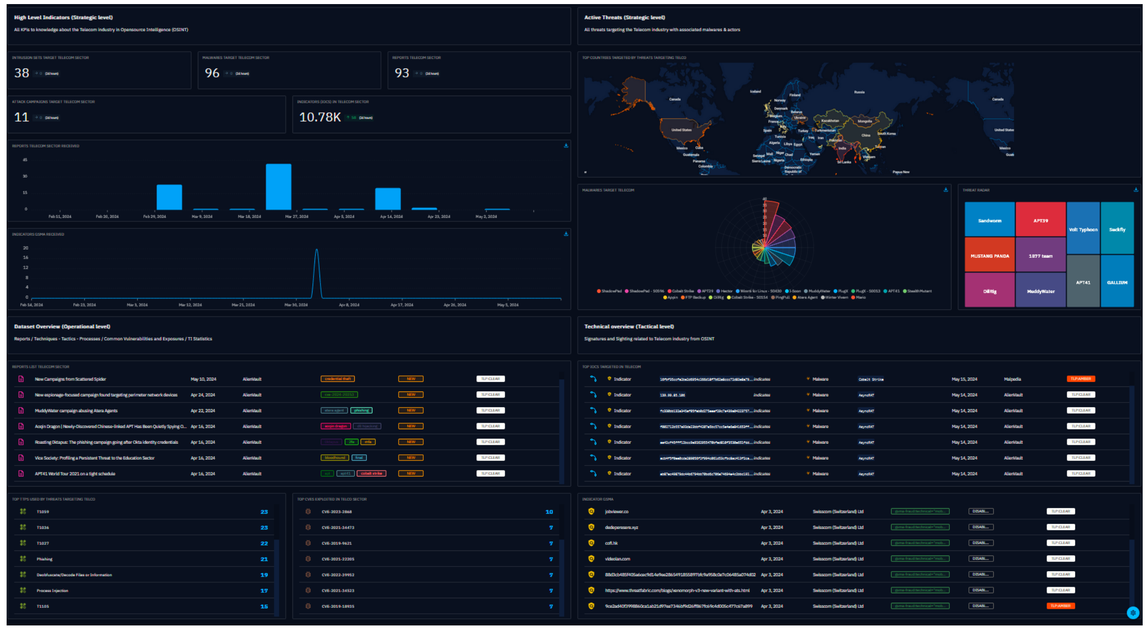


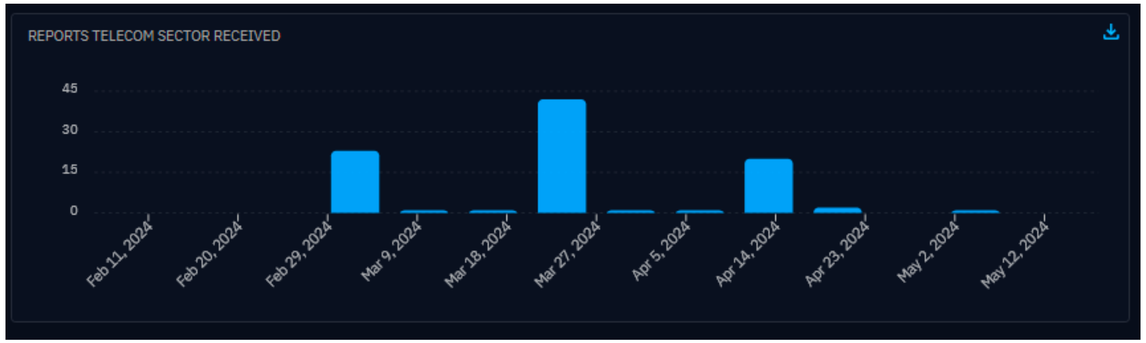
Figure 4 shows examples of key telecom cyber threat activity that can be monitored from open-source intelligence (OSINT).

Following is a breakdown of what each key performance indicator (KPI) means:

- **Intrusion set telecom sector widget:** Displays information about intrusion sets specifically targeting the telecom sector.
- **Malware target telecom sector:** Shows data about malware that targets the telecom sector.
- **Report telecom:** Generates reports related to telecom threats and incidents.
- **Attack campaign:** Number of cyber campaigns launched by threat actors.
- **Number of indicators of compromise (IOCs):** IOCs found for attacks against CSPs.

Figure 4. High-level cyber threat activity statistics

Figure 5. Dates and number of reports of cyberattacks in the telecom sector



GSMA MoTIF Framework: A vital resource for CSPs

The GSMA Mobile Threat Intelligence Framework (MoTIF) is designed to systematize the understanding and mitigation of adversarial threats against mobile networks.

For CSPs, MoTIF refers to a targeted approach to defending against mobile network attacks, encompassing every generation from 2G to 5G. It also covers essential services like roaming, SMS, and VoIP, ensuring comprehensive protection across all mobile technologies.

MoTIF's scope includes adversary TTPs not covered by other public frameworks, incorporating unique mobile network threats like fraud against networks and their customers. It serves to document and analyze how adversaries exploit mobile networks, offering structured descriptions of their actions and impacts. The framework details TTPs by breaking down adversarial activities into tactics for easy categorization and response.

The framework also introduces several core concepts such as "techniques" and "sub-techniques" specific to mobile network security. These are aligned with MoTIF's High-Level Strategy (HLS), which provides an overarching strategic context for attacks, helping guide mobile network operators in their defense strategies. HLS components include the attack goal, attack surface and specific attack targets, with each element given a distinct MoTIF number for identification and reference.

MoTIF also integrates with the STIX framework, enabling interoperability with other threat intelligence tools and facilitating the exchange of information across different platforms and stakeholders involved in mobile network security.

By providing a comprehensive and specialized framework, MoTIF assists security professionals in not only understanding and tracking adversarial tactics but also in developing and refining defensive measures tailored to the complex environment of mobile networks. This strategic tool thus plays a crucial role in enhancing the security resilience of mobile communication infrastructures globally.

What does this mean for CSPs?
MoTIF is a vital resource for CSPs as it empowers them to proactively combat evolving mobile threats and safeguard their networks, customers and reputation.

Through shared intelligence and collaboration on best practices, MoTIF enables CSPs to:

- Stay ahead of the curve: Gain access to a wider pool of threat intelligence, including early detection of malware, phishing campaigns, and other malicious activities targeting mobile users.
- Enhance customer trust: Proactively address security threats, protecting users from financial fraud, data breaches, and other security risks that can impact customer trust and satisfaction.
- Optimize operational efficiency: Reduce costs associated with security incidents, such as remediation efforts, customer support, and reputational damage.
- Meet regulatory requirements: Align with industry regulations and best practices, demonstrating a commitment to security and meeting compliance obligations.

This framework empowers CSPs to move beyond reactive security measures and adopt a proactive approach to threat management.

SPOTLIGHT: How GTPDOOR works

Earlier this year, a new telecom-oriented malware named GTPDOOR was found, likely attributed to UNC1945 (Mandiant) / LightBasin (CrowdStrike). This malware allows attackers to execute remote commands and stealthily extract the output over the GPRS (general packet radio service) roaming exchange (GRX) backbone that interconnects mobile network operators for roaming purposes.

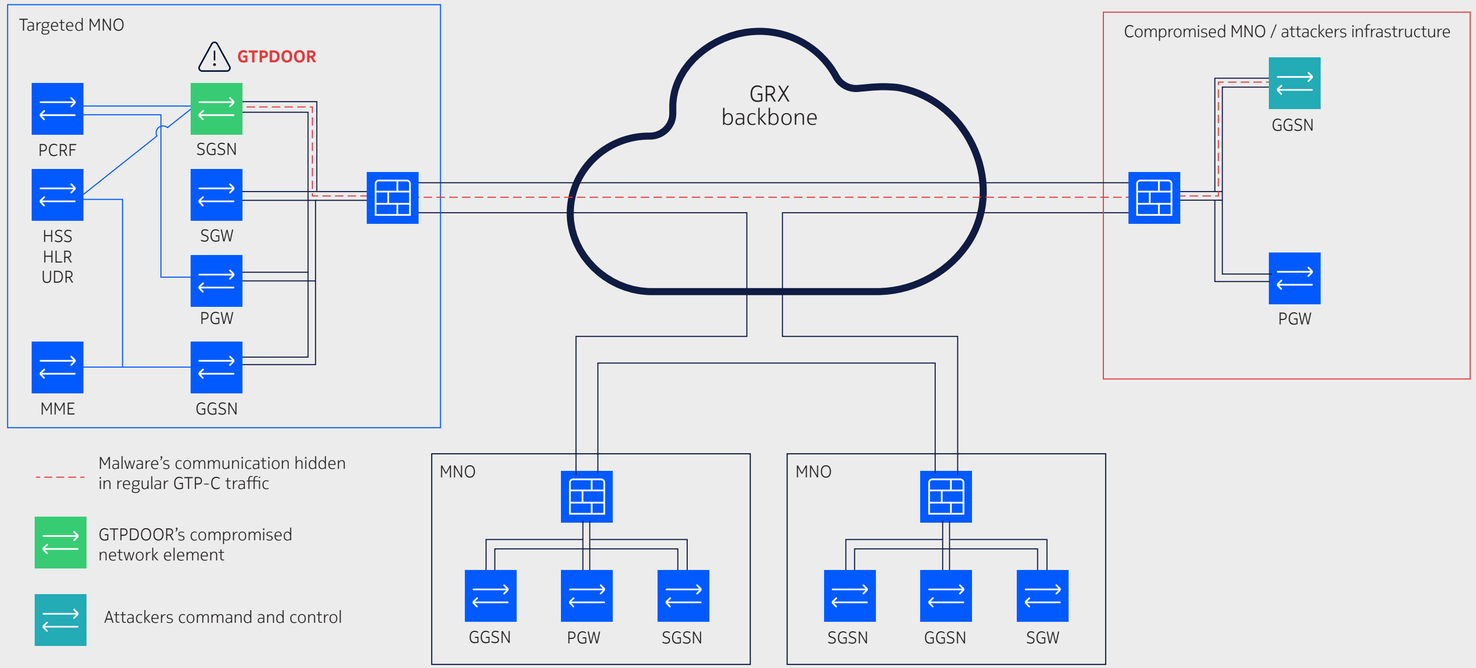
In the 2023 Threat Intelligence Report, we highlighted the LightBasin threat with an analysis using the FiGHT framework. For reference, LightBasin is a malware that mainly allows attackers to run commands on the compromised host and exfiltrate outputs over GTP-C protocol using the GRX network. Hackers can move laterally within the mobile network operator network to non-GRX-connected devices.

