

NOKIA

Threat
Intelligence
Report
2025



Executive summary

Threat actors have broadened their horizons and raised their attack sophistication, making telecoms a key target in 2024-2025.

Beyond ransomware and data theft, campaigns systematically targeted lawful interception systems, mobile core signaling, orchestration layers, and subscriber databases. The patterns indicate coordinated infrastructure compromise rather than isolated opportunistic attacks.

“Salt Typhoon was definitely a change of strategy. It was a big investment, impacted a lot of people and it took six to nine months.”


- CISO, Leading Communications Service Provider (CSP) in North America

This year’s report draws on Nokia’s broad security expertise: intelligence from our NetGuard and Deepfield portfolios, real-world insights from Managed Security Services operations, advanced research from Nokia Bell Labs, and expertise in cybersecurity consulting and quantum-safe networking. These are complemented by fresh quantitative and qualitative insights from a global survey of telecom security leaders conducted this summer, capturing the full scale and nature of this shift.

The impact is measurable.

This report is based on public data and provided for informational purposes only. It does not constitute legal, regulatory, or security advice, and shall not replace independent risk assessments or professional judgment.





Over **63%** of surveyed operators faced at least one “living off the land” attack last year, and **32%** saw four or more, reinforcing that stealthy techniques are now a persistent reality in telecom networks.

Human factors still drive the majority of high-cost breaches. **59%** are caused by human error or insider activity, yet fewer than one-third of decision makers view training gaps as a major challenge.

Targeted malware is growing: **55%** of operators report threats adapted to telecom infrastructure, and **45.1%** have faced custom-built toolkits.

Recovery times are slow: **63%** of major incidents take more than a week to fully recover, long enough to hurt uptime, revenue, and trust.

Hygiene gaps still open doors. **76%** of vulnerabilities stem from missing patches. Application-layer issues, including poor access controls and exploitable software flaws, remain prevalent as digital services expand.

DDoS attacks have reached new heights. Residential proxy botnets now include over 100 million compromised endpoints, enabling terabit-scale floods. **52%** of DDoS campaigns now target multiple hosts simultaneously, **58%** of them utilize multiple attack vectors, and **78%** are completed within five minutes (**37%** within two minutes).

Timelines for the deployment of quantum-safe cryptography are accelerating. While some standards have been finalized, migration is still in its infancy. Certificate validity periods were also announced to be shrinking from **398 days now to 47 days by 2029**, making manual management impossible at telecom scale.

Global cybersecurity regulation is accelerating, driving CSPs to meet tighter reporting deadlines, secure supply chains, and adopt risk frameworks.

By 2028, over half of telecom operators expect to run highly or fully autonomous SOCs. Success will depend on how well these systems are governed and secured to maintain trust while operating at full speed.

Telecom sector attack trends

Major incidents in 2024-2025

Adversaries shifted strategy. Instead of opportunistic strikes, they now execute multi-year campaigns targeting telecom infrastructure.

Incidents show persistent exploitation of vulnerabilities, compromised credentials, ransomware, and web shells, causing operational disruption and large-scale data exposure.

Table 1: Publicly reported or research-attributed incidents 2024-2025 (Based on open-source intelligence; attribution and impact details reflect public reporting as of Sept 2025.)

Date	Target(s)	Type	Actor (as reported)	Key impact (per resources)
Late 2023 - Feb 2024	Undisclosed telecom operators	Espionage	Suspected Lightbasin	GTPDoor malware reportedly used for covert data exfiltration
Sep - Oct 2024	Major telecom operators	Espionage	Salt Typhoon (Microsoft attribution)	Intrusion into lawful interception systems
Jan 2025	Regional telecom operator	Ransomware	RansomHouse (attacker-claimed)	Attacker claims unauthorized access to some customer data
Feb 2025	European telecom operator	Data breach	Unknown	Data of individuals and organizations exposed
Mar 2025	ISP (attacker-claimed)	Ransomware	Arkana Security (attacker-claimed)	Attacker claims theft of ~2.6M records; unverified
Mar 2025	Asian telecom operators	Espionage	Weaver Ant (Sygnia attribution)	Web shells deployed for persistent access
Apr 2025	Asian telecom operator	Data breach	Unknown	~26.95M USIM records exposed; SIM-cloning risk; BPFDoor on HSS
Apr 2025	African telecom group	Unauthorized access	Unknown	Unauthorized access to personal info in select markets
May 2025	Urban areas in Turkey	Telecom fraud	Local group (7 arrested)	Fake base stations used for spoofed SMS
May 2025	US regional telecom operator	Cyber incident	Unknown	Multi-day outage
May - Aug 2025	Major telecom operator (attacker-claimed)	Data breach	HellCat (attacker-claimed)	Attacker claims theft of internal files (~106 GB); validity disputed
Jun 2025	Major telecom operator (attacker-claimed)	Data breach	Dedale (attacker-claimed)	Attacker claims theft of ~22M customer records; unverified

What is known and reported can only represent the tip of the iceberg. This is especially true of state actors’ “living off the land” attacks, where adversaries use legitimate tools and deep knowledge of telecom technologies to blend in and evade detection.

Reflecting industry concerns at TM Forum DTW Ignite 2025, BT Group’s Howard Watson described the threat as “unprecedented,” noting a 160-170% increase in security events compared to the previous year.

Table 1: Publicly reported or research-attributed incidents 2024–2025 (Based on open-source intelligence; attribution and impact details reflect public reporting as of Sept 2025.)

Date	Target(s)	Type	Actor (as reported)	Key impact (per resources)
Jul 2025	European telecom operator	Unauthorized access	Unknown	Internal systems compromised; service disruptions
Jul 2025	European telecom operator	Service disruption	Unknown	Targeted cyberattack disrupted services
Aug 2025	European telecom operator	Data breach	Unknown	~6.4M accounts exposed
Aug 2025	Enterprise connectivity provider	Ransomware	WarLock (attacker-claimed)	Attacker claims support systems disrupted and ~1M documents stolen
Aug 2025	European telecom operator	Data breach	Unknown	Unauthorized access to certain data from 850,000 customer accounts
Aug 2025	Australian telecom operator	Data breach (credential theft)	Unknown	~280K records exposed
Sep 2025	Asian telecom operator	Data breach (via fake base stations)	Unknown	~19,000 users affected; IMSI leak and fraud risk
Sep 2025	Submarine cable infrastructure (regional corridor)	Service disruption	Unknown	Multiple cable faults caused rerouting and elevated latency
Sep 2025	Asian telecom operators	Initial access sale	NetworkBrokers (with Psych1c)	Access offered for sale; RCE vulnerability reportedly enables root access; unverified
Sep 2025	Regional ISP	Data breach	Sorb	Attacker claims ~209K user records exposed; unverified
Sep 2025	Multiple telecom operators	Cyber espionage	UNC1549	Devices compromised via LinkedIn lure; credential theft and data collection
Sep 2025	Unknown	Abuse of telecom systems	Unknown	Large SIM-server network discovered; capable of automating swatting attacks and disrupting emergency services

The Salt Typhoon campaign

Context

Salt Typhoon is an advanced persistent threat (APT) group linked to a large-scale cyber-espionage campaign targeting telecom infrastructure. The group exploited vulnerabilities in network operating systems, including IOS XE, to gain persistent, high-privilege access at the device level, bypassing traditional security controls. This access enabled the exfiltration of call detail records and some lawful-interception data for selected high-value targets.

Impact

A [joint Cybersecurity Advisory issued on August 27, 2025](#), confirmed that the campaign affected telecom and critical infrastructure networks in more than 80 countries. Confirmed compromises include systems supporting lawful interception, which are essential for regulated communications monitoring.

Authorities have described this as one of the most significant telecom-targeted campaigns disclosed in recent years, due to its global reach, the sensitivity of the data accessed, and the attackers' ability to maintain long-term control within core network environments.