Security researchers have uncovered evidence of at least 13 telecommunication companies worldwide compromised by LightBasin dating back to at least 2019. GTPDOOR showcases the capabilities of the LightBasin arsenal for backdoors and gives a sense of the group's level of knowledge.

GTPDOOR was built to avoid detection. Its flow is hidden inside regular GTP-C traffic and captured using a raw socket, and it implements a kind of access list to allow only specific IPs to use it. The process also mimics a kernel thread by renaming itself "[syslogd]." GTPDOOR uses raw sockets for communication rather than opening a new port, which can be detected.

As hackers refine their tactics to evade detection, strong, multilayered defense mechanisms become increasingly critical. The emergence of GTPDOOR serves as an important reminder of the need for continuous monitoring, advanced detection capabilities, and robust security measures to safeguard critical telecom infrastructure.

Figure 6. GTPDOOR enabling malicious communication through GTP-C traffic over GRX



use it. The process also mimics a kernel thread by renaming itself "[syslogd]." GTPDOOR uses raw sockets for communication rather than opening a new port, which can be detected.

As hackers refine their tactics to evade detection, strong, multilayered defense mechanisms become increasingly critical. The emergence of GTPDOOR serves as an important reminder of the need for continuous monitoring, advanced detection capabilities, and robust security measures to safeguard critical telecom infrastructure.

The hidden threat of system-on-chip (SOC attacks): Securing 5G innovation

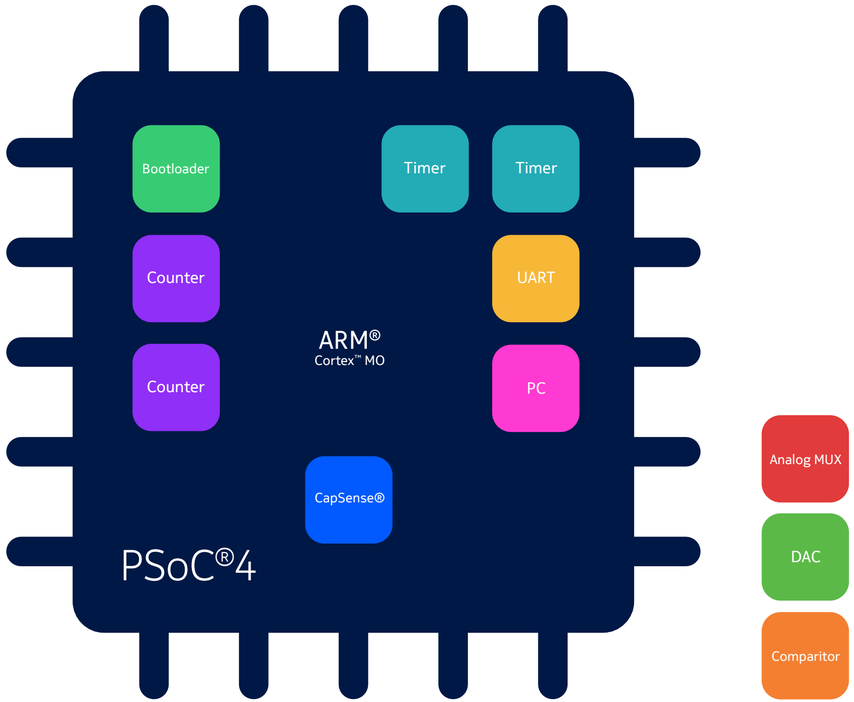
What is a system-on-chip?
System-on-chips (SoCs) are hardware-integrated circuits that integrate computer components or other electronic systems. In terms of cost and reliability, SoCs are one of the only feasible solutions for achieving higher performance while minimizing power consumption. This technology is embedded in base station solutions to boost network performance, cut energy consumption, and meet the escalating demands of 5G networks.

Unlike microcontroller units, which are small computers with integrated boards, SoCs are integrated into a single-chip package that does everything that once required multiple chips. SoCs are typically a hardware encapsulation of one or more central processing units (CPUs), memory, microcontrollers, digital signal processors (DSPs) and accelerators.

SoCs are used across a wide range of industries to enhance device performance and efficiency. In the realm of IoT, SoCs are the backbone of smart devices and sensors used in smart homes, industrial automation and healthcare. Their ability to integrate multiple functions onto a single chip allows for compact, low-power devices that can efficiently collect, process and transmit data. This is crucial for applications such as smart thermostats, wearable health monitors and remote industrial sensors.

SoCs are also critical in the development of high-performance computing and data centers. They are used in servers and specialized processors for tasks like machine learning and artificial intelligence (AI). These chips help in handling large volumes of data and complex computations with greater speed and efficiency, driving advancements in fields such as big data analytics and scientific research.

Figure 7. Illustration of a SoC



SoC attacks

SoC attacks have emerged as a significant concern in cybersecurity. With the proliferation of SoCs across a wide range of devices and industries, these attacks are becoming more frequent and sophisticated, posing substantial risks to both individuals and organizations.

While the integration of numerous functions onto a single chip enhances performance and efficiency, it also creates a larger attack surface. Cybercriminals are increasingly targeting SoCs to exploit vulnerabilities in various components, such as firmware, software and hardware interfaces. These attacks can lead to unauthorized access, data theft and even complete system compromise.

One of the primary drivers of the growth in SoC attacks is the widespread adoption of connected devices, especially in the IoT space. Often designed with cost and functionality as primary considerations, many IoT devices lack robust security measures, making them attractive targets for cybercriminals.

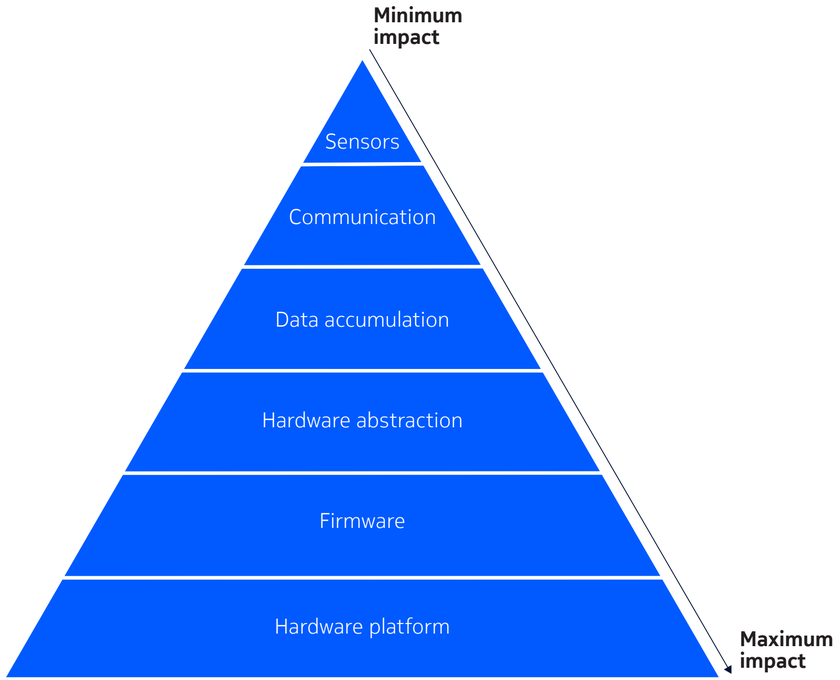
The consequences of SoC attacks can be severe. In critical infrastructure, such as energy grids or transportation systems, an attack on SoC-based controllers could lead to widespread disruptions and safety hazards. In the automotive industry, vulnerabilities in SoCs used in advanced driver-assistance systems or vehicle-to-everything communication could result in unauthorized control over vehicles, posing significant risks to public safety.

SoC security

Given the growing threat, it is crucial to prioritize the security of SoCs. To effectively safeguard against SoC-based threats in telecommunications, particularly within the 5G infrastructure, CSPs should consider implementing a comprehensive set of robust security measures such as strong data encryption, enhanced endpoint detection and response agents, strict access control on the principle of least privilege, and an artificial intelligence (AI)/ machine learning (ML) advanced threat analysis and mitigation orchestration. These measures are designed to enhance the resilience of the network, protect data integrity, and ensure continuous service availability.

It is vital that end users stay informed about devices' security features and regularly update software and firmware. Implementing network security measures, such as firewalls and intrusion detection systems, can also help protect devices that rely on SoCs.

Figure 8. Relative impact of attacks on different components



DDoS traffic and attack trends

Rising DDoS attacks and shifting threat trends

In 2024, DDoS traffic growth continued to surpass the growth rates of all other network traffic types. DDoS traffic volume increased 166% year over year (between June 2023 and June 2024). This growth has been fueled by the proliferation of insecure IoT devices, which have more bandwidth available to them due to gigabit and multi-gigabit broadband offers.

Many attacks continue to employ multi-vector strategies, but the use of Domain Name System (DNS) amplification still constitutes the primary legacy driver: 36% of all DDoS attacks are driven by DNS amplification. Other vectors — such as Network Time Protocol (NTP) amplification, Connectionless Lightweight Directory Access Protocol (CLDAP) amplification and Memcache amplification — are rapidly declining, with a recorded 20–70% year-over-year drop, depending on the vector.

Botnets remain a significant threat in the DDoS landscape. While the potential number of unsecured devices that can be used in DDoS attacks is in the hundreds of thousands, if not millions, most individual botnet DDoS attacks involve a small number of bots: 60% of all botnet DDoS attacks involve fewer than 100 bots.

Carpet-bombing DDoS attacks

Attacks on multiple targets using a range of target IP addresses within a network or multiple networks are referred to as carpet-bombing DDoS attacks. Unlike DDoS attacks that target specific servers or services, carpet-bombing DDoS attacks aim to disrupt a whole subset of IP addresses, attacking a broader array of resources and infrastructure. In 2024, they grew in scope: 13% of carpet-bombing DDoS attacks targeted 256 destination IP addresses or more, and 2.8% of attacks targeted 1,024 IP addresses or more. The largest observed carpet-bombing attack in 2024 targeted more than 16,000 IP addresses. The top vectors used in carpet bombing attacks are a small subset of what is otherwise observed for other types of DDoS attacks: 80% are DNS-based, 16% use botnets and 2% use Transmission Control Protocol (TCP) reflection.

Attack durations

There was a marked shift toward shorter attack durations: 44% of the DDoS attacks observed in 2024 lasted less than five minutes, underscoring the necessity of a rapid, automated response to detect and neutralize these threats in seconds rather than minutes.

This shift to shorter attack durations is not "good news" per se, because the number and frequency of DDoS attacks are also on the rise. Many CSPs see large numbers of significant DDoS events that require attention by security operations teams. In many networks, the frequency of these events has grown from one or two a day to well over 100 per day.

Many of these shorter attacks exhibit a level of dynamism that indicates added sophistication, likely driven by artificial intelligence (AI). Attacks on the same targets frequently employ morphing techniques, changing attack vectors and changing behavior during the attack. This trend underscores the need for advanced, AI-driven defense strategies to combat evolving DDoS threats.

2024: The surge of AI in DDoS attacks

DDoS is a well-established area within computer science and software engineering, both in terms of the methods and techniques used to coordinate and launch attacks and in terms of protection and defense against them.

However, 2024 was a turning point, as new capabilities were introduced that made DDoS more pervasive and visible and brought it into mainstream conversations and news.

As AI technology continues to rise steadily across all types of applications, the novel use of AI for launching DDoS attacks was also evident in 2024. The use of AI for DDoS attacks leads to a stepwise increase in malicious actors' capabilities and threat potential.

The early 2020s saw the exponential increase of botnet-driven DDoS traffic, enabled by hundreds of thousands of IoT devices providing virtually unlimited distributed compute and increased accessibility to gigabit (and multi-gigabit) uplink connectivity.

Botnets remain a major driver in today's DDoS landscape, accounting for about 60% of traffic monitored by Nokia Deepfield through its Emergency Response Team (ERT). However, 2024 has been the year of AI and automation for new DDoS threats — and the year in which significant abuse of residential proxies started in large-scale DDoS attacks.

Residential proxy abuse is on the rise

Proxies have been around since the advent of the internet, facilitating two-step connectivity: one step to the proxy, and the second to the desired destination on the internet. Running on consumer devices using a fixed or mobile broadband connection, residential proxies (also known as RESIP) use proxy software that aims to represent the originating system or a device toward the internet with a different IP address or a number of IP addresses that dynamically change over time.

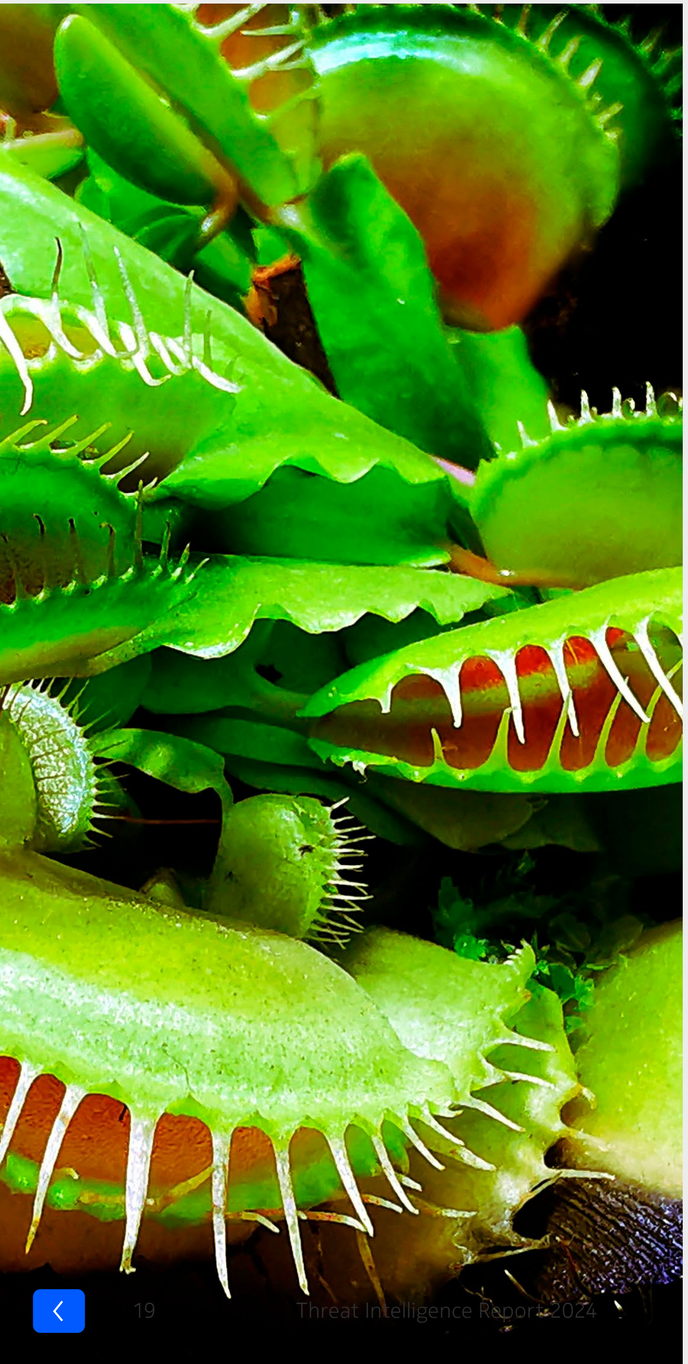
Residential proxies have been widely used for a variety of use cases. Some sit in a gray legal or ethical zone, such as web scraping, price monitoring, spam, and sneaker auctions. Others are used in criminal activities, including identity theft, phishing, click/credit card/auction fraud, malvertising and many more.

The main appeal for users of residential proxies — that their traffic will originate from a "clean" IP address that changes dynamically — also attracts DDoS threat actors. This is because traffic sent from and through these proxies is not likely to be listed on various ill-reputation lists associated with prior botnet activity. This also affords attackers some amount of obfuscation, making it more difficult to trace back the real source of malicious traffic.

From the perspective of security teams, there is one major difference between bots and residential proxies: scale.

While the number of bots used for DDoS today is in the order of several hundreds of thousands, several residential proxy service providers offer access to tens of millions of IP endpoints. This makes the problem space vastly larger and allows threat actors to choose which country (and even city) they want to reflect attacks from.

Lured by a "free" virtual private network (VPN) service, people who install residential proxy software on their devices may inadvertently turn their devices into DDoS attack endpoints. Residential proxies have already been exploited this way and are behind many DDoS attacks. With millions of IP addresses that appear legitimate and have not (yet) been compromised in observed attacks, these endpoints can and continue to generate DDoS traffic that can pass traditional DDoS security systems.



SPOTLIGHT:
How threat actor group NoName016(57) uses residential proxies

One of the most active malicious users of residential proxy services is a pro-Russian hacktivist group called NoName016(57). The group openly recruits volunteers through a Telegram channel and provides a daily list of targets through their command-and-control server, which participants' machines then attack using the DDoSia toolkit software. These attacks are executed synchronously to overwhelm the targeted web server.

This type of attack is not a volumetric DDoS attack. Rather, the NoName016(57) attacks primarily rely on HTTPS POST requests using valid parameters, indicating some level of reconnaissance on a given target ahead of the actual attack.

When the Nokia Deepfield Emergency Response Team (ERT) first investigated the attack sample provided by a customer under attack, the bandwidth represented just 10 Mbps (<5 kilopackets per second [kpps]), which is far below typical volumetric thresholds. While these attacks use low-volume attack traffic, they can often be enough to disrupt service availability because each request generates a significant workload at the application layer.

A common way to mitigate this type of attack is to create a geofence that permits traffic only from countries where legitimate users are expected to be. This has been evident when threat actors post evidence of the relative success of their attack(s), marking them with a common "blocked by geo" note.

Geo-blocking is not a silver bullet. Using residential proxies and a large pool of IP addresses that are not yet compromised, attackers can pick which countries they want malicious traffic to appear to originate from. This means a large portion of the traffic will not be blocked, but legitimate users from different countries will be blocked based on their geo-IP location. This has resulted in high rates of false negatives (DDoS not detected) and false positives (legitimate traffic identified as DDoS).

Nokia Deepfield ERT devised an alternative mitigation method that only blocks proxy traffic at the edge of the service provider network. For more details, refer to the Nokia blog post on adding layers of DDoS protection to IP routers.

Threat actor profile: NoName016(57)

- Pro-Russian hacktivist group that emerged in March 2022 following Russia's invasion of Ukraine
- Conducts DDoS attacks against various websites from organizations (both governmental and private) deemed "anti-Russian"
- Uses Telegram channels to claim responsibility for attacks, make threats and share tools like DDoSia, their custom DDoS software
- Developed a cryptocurrency payment system to reward contributors (volunteer-based system as opposed to malware/exploitation)
- Attacks primarily rely on web DDoS, i.e., crafted HTTPS GET/POST requests that can overwhelm a server even with a relatively low number of sources/requests
- Attackers use proxy services to hide their IPs from known botnet lists and to pretend that traffic originates in the destination country

Automation is driving attack sophistication

While proxy-based, application-layer DDoS attacks rose in 2024, volumetric DDoS (network-level) traffic volume did not let up.