Key facts

- **Activity window:** Public reporting from September 2024 onward; likely active since at least 2019
- **Confirmed targets:** Telecom providers and critical infrastructure operators across 80+ countries
- **Likely objectives:** Access to call detail records and some lawful-interception data for high-value targets
- **Initial access methods:** Exploitation of network infrastructure vulnerabilities, including IOS XE
- **Tactics:** GRE/IPsec tunnels, firmware/config tampering, credential theft, traffic mirroring, and “living off the land” (LOTL) tools (PsExec, Impacket)
- **Malware/tooling:** GhostSpider, Masol RAT, Demodex rootkit used for persistence and EDR evasion in telecom environments

“Salt Typhoon was the most significant cybersecurity incident we faced in the last 12 months. This was an attack against the infrastructure that was well planned and well thought through...some of the entry points were put in place years ago, just sitting and waiting for the right moment to trigger.”

- CISO, Leading CSP in North America



Recommended mitigations

- **Patch and harden infrastructure:** Apply telecom patches rapidly; audit for unauthorized accounts, tunnels, or firmware tampering
- **Strengthen access controls:** Enforce MFA, rotate privileged credentials, and isolate lawful-interception and management systems; adopt zero trust principles
- **Enhance monitoring & detection:** Deploy advanced EDR/XDR for real-time endpoint visibility across IT and OT assets; analyze OE&M and control traffic in real time; use traffic analysis, UEBA, and proactive threat hunting to detect fileless, “living off the land,” and covert attacks
- **Improve response readiness:** Establish immutable logging, maintain updated IOCs via CERTs/ISACs, and rehearse tailored incident response playbooks
- Rely on trusted technology from trusted vendors

The Typhoon cohort

Microsoft uses the “Typhoon” naming convention for multiple threat groups targeting critical infrastructure sectors. Salt Typhoon has been linked to telecom-focused intrusions, while other Typhoon groups have been reported in open-source intelligence as targeting sectors such as energy, IT supply chain, and IoT.

Group	Primary targets	Tactics	Tools / Techniques
Salt Typhoon	Telecom operators	Vulnerability exploits, backdoors	GhostSpider, Demodex
Volt Typhoon	Critical infrastructure	LOTL, credential theft	Built-in admin tools, proxies
Flax Typhoon	IoT networks, SOHO devices	IoT exploitation, botnet operations	Mirai-based malware variants
Charcoal Typhoon	Gov, education, energy	Phishing, AI-assisted social engineering	Phishing kits, LLM misuse
Salmon Typhoon	Defense, crypto tech	Espionage, custom malware	Exfiltration tools, RATs
Silk Typhoon	IT supply chain, MSPs	Supply chain compromise, zero-day exploits	Web shells, stolen API keys

Table 2: The Typhoon cohort. Based on Microsoft’s threat actor taxonomy and open-source intelligence; subject to change.



Surveyed telecom operators report their lowest readiness for nation-state attacks, **just 7% feel fully prepared.**

BPFDoor and the compromise of USIM systems

Context

South Korea's Ministry of Science and ICT confirmed a breach involving BPFDoor, a Linux backdoor known for stealth and persistence. BPFDoor uses Berkeley Packet Filter (BPF) to capture traffic at the kernel level and activates via "magic packets," bypassing firewalls without opening ports.

Key facts

- **Persistence:** Long-term presence suspected; exact start date unconfirmed
- **Scope:** MSIT confirmed compromise of USIM systems and exfiltration of ~26.96M IMSI records
- **Impact:** SIM-cloning risk prompted a nationwide SIM replacement campaign
- **Techniques:** Passive packet capture, firewall bypass, reverse shell via magic packets, process masquerading

Impact

BPFDoor enabled stealthy, kernel-level persistence, bypassing traditional defenses and leading to large-scale exposure of subscriber identifiers.

Recommended mitigations

- Treat USIM systems as Tier-0 assets; enforce isolation and immutable logging
- Apply MFA and rotate credentials across admin systems
- Patch IMS/signaling infrastructure and segment management networks
- Deploy telco-grade network function security with anomaly detection of stealth patterns
- Strengthen supply chain security for orchestration platforms

44.4% of operators rank reputational harm as the #1 breach consequence, more than financial or technical impact. Crisis communication and transparency are now core components of cybersecurity strategy.

74% of operators say they're prepared for malware/ransomware, yet **83%** of incidents cost over \$500K, half exceed \$1M.



How BPFDoor becomes a malicious implementation of BPF

01 → **02** → **03** → **04** → **05**

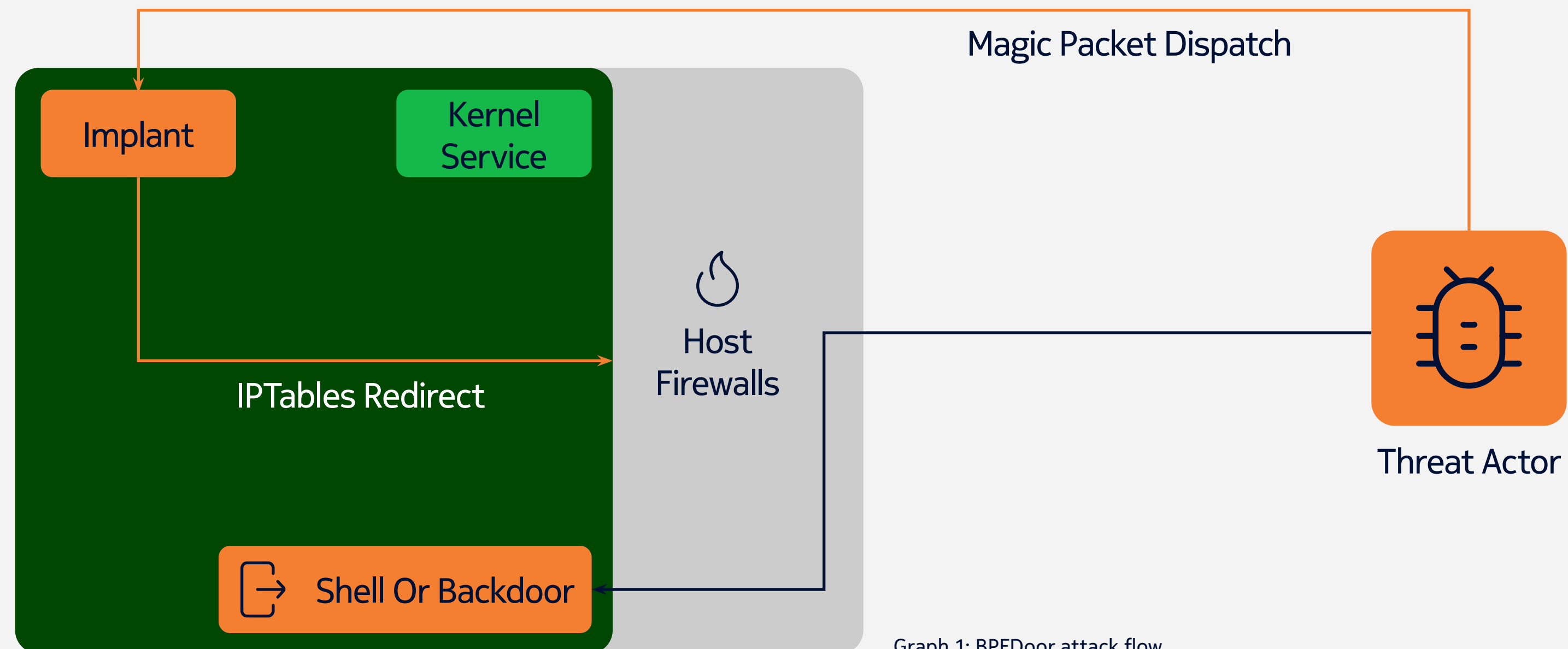
Attacker sends packets to any port with magic credentials