Nokia Deepfield observed a notable change in the methods used in these attacks. Instead of using mostly fixed attack vectors and targets over the lifetime of a given attack, we noticed rapidly evolving DDoS vector changes and microbursts, as well as automated target changes over many subnets.

Morphing attacks

Morphing attacks (also referred to as adaptive or dynamic DDoS) can present significant challenges for mitigation, particularly when it comes to out-of-data-path solutions used by large service providers.

Along with obvious attack vector changes — for example, quickly switching from botnet-based TCP SYN flood to User Datagram Protocol (UDP) flood — we also observed behavioral changes within a given attack vector. For instance, several customers were targeted with a multi-hundred Gbps UDP flood featuring a specific packet length invariant, then quickly by a different size. This tactic can be more challenging to combat in manual mitigation scenarios where identifying a consistent pattern leads security teams to instantiate a specific filter entry on the network edge.

More saliently, during several such attacks, we observed rapid shifts in attack patterns as a response to newly created router filter entries. In other words, the attacks were responding to defense tactics and changing their tactics accordingly.

While it is possible for well-trained and on-task humans to do this, software automation that probes the target's reachability and adapts DDoS payloads accordingly can clearly accelerate the response time. Network operators have had access to different levels of automation for configuration and performance management, but it seems that certain threat actors have gained some level of automation for their DDoS activities.

Exploring distributed attacks and automation: Qualitative research on evolving tactics

We also observed hundreds of attacks for a given customer in which the destination addresses changed continuously throughout the attack's lifetime.

Carpet-bombing attacks targeting a range of IP addresses or a whole subnet have been around for some time. However, traditionally, the ranges of IP addresses targeted have been static. In this new generation of distributed carpet-bombing DDoS attacks, attackers spread the malicious traffic across several subnets in an attempt to evade detection (for defense systems that monitor per-host bandwidth) and to raise the cost and complexity of mitigation.

In 2024, we observed a significant increase in highly distributed carpet-bombing attacks. These attacks not only targeted a vast number of hosts (one of the largest attacks we observed targeted 49 individuals/24 subnets) but also alternated between different destination subnets over time.

These morphing distributed carpet-bombing DDoS attacks make protection much more challenging for conventional scrubbing solutions. This is because they depend on traffic diversion to be effective, and diverting traffic aimed at a large number of IP addresses that are dynamically changing over time represents a great challenge for the speed and accuracy of detection and the scalability of mitigation.

Learnings and recommendations

Detecting DDoS attack traffic in 2024 continues to be challenging because traditional approaches to detection, such as thresholds or baselines, are no longer effective. Botnet traffic and shorter DDoS attacks circumvent traditional anti-DDoS systems. Due to this, the primary challenge today is to improve detection, accuracy and speed of new generations of DDoS attacks as they happen and to ensure this detection happens in seconds, not minutes.

To combat contemporary DDoS attacks, modern defense approaches must better understand the larger internet security context. Continuous monitoring and tracking and real-time updates can help identify a much wider range of new attack points originating from botnet DDoS and residential proxies.

Additionally, while network owners have traditionally been guarding only the "front door" (i.e., internet peering/transit links), attacks now come from many other entry points, including their customers, partners (e.g., cloud providers), and compromised devices in their networks. Legacy-based solutions cannot adequately monitor and detect DDoS traffic originating from these new entry points. Forward-looking DDoS solutions need to enable protection from all directions: inbound and outbound, across all network edges.

CSPs and data center operators should evaluate DDoS mitigation solutions based on their ability to detect new generations of attacks with improved accuracy and speed, but also scale, cost and efficacy. They should also consider DDoS mitigation false-positive tolerances against the cost and complexity of different solutions.

Global Security Operations Center (SOC) through Managed Security Services (MSS) trends

Managed Security Services driving new trends in global SOC

At Nokia's global security operation centers, our telecom experts manage more than 360,000 incidents and triage more than 3,500 security issues, including more than 20 global critical incidents across multiple SOC in the APAC, EU + MEA, and Americas regions. Our experts track hundreds of security incidents each month, while our EDR team monitors a similar volume every six months. This section dives into the evolving security trends these teams have uncovered.

Trends identified through telecom interface assessments and penetration testing

Our telecom security specialists evaluate CSP networks by emulating the tactics, techniques, and procedures of threat actors, offering a hacker's perspective in an operational telecom environment. The following describes how our team identifies key security trends and critical concerns through in-depth analysis of CSP telecom nodes.

5G core network

- Due to the lack of Transport Layer Security (TLS) and Oauth2 implementation in CSP networks, the basic security principle of 5G mutual authentication and token-based communication with the use of the network repository function (NRF) is a year away. For now, the CSPs focus is on first building the networks with basic requirements. Enhancing security is a secondary priority.

5G roaming

- Globally, very few CSPs have implemented 5G roaming security edge protection proxy (SEPP). This means that legacy security issues with roaming on old technologies remain.

Interconnect (SS7/GTP/DIAMETER)

- Gray areas remain even after implementing an appropriate solution, which might be due to misconfigurations or a lack of signaling firewall features. These gray areas could allow certain attacks on subscribers and networks from a rogue roaming partner network. Examples of tactics that may be possible include location tracking, Unstructured Supplementary Service Data (USSD) code fraud, call interception, tunnel hijacking and denial of services on network nodes.

Radio access network (RAN)

- International mobile subscriber identity (IMSI) catching remediation in 5G can take a long time on the ground because old SIM cards cannot be updated with applets that support subscription concealed identifier (SUCI) computations. SIM cards must be replaced for this, which comes with a cost. End users are also generally unaware of the benefits of IMSI hiding, making it a non-priority for them.
- Weak or no ciphering over the air interface is one of the security concerns still unaddressed by legacy operators due to handset capability issues and legal requirements in certain countries.
- The second most common security concern is a fake base transceiver station (BTS) attached to an actual core network. This threat persists due to the lack of mutual authentication between the RAN and core network access in LTE and 5G. While some operators have started using the certificate/IPsec base solution to mitigate this risk, there is still a long way to go to overcome it.
- User plane integrity protection in 5G to mitigate man-in-the-middle attacks was also frequently missing.

Open radio access network (ORAN)

- The lack of IPsec for authentication and encryption on fronthaul, mid-haul, and backhaul undermines ORAN's core security features. As these interfaces operate on distinct transports, there is a false sense of security. This gap leaves unprotected cell sites vulnerable to exploitation.

VoLTE/VoWiFi

- Due to the lack of security hardening and availability of appropriate solutions, security issues such as billing fraud and caller ID spoofing still exist.
- Another significant security issue is the lack of traffic separation, which can expose network nodes publicly and allow unauthorized access to them.
- If VoIP traffic encryption is missing, whether for operational and/or financial reasons, it allows user voice traffic to be intercepted.

Fixed-line networks

- The fixed-line core network remains a top target for attackers due to a lack of traffic separation and hardening of CSP devices.
- Due to the routing definition at the IP/transport nodes and exposure of CSP devices outside the CSP's control, an enterprise became the target of several cyberattacks, including denial of services, caller ID faking, unauthorized takeover and unauthorized interception of calls.

Key findings revealed in quarterly vulnerability assessment and penetration testing (VAPT)

Every quarter, our network vulnerability assessment and penetration testing (VAPT) experts provide scanning, analysis and remediation support for an average of more than 1500 IP addresses on average per month. Some of the critical and high vulnerabilities identified include:

Protocol misconfiguration

Our team observed multiple protocol misconfigurations, for example, with Secure Socket Layer (SSL)/TLS. Protocol misconfigurations can unintentionally expose vulnerabilities in network communication, potentially leading to unauthorized access, data breaches, or service disruptions.

Potential impacts

- Padding Oracle on Downgraded Legacy Encryption (POODLE) attacks
- Man-in-the-middle attacks
- Denial of service (DoS) attacks
- Data interception

Missing security patch updates

Vendors release fixes or updates to address known vulnerabilities or weaknesses in their products. When patches are not applied, systems remain exposed to potential security threats. Attackers can exploit these vulnerabilities to gain unauthorized access, steal data, or disrupt services. It is important to apply patches promptly to avoid security breaches and compromised integrity, confidentiality, and availability of systems and data. 90% of the vulnerabilities identified solely because of not implementing security patches in the network.

Potential impacts

- Increased vulnerability exploitation
- Malware infection
- Data breaches and increased attack surface

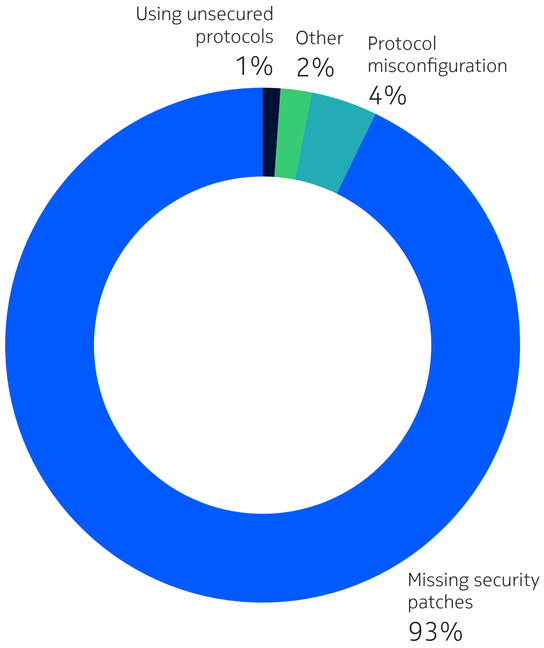
Using unsecured protocols

Our team observed the use of protocols like FTP and HTTP. Unsecured protocols pose significant security risks, with data transmitted through them vulnerable to interception, tampering, and unauthorized access. The use of secure protocols is recommended.