Implant sees packet at the same time as firewall

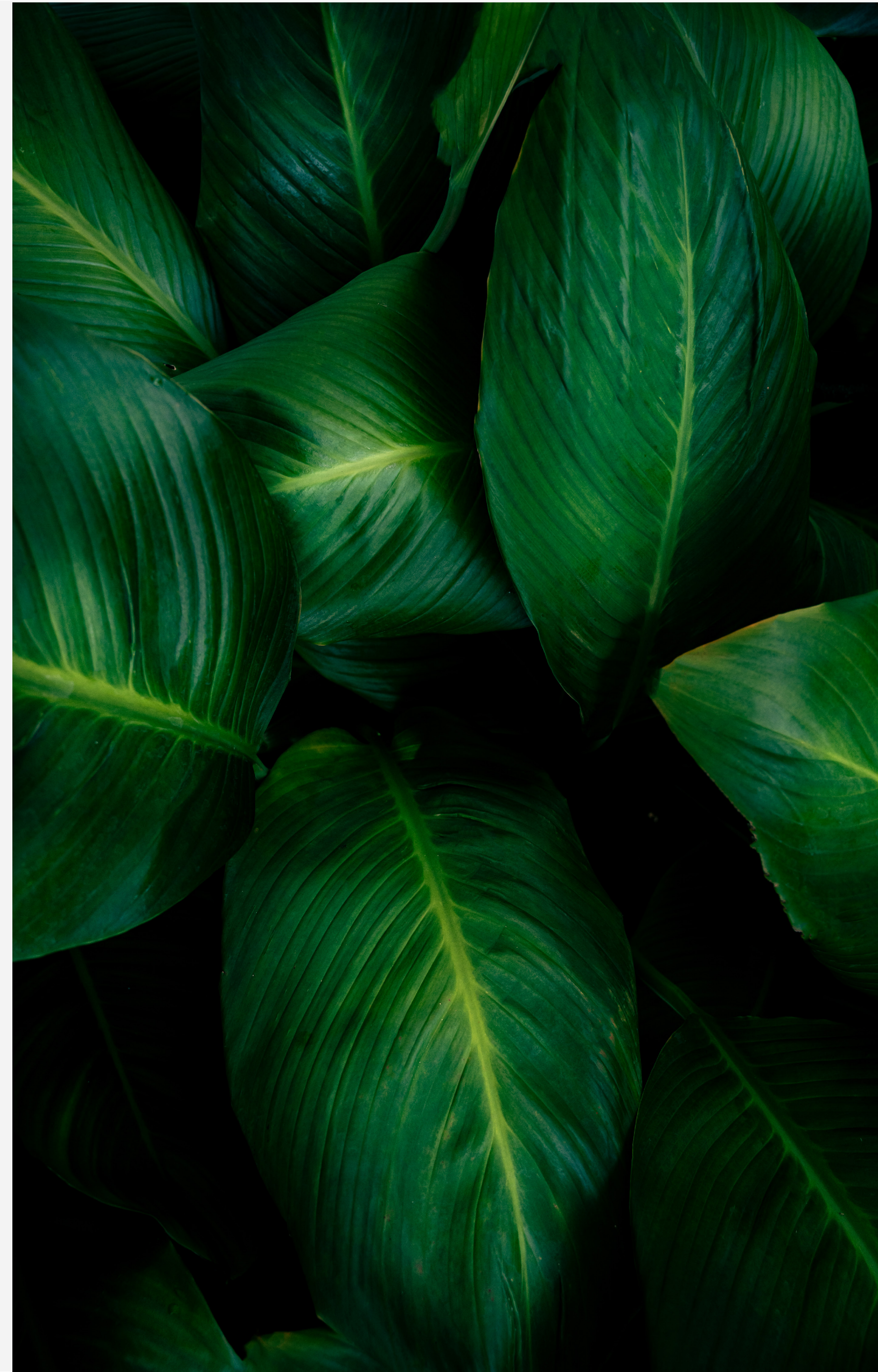
Starts a shell on TCP port

IPRouting tables changes after magic packet received

Any data exfiltration flow achievable as traffic appears to go to legit port but being routed in intended direction



Graph 1: BPFDoor attack flow



Insider and third-party risks

Context

Insider-driven incidents, malicious or accidental, are a leading cause of costly breaches. Telecom's complex supply chain amplifies the risk.