Potential impacts

- Man-in-the-middle attacks
- Unauthorized access
- Compliance concerns
- Data exposure and tampering

Figure 9. Vulnerability classification among CSPs



90% of the vulnerabilities identified solely because of not implementing security patches in the network.

Top vulnerabilities and application security trends identified (AppSec)

On average, our application security experts perform more than 200 scans per year. The vulnerabilities identified included:

Broken authentication

- Authentication is a critical component of ensuring the security of web applications. A security risk is created when specific endpoints within applications can be accessed without the need for authentication.

Session hijacking

- With session hijacking, the attacker forces the user's session identifier (e.g., session ID or token) to a known value. The attacker typically persuades the user to use a session identifier the attacker provides, often through a URL parameter or malicious script. Once the user logs in using the manipulated session identifier, the attacker can hijack the session and gain unauthorized access to the user's account and sensitive information.

Host header injection

- Host header injection occurs when an attacker manipulates the host header of an HTTP request to exploit weaknesses in a web server or application. By altering this header, which specifies the domain name of the server being accessed, attackers can trick the server into processing requests intended for other domains. This can lead to various security issues, such as unauthorized access, data leakage, cache poisoning, cross-site scripting (XSS) and server-side request forgery (SSRF).

Phishing attack susceptibility

- Phishing attacks involve sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the target's machine. Attackers may spoof email addresses to make their emails appear as though they are coming from a legitimate source, which can deceive recipients into believing the email is trustworthy.

Unencrypted communication

- Unencrypted communication refers to the transmission of data over a network or communication channel without any form of encryption applied to protect the confidentiality and integrity of the data. When data is transmitted in plain text, it is vulnerable to interception, eavesdropping and manipulation by attackers who may have access to the network or communication medium.

Malicious file upload

- The consequences of an unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, the forwarding of attacks to backend systems, client-side attacks, or simple defacement. It depends on what the application does with the uploaded file and where it is stored. The application may execute malicious code if the uploaded file has executable code in it and is used to run as part of a program. If the file is run after uploading, the server may get infected with a virus, malware or other malicious software.

Outdated and vulnerable components

- Attackers can exploit outdated and vulnerable components or software used by applications. For example, old versions of jQuery contain an XSS vulnerability that is easy to exploit.

User enumeration

- User enumeration deals with the discovery of valid usernames or user IDs through means such as predictable user IDs, differentiated error messages, insecure application programming interfaces (APIs) or directory listing vulnerabilities. Once attackers have enumerated valid usernames, they can attempt to exploit other weaknesses in the authentication process, such as weak passwords or insufficient session management controls.

Information disclosure

- Information disclosure through error messages occurs when a web application inadvertently reveals sensitive information in its error responses. For example, web server disclosures and database errors can expose database types, versions and query details, and reveal the names of hidden directories, as well as their structure and contents.

Cross-origin resource sharing (CORS)

- CORS is a security feature that web browsers use to control interactions between web applications from different origins. It allows web servers to specify which origins are permitted to access resources from the server, thereby mitigating certain types of cross-origin attacks, such as XSS and cross-site request forgery (CSRF).

Security trends observed by Minimum Baseline Security Standards (MBSS)

Minimum Baseline Security Standards (MBSS) experts audit CSP networks and original equipment manufacturer (OEM) infrastructure and are developing new auditing controls. While these controls are defined, there has been a major gap in adoption as regular changes to network elements are made as the network scales in deployment to meet demands. The baselines are beyond traditional Center for Internet Security (CIS) baselines (which are not available for most telecom network elements) and are created in house by experts to provide a preventive analysis of hardening configurations.

Key trends based on recent MBSS audits performed on telecom nodes include:

- Use of unsecured protocols
- Missing security patch updates called for by the latest releases and security advisories
- Missing two-factor authentication and strong password policies
- Missing banner for authorized user legal/ corporate obligations in command line interface (CLI) servers

About 9% of the CSP network remains noncompliant by security standards. Of this, nearly half is related to access management.

Table 3. Compliance and noncompliance among CSPs based on 3GPP and CIS benchmarks

Category	Compliant	Non-compliant
OS and platform configurations	7	1
System security architecture	11	N/A
Accountability	14	1
Access control	20	4
Business continuity plan and disaster recovery	9	N/A
Data security	N/A	N/A
Privacy	4	N/A
Legal and regulatory	15	1
Cloud computing	N/A	N/A
Mobile security	N/A	N/A
API security	N/A	N/A
Container security	N/A	N/A
Node specific	5	1
Total	**85**	**8**

Regulatory changes will drive new threat intelligence insights

New security regulations are paving the way

As incident detection and reporting regulations tighten, the mandatory disclosures will reveal new threat intelligence insights and security practices within CSPs and other critical entities in the years to come.

This transparency will reveal the full scope of cyber threats, enabling operators to anticipate and counter attacks with precision. Mandating these reports is about more than compliance. It's about empowering operators to better protect their systems and data through collective threat intelligence. Navigating country-specific regulations enhances the security posture and results in significant savings through threat intelligence.

The following are some of the key regulations that have already taken effect and will impact threat intelligence collection:

- **Telecom Security Act (TSA):** Enacted in the UK in October 2022, this law impacts telecom and service providers, hardware vendors and software developers. By March 2024, Tier 1 providers are tasked with rolling out initial measures, such as alerting affected parties of security breaches and promptly notifying the Office of Communications, the UK's communications regulator. Failing to comply could lead to fines of 10% of turnover and then £100,000 per day for continued noncompliance.
- **Telecom Security Regulations (TSR):** Part of the UK TSA framework, TSR recommends operators implement a four-tiered approach to assessing the security posture of vendor products. This involves a security declaration, spot checks on implemented security processes for specific and independently chosen product releases, lab tests, and ongoing monitoring.
- **Executive Order 14028:** Launched in May 2021 in the US, this mandate compels network providers operated by federal institutions to disclose cyber incidents and threats that may jeopardize government networks.
- **EU Cybersecurity Act (CSA):** This 2019 act introduces an EU-wide cybersecurity certification framework for information and communications technology (ICT) products, services and processes. It also establishes the European Union Agency for Cybersecurity (ENISA) as a permanent regulatory agency to support the coordination of the EU in case of a major cross-border cyberattack. Noncompliance can lead to fines of €15 million, or 2.5% of annual revenue.
- **NIS2 Directive:** Revised in 2023, this EU legislation now extends the responsibilities of telecom companies in the realm of cybersecurity. Entities must integrate cyber risk management strategies, exchange cyber threat intelligence and adhere to rigorous reporting schedules for cyber incidents, with some reports due within 24 hours. Potential penalties for noncompliance amount to up to 2% of the company's annual turnover. Entities that fall under the scope of NIS2 must comply with the regulation by April 17, 2025.

Infocomm Media Development Authority (IMDA) regulations: In Singapore, legislation establishes stringent quality of service (QoS) requirements for operators and requires the submission of regular reports on service quality. Operators found in breach of these telecom and postal QoS regulations are subject to financial penalties that can amount to as much as $50,000 for each instance of noncompliance.

Security of Critical Infrastructure Act 2022: In Australia, this legislation mandates that CSPs rigorously safeguard their telecom networks with a risk management program that is regularly reviewed and updated. Additionally, critical infrastructure providers are required to discuss any proposed changes to their telecom systems with the government. Failure to comply can lead to civil penalties.

Best regulatory practices for accelerating incident response

The stakes of regulatory noncompliance are high: fines, legal issues and reputational damage are just the tip of the iceberg. Regulatory frameworks are becoming increasingly stringent and more inclusive, especially for telecom infrastructure. Cybersecurity is a high international priority, and vendors are expected to share the measures they are implementing to deter threat actors.

These new regulations focus not only on reducing attack risks but also on enhancing the quality of incident response. With significant incidents having to be reported to authorities within 24 hours, a threat intelligence platform can lay the groundwork for effective reporting by collecting real-time intelligence during incidents, triggering automated response plans, and promptly notifying the relevant authorities.

There are two key steps CSPs can take to ensure they comply with regulations and minimize network disruptions during a cyberattack. First, CSPs should thoroughly research and understand the regulatory requirements of the country where they are based. Second, CSPs should leverage features and capabilities provided by relevant standards (e.g., 3GPP, ITU-T, ETSI, etc.) and customer reference installations.

Software supply chain security land the impact of regulations

With the scrutiny on software supply chain security intensifying, suppliers are now under pressure from an ever-growing list of regulatory demands.

Global regulations are looming, and software suppliers are now on high alert as new requirements emerge to defend against attackers targeting widely used platforms. These regulations are not just guidelines but the last line of defense to protect governments and nations from devastating software supply chain attacks.

CSPs must be ready before new rules come into effect:

- **US:** Proposed bill H.R.4611 from the Department of Homeland Security, known as the DHS Software Supply Chain Risk Management Act of 2021, aims to tighten the reins on software security. It will require US government software vendors to deliver software bills of materials, certify their vulnerability status and share plans for patching vulnerabilities as they emerge, ensuring a proactive stance on cybersecurity.
- **EU:** Legislation is currently working its way through parliament to strengthen software security. In the interim, ENISA lays out essential guidelines for software vendors to elevate their security posture, including monitoring security vulnerabilities, maintaining an inventory of assets that include patch-relevant information, and other measures.
- **Association of Southeast Asian Nations (ASEAN):** Ten members are currently in planning mode and will not reveal their comprehensive set of cybersecurity regulations until 2025.

Outpacing regulatory pressures, CSPs must enhance their security operations with continuous assessments and optimized reporting to meet industry standards.