Observed trends based on global survey

- **59%** of the most impactful incidents stem from people-related causes, yet only 30% of decision makers cite inadequate staff training as a challenge
- Vendor and third-party compromise accounts for **10%** of these incidents, despite ranking among telecoms' top security concerns

Impact

Gaps in detection for insider-like behavior, including stolen credential misuse, leave operators exposed to outages, espionage, and fraud.

Example: Raccoon Stealer compromised an admin account at a major telecom operator for months, leading to Border Gateway Protocol (BGP) hijack and nationwide outage.

Real-world example: Physical access exploited in regional server breach

A senior technical leader at a major North American CSP described a breach where an individual gained physical access to a regional server room and planted a device. "The more we think about AI and sophisticated threats, the more we drop guard on traditional threats." - he said. The intrusion went undetected until a ransom demand revealed access to sensitive billing and customer data.

"Someone physically walked into a server room and planted something ... That was one of the days that I feared for my job."

While the attacker's identity wasn't confirmed, the executive noted they may have posed as or exploited contractor-level access, prompting a network-wide audit and overhaul of physical ports and access controls.

"We had to disable every unused physical port and overhaul contractor access management after the incident."

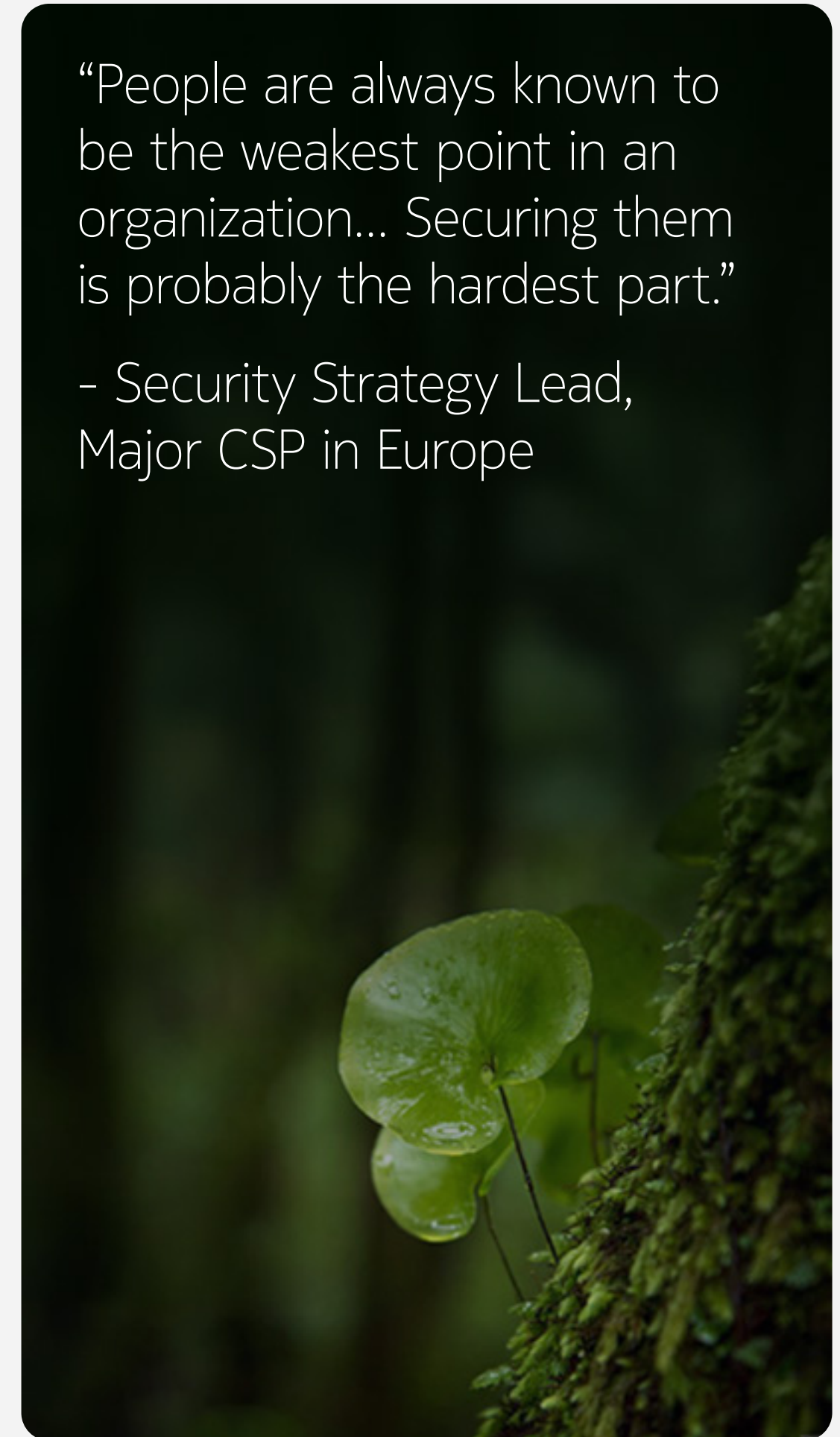
Recommended mitigations

- Deploy telecom-specific UEBA that integrates OSS/BSS, EPC, RAN, lawful interception telemetry
- Combine UEBA with PAM, EDR, and network telemetry in a central view to detect:
 - Privileged misuse - Admins or engineers accessing sensitive systems (e.g. signaling, subscriber DBs) without valid tickets
 - Privilege escalation - Unauthorized jumps in access level (e.g. OSS Tier 1 to Core Admin)
 - Credential compromise - Phished or stolen credentials used to mimic insider behavior
 - Remote access anomalies - Unusual logins to EPC, 5GC, or RAN from unexpected geos or hours
 - Data exfiltration - Stealthy transfers of subscriber data, config files, or interception logs
 - Behavioral outliers - Sudden spikes in access, external connections from management zones, or logins outside normal patterns

Learn more about [NetGuard Cybersecurity Dome](#)

"People are always known to be the weakest point in an organization... Securing them is probably the hardest part."

- Security Strategy Lead,
Major CSP in Europe





Operational security telemetry and threat patterns

Access abuse is now a systemic risk

Access misuse dominated incident logs. These were not brute-force intrusions but subtle violations of operational norms:

- Privileged commands executed outside change windows triggered outages and compliance violations
- Logins to critical devices during non-maintenance periods increased operational risk
- Unauthorized access to PII files and credential sharing exposed sensitive subscriber data
- Privilege escalation attempts often mimicked routine admin activity

Telcos must treat insider access as a dynamic threat surface. Without behavioral baselining and privilege monitoring, attackers don't need to break in, just simply log in.

Telecom interfaces show persistent architectural weaknesses

Security assessments across SS7, GTP, Diameter, and RAN interfaces revealed systemic gaps:

- Signaling firewall configurations showed incomplete packet inspection and inconsistent handling of HLR/HSS queries
- RAN backhaul lacked sufficient traffic separation and topology obfuscation, creating lateral movement opportunities
- IMSI catching remains unresolved due to legacy SIMs unable to compute SUCI
- Fake BTS attachments bypassed core network authentication in LTE/5G deployments

These are architectural blind spots. Telcos must accelerate remediation or risk systemic exploitation.

Firewall configuration gaps widen the attack surface

Firewall audits identified recurring configuration weaknesses:

- Some firewall policies included overly permissive any-to-any rules
- Logging and monitoring were disabled, leaving SOCs blind to traffic anomalies
- Weak SNMP strings and outdated firmware exposed devices to remote control and data leaks

Firewall hygiene remains an area for improvement. Telcos must enforce least privilege and visibility as non-negotiable standards.

SOC data highlights what attackers