SPECIAL EDITION
Emerging cybersecurity trends and technologies

Exploring the future of security with emerging technologies and trends Generative AI in security

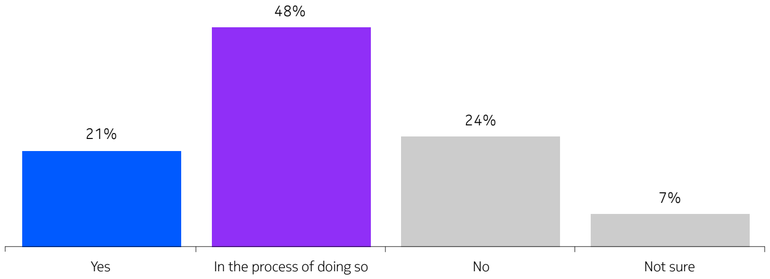
Traditional security measures are no longer sufficient in the age of advanced threats. AI has the potential to transform cybersecurity by analyzing vast datasets and identifying critical patterns. Its role in security is essential, with generative AI offering unique advantages in advanced threat detection, rapid incident response, and comprehensive security management.

According to an Omdia Industry Insight Report, when evaluating new products or services, 55% of telecom businesses consider it "very important" or "critical" that generative AI (GenAI) is part of the package. Predictably, those whose companies have or are currently incorporating GenAI into their cybersecurity strategies find the inclusion of GenAI particularly important. However, the report also found that insufficient knowledge is a barrier to GenAI adoption, which is holding some back from implementing this technology.

Figure 10. GenAI in cybersecurity adoption among CSPs

Making the move: 69% of respondents are shifting towards Gen AI in cybersecurity

One in 5 respondents (21%) report their organization have already incorporated Generative AI into their cybersecurity strategies. Another 48% report they are currently in the process of doing so.



69%

of telecoms business have incorporated, or are in the process of incorporating, Generative AI into cybersecurity

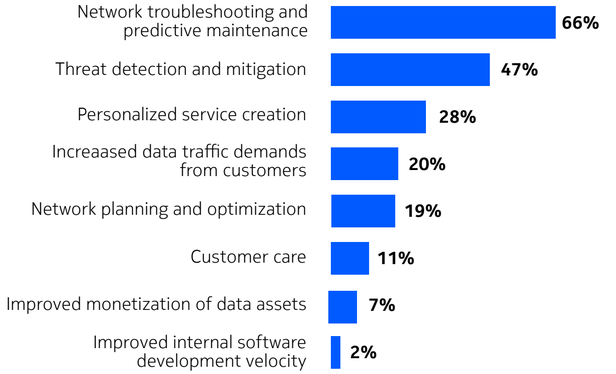
Question: Has your organization incorporated GenAI into its cybersecurity strategy?
Base: All respondents (n=126)

GSMAi's 2023 network transformation survey reveals that 66% of operators see GenAI as transformative for network troubleshooting and predictive maintenance, while 44% believe its threat detection and mitigation capabilities will have the greatest impact on their business. This highlights a clear need to efficiently identify and neutralize cyber threats with minimal human error.

Figure 11. Perceived impact of GenAI among CSPs

Use of Generative AI by operators: Where do network decision-makers see the business impact

Generative AI: Business impact
How do you believe Generative AI use cases will have the greatest impact on your business? (Top two choices – not ranked)



A more holistic approach is needed

With 18% of operators having already commercially deployed Generative AI (GenAI) solutions and 56% currently testing it, 2024 will be crucial for proving the value of GenAI's impact on telecoms.

Network troubleshooting, predictive maintenance and threat detection/mitigation topped the expected benefits of GenAI by a large margin in our network transformation survey. However, while it is natural for network decision-makers to focus on network-relaed benefits, other use cases such as personalized service creation, data monetization and customer care need to be considered. This means that network teams (who may not see the full potential of GenAI) will need to plan and coordinate with service colleagues to help materialize the GenAI opportunities.

Source: GSMA Intelligence Operators in Focus: Network Transformation Survey 2023

How threat actors are using GenAI for advanced attacks

Threat actors are increasingly using GenAI to mount sophisticated attacks faster and on a larger scale. Sophisticated phishing attacks and deepfakes using GenAI will more easily compromise telecom admins. Complex technology standards that were previously difficult to analyze and exploit are now within easy reach of even low-skilled attackers using GenAI. Coupled with the code-generation capabilities of GenAI, this will result in a new level of attacks against mission-critical telecommunication infrastructure that could previously only be achieved by nation states.

The role of GenAI in security teams

Operators are also using GenAI for defense. Within security operations centers, AI models play a pivotal role in identifying patterns that signal potential cyber threats — including malware, ransomware, and irregular network activity — that conventional detection systems might overlook.

GenAI assistants enhanced with knowledge of telecom-network architectures and telecom-specific threats can amplify the speed and quality of the security operations center response to an emergent threat. A variety of use cases can benefit, ranging from forensic analysis to guided response. This helps address the ever-growing skills gap for telecom security operations centers. GenAI assistants can also help automate the compliance reporting required by an ever-growing array of regulatory requirements.

By constantly learning from data, generative AI keeps up with new threats, reducing the chances of breaches and lessening their impact if they occur. Security teams benefit from detailed insights into how threats work. This helps them plan targeted responses and strengthen their defenses against future attacks.

Another key benefit of GenAI is automating and streamlining security operations. This frees up human resources to focus on tackling more intricate challenges and reduces the risk of human error. Additionally, security protocols can be tailored by analyzing extensive data to predict and implement the most efficient measures for specific threat scenarios.

Balancing GenAI risks and rewards

While GenAI presents inherent risks, it also offers opportunities for proactive defense and resilience-building in the face of evolving cybersecurity challenges. With responsible AI usage and a commitment to data privacy, stakeholders across the landscape can collaborate and navigate these complexities to drive positive change in cybersecurity.

Cybercriminals can use GenAI to automate the creation of sophisticated malware, evade detection systems, or launch targeted attacks with unprecedented precision. As this technology matures, hackers will increasingly exploit its capabilities for malicious purposes, and bad actors will refine their strategies to leverage this technology to their advantage. Security vendors must expedite the enhancement of their products' capabilities to effectively address emerging threats. Pairing GenAI with human security expertise can help level the playing field and strengthen defense strategies against evolving cyber threats.

The prospect of data poisoning poses an additional concern. Maliciously crafted inputs could corrupt the training process of GenAI models, leading to compromised security measures. Adopting robust security measures is essential for the safe deployment of GenAI and large language models (LLMs) in CSPs and enterprises to maximize the full capability of this emerging technology.

Key security measures that help ensure safe deployment of GenAI and LLMs include:

- Sanitizing training data to prevent leaks
- Implementing strong user authentication
- Filtering outputs to ensure content safety

The rise of post-quantum cryptography

As quantum computers evolve, they pose significant risks to existing encryption technologies, rendering them obsolete. Quantum computers have the potential to perform calculations at speeds far beyond those of classical computers. This capability could enable cybercriminals to break public key-based encryption algorithms, making possible a new wave of cyber-attacks.

One emerging threat is the "Store Now, Decrypt Later" (SNDL) attack, also known as "Harvest Now, Decrypt Later" (HNDL). In these attacks, cybercriminals steal encrypted data and store it, waiting for quantum computing capabilities to become accessible enough to decrypt it. This approach puts confidential data at significant risk of future exposure.

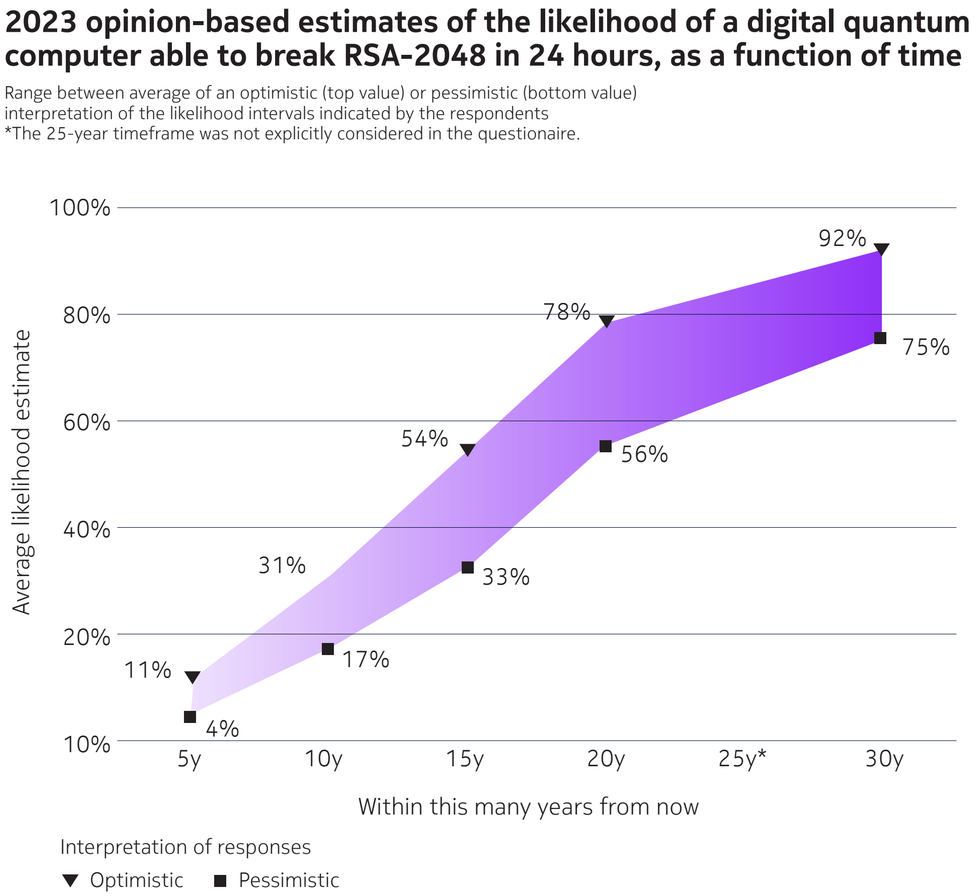
As we approach Q-Day – the day a Cryptographically Relevant Quantum Computer (CRQC) becomes a reality – critical infrastructure providers' decision-makers must urgently assess and prioritize the most vulnerable parts of their networks. Although the quantum era may seem distant, it is essential to implement countermeasures now. Even if customer data is secure today, it remains vulnerable to future unauthorized decryption.

Post-quantum cryptography (PQC) is a range of advanced asymmetric algorithms designed to withstand the power of quantum computers. The goal of PQC is to develop cryptographic frameworks that protect against both quantum and classical computing threats while ensuring smooth integration with current communication protocols and network infrastructures.

The present mode of operation may not be as secure as we believe. Many cryptographic algorithms in use today have already been deprecated due to vulnerabilities, and their lack of quantum safety is just one aspect of their inadequacy. These outdated algorithms pose significant security risks in today's cyber threat landscape, even before considering the advancements in quantum computing.

The Global Risk Institute's 2023 Quantum Threat Timeline Report underscores the growing risk of a CRQC compromising RSA-2048, a commonly used public-key cipher. According to the report, there is up to an 11% likelihood that this encryption method could be rendered ineffective within the next five years. Within 10 years, this risk triples to over 31%.

Figure 12. Estimated timeline for a CRQC capable of breaking RSA-2048



Global Risk Institute's 2023 Quantum Threat Timeline Report – Executive Summary (January 2024) By Dr. Michele Mosca, Co-Founder & CEO, evolutionQ Inc., and Dr. Marco Piani, Senior Research Analyst, evolutionQ Inc.* Global Risk Institute

In August 2024, the National Institute of Standards and Technology (NIST) announced the formal publication of its first PQC algorithms since the standardization process began in 2016.

In this first set, 3 algorithms have been standardized: one for encryption, ML-KEM, formally known as CRYSTALS-KYBER, and two for digital signatures, ML-DSA, formally known as CRYSTALS–Dilithium, and SLH-DSA, formally known as SPHINCS+.

While the standards themselves remain largely unchanged from the draft versions, NIST has made a key update by renaming the algorithms to reflect the specific versions included in the three finalized standards. Here's what's new:

- **Federal Information Processing Standard (FIPS 203)** – This algorithm is the primary standard for general encryptions. Based on the CRYSTALS-Kyber algorithm, it was renamed ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism).
- **FIPS 204** – This algorithm is the primary standard for protecting digital signatures. Based on the CRYSTALS-Dilithium algorithm, it was renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.
- **FIPS 205** – This algorithm (based on the Sphincs+ algorithm) is also designed for digital signatures but is based on a different mathematical approach and serves as a backup method in case FIPS 204 (ML-DSA) proves vulnerable.
- **FIPS 206** – Built around the FALCON, this will be finalized in late 2024 and will be renamed FN-DSA.

This is a groundbreaking development for PQC. With NIST's approval of these algorithms, they are set to become integral to industry standards (e.g., IETF, 3GPP) for internet, network, and data encryption. These PQC standards will play a crucial role in building quantum-safe networks and products.

In addition to algorithmic advancements, significant strides have been made in physics-based quantum-safe cryptography. Quantum security includes physics-based solutions like pre-shared keys with symmetric distribution and quantum-key distribution (QKD). QKD uses quantum properties to securely exchange encryption keys, ensuring that any attempt at eavesdropping alters the key and alerts the parties involved. These cutting-edge techniques offer a promising pathway to secure communications in the quantum era, complementing algorithmic solutions and enhancing overall cybersecurity resilience. By implementing a defense-in-depth approach (where additive network-layer quantum-safe cryptography complements application layer quantum-safe cryptography), we can ensure our data remains protected even if one line is breached.

How the formalized PQC algorithms are relevant to standards

The next major step in standardization is integrating PQC algorithms into public key cryptographic protocols and digital certificates like Internet Engineering Task Force (IETF), Transport Layer Security (TLS), IPSec and X.509. IETF has been addressing this, using draft NIST PQC standards from 2023, with a key challenge being the migration from traditional cryptography to PQC.

Migration to PQC cannot happen overnight, as these algorithms may still have vulnerabilities. To address this, a hybrid approach is being explored where security protocols and certificates support both traditional cryptography and PQC. This ensures continued security even if one method fails. IETF is using existing extension mechanisms rather than creating new versions. Once the IETF updates its RFCs for this hybrid approach, 3GPP will adopt these profiles.

ABI Research predicts that the PQC market will reach a valuation of $246 million by the end of 2024. As new algorithms are introduced and national guidelines are established, the demand for quantum-safe cryptography solutions is expected to soar, more than doubling to $530 million by 2028.

Why CSPs must prepare for quantum computing

Quantum computers are quickly moving from theory to reality, making it crucial time that CSPs begin the quantum security journey and prepare for HNDL attacks. Each day of delay in implementing quantum-resistant strategies could lead to future data exposure.

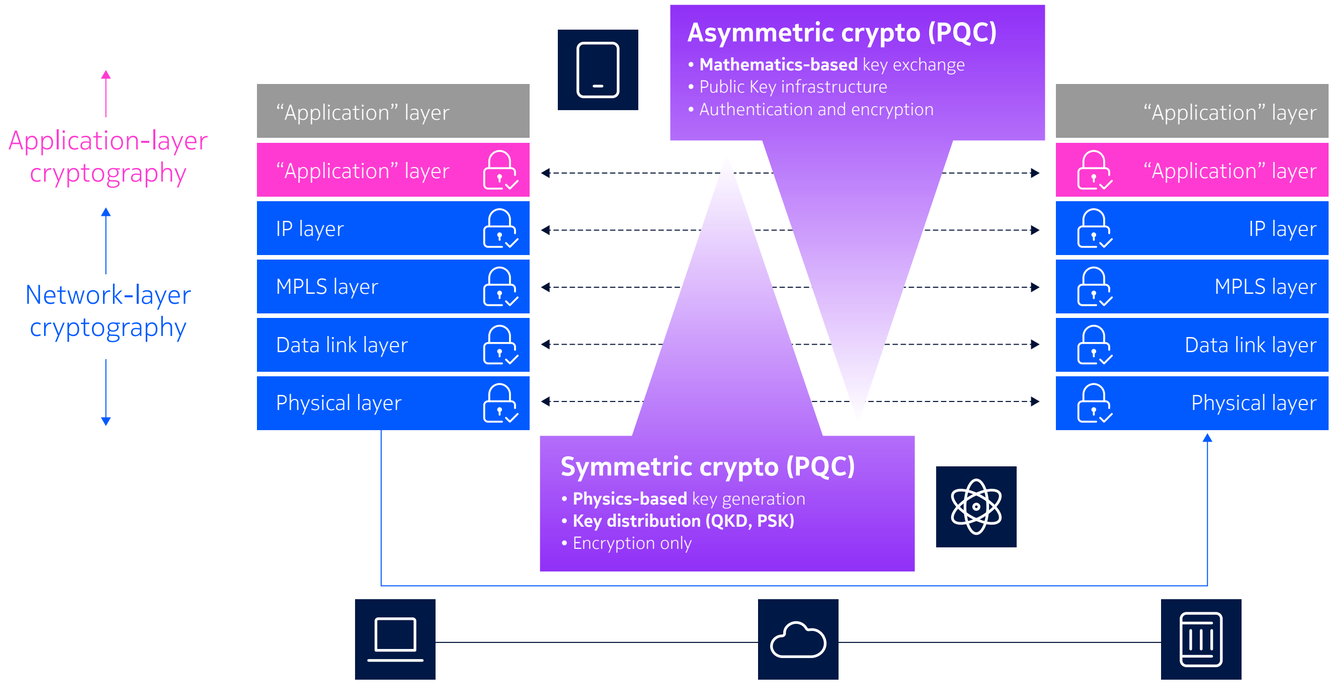
A recent Deloitte survey of over 400 professionals revealed that more than half (50.2%) believe their organizations are at risk of HNDL attacks. The message is clear: the time to act is now before the quantum threat becomes an unavoidable challenge.

Quantum threats are a concern for more than just companies using quantum computers. These threats can impact every industry and everyone they serve. As quantum technology advances, the risk of these attacks becomes increasingly real. CSPs must proactively address these risks to ensure data privacy and security for critical telecom infrastructures.

This requires a proactive approach, leveraging both classical and quantum-safe networks through private and/or managed private networks and enhancing retail connectivity services with quantum-safe virtual private networks (VPNs).

When it comes to quantum safety, there is no "one-size-fits-all" solution. It is necessary to adapt, scale, and evolve using a layered Defense-in-Depth approach to stay ahead of the threats.

Figure 13. Defense-in-depth approach



Start today with a layered approach: **1 + 1, 1 + 2, … 1 + N**

Five steps to prepare for quantum threats

Proactive steps must be taken to safeguard data and infrastructure in the face of emerging quantum threats. Timelines and guidelines set by regulators will be crucial in accelerating investments toward a quantum-safe migration, underscoring the need for telecom operators to stay ahead of regulatory and technological advancements to maintain robust security measures.

1. **Raise awareness of quantum risks within your team:** Educate your team about the potential risks posed by quantum computing and the importance of quantum-safe cryptography in mitigating these threats.
2. **Conduct comprehensive risk audits:** Conduct thorough risk assessments to identify cryptographic vulnerabilities and establish a cryptographic bill of materials (CBOM). This includes discovering cryptographic inventories and managing certificates effectively.
3. **Develop a strategic roadmap:** Outline the plan and timeline for implementing quantum-safe solutions across your organization.
4. **Implement quantum-safe solutions:** Deploy quantum-safe solutions, starting with high-risk areas, to protect sensitive data and critical infrastructure.
5. **Test and update regularly:** Continuously test and update your security measures to ensure they remain effective against evolving quantum threats. Stay proactive and agile in adapting to new challenges and advancements in quantum technology.

How CSPs are tackling cybersecurity challenges

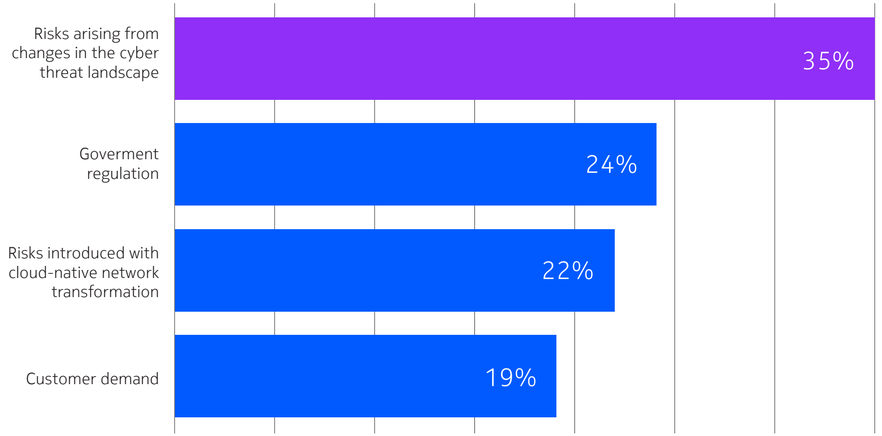
CSPs are transforming their cybersecurity strategies, and the Chief Information Security Officer (CISO) role is evolving to cover both enterprise and IT networks. Insights from the 2023 Nokia-commissioned TM Forum report, *Cybersecurity strategies: Risk management moves firmly into the telco spotlight,* include that 71% of respondents said their organization has a single CISO or CSO across both enterprise IT and network domains. For example, the CISOs of Telefónica, KPN and Telus all have responsibility across both domains today.

Top three insights and trends from the TM Forum report

Drivers behind CSP's security strategies

Understanding and addressing risks from the evolving cyber threat landscape is the most important factor in shaping security strategies for telecom operators. Government regulations play a pivotal role, as compliance is now seen as a baseline requirement rather than a competitive edge. Meeting these regulatory standards is essential for telecom operators, but according to 34% of CSP respondents, it's the proactive management of emerging threats that truly sets the stage.

Figure 14. Most important factors driving CSPs' security strategy

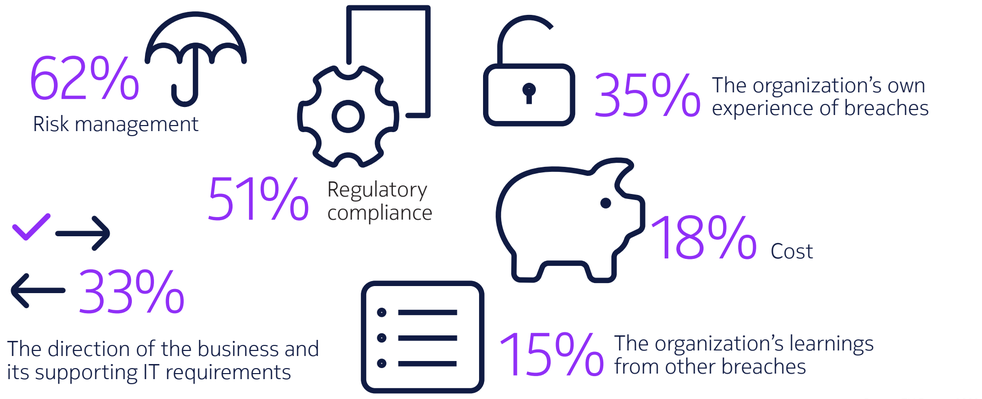


Source: TM Forum, 2023

Effective risk management shapes spending decisions

Survey findings reveal that risk management is revolutionary in how CSPs allocate their cybersecurity budgets. Over 60% of respondents ranked risk management as a top priority, surpassing the 50% who focused on regulatory compliance. This underscores the growing recognition that effectively identifying and mitigating risks is crucial for not just compliance but for robust security and operational resilience. As threats become more sophisticated and regulations tighten, prioritizing risk management allows CSPs to proactively address vulnerabilities and protect their assets.

Figure 15. Most important factors for CSPs in prioritizing security spending



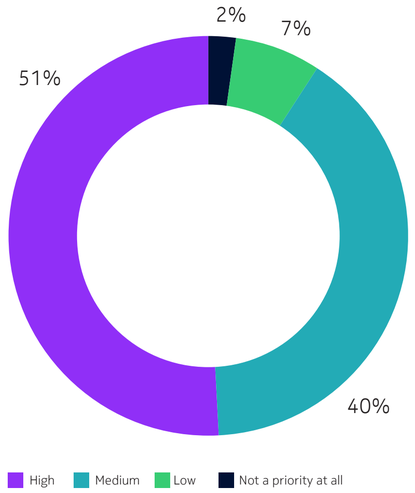
Source: TM Forum, 2023

24/7 threat monitoring is lacking

When it comes to cyber threat monitoring, detection, and response, telecom infrastructure often lags behind enterprise IT environments in terms of investment and advancement.

Threat monitoring is crucial for a resilient telecom infrastructure because it reduces insider threats and enhances data protection. By gaining full visibility into data access and usage across their networks, telecom operators can better defend against both internal and external threats. Enforcing stringent data protection policies helps prevent sensitive information from being compromised.

Figure 16. CSP investment priorities for extended detection and response (XDR) and security orchestration, automation and response (SOAR)



Source: TM Forum, 2023

Conclusion

In 2023 and 2024, the telecom sector is grappled with a diverse range of cyber threats across different regions. In North America, advanced techniques like ransomware, potentially state-sponsored, are targeted at data theft and service disruption. East Asia faces significant data leaks due to inadvertent exposures by companies themselves, while Western Europe contends with a mix of cyber espionage and financially motivated breaches, reflecting a complex threat landscape.

DDoS attacks are growing in both scale and sophistication. In 2024, 13% of carpet-bombing DDoS attacks targeted 256 or more IP addresses, with 2.8% hitting 1,024 or more. Botnets, which accounted for about 60% of DDoS traffic observed by Nokia Deepfield, continue to be a major driver. The use of AI, automation and residential proxies has become more prominent, reflecting a rise in attack sophistication.

Emerging technologies bring both opportunities and challenges. Generative AI enables faster, more sophisticated attacks, while CSPs are using the same technology to improve their response times and effectiveness. Additionally, quantum computing poses a significant risk to critical networks. ABI Research forecasts that the PQC market will be valued at $246 million by the end of 2024. This underscores the urgent need for advanced, quantum-safe solutions to protect sensitive data and infrastructure. Staying ahead of these evolving threats requires continual adaptation and strategic foresight.

Abbreviations

AppSec	Application security assessment
BSS	Business support system
CIS	Center for internet security
CRQC	Cryptographically Relevant Quantum Computer
CSP provider	Communications service
DDoS	Distributed denial-of-service
EDR	Endpoint detection and response
GTPDOOR	New telecom-oriented malware
MSS	Managed Security Services
NE	Network element
OSS	Operations support system
PAM	Privileged access management
PQC	Post-quantum cryptography
SBA	Service-based architecture
SIEM	Security information and event management
SOAR	Security orchestration, automation, and response
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TCP	Transmission control protocol
TPT	Telecom penetration testing
TLS	Transport layer security
VAPT	Vulnerability assessment and penetration testing

About Nokia's security capabilities

Nokia has a team of highly experienced analysts with extensive expertise in Threat Intelligence for the telecom industry. These analysts use the latest tactics, techniques and procedures to analyze and prevent cyber threats. We also offer a broad range of security products and services to help CSPs identify threats quickly, stop them automatically and take fast remediation actions when needed — so they can protect their networks from degradation and deliver on their service-level agreements.

Nokia Deepfield Defender uses AI-driven big data and, real-time analytics with detailed network context (Deepfield Genome®) to monitor, recognize and stop DDoS attacks. The Nokia anti-DDoS solution provides 360-degree protection against inbound (external, from the internet) and outbound (internal, from hijacked or malicious devices within a network) DDoS threats – from volumetric to application-layer attacks. With broad expertise and deep experience handling DDoS attacks, the Nokia Deepfield Emergency Response Team of security experts can help service providers minimize the effects of DDoS on their services and customers.

Nokia's Managed Security Services (MSS) global security intelligence and operations centers (SIOCs) manage the security of multiple telecom networks 24/7 to rapidly prevent and stop threats, includes Nokia MSS SIOC conduct preventative and reactive operational activities, protecting networks serving hundreds of millions of subscribers around the globe. The comprehensive views of critical security incidents, application security trends and VAPT trends are based on observations across global networks.

Nokia quantum-safe networks (QSN) employ a defense-in-depth approach to deliver quantum-safe security at multiple layers through multi-layered cryptography. Nokia QSNs can adapt to individual business and use case needs and give CSPs the confidence to securely scale their quantum deployments. Together with Nokia Bell Labs, the Nokia QSN team is shaping the future of quantum-safe network solutions.

Nokia Cybersecurity Consulting, part of Nokia's Advanced Consulting Services, brings deep 3G, 4G and 5G security expertise to help CSPs assess their security risks, processes and designs so they can secure their network and services with acceptable risks. With one of the world's only end-to-end 5G security capabilities based on in-house research and products, the team guides critical infrastructure providers to navigate the challenges and opportunities presented by global cybersecurity regulations.

Nokia NetGuard security solutions, designed with real-world applications in mind, our end-to-end security products portfolio, includes use-case driven technologies and are effective at blocking threats in Security Operations Centers such as the NetGuard XDR Security Operations suite including NetGuard Cybersecurity Dome, NetGuard Endpoint Detection and Response, NetGuard Identity Access Manager, NetGuard Audit Compliance Manager and NetGuard Certificate Manager.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214202 (September)

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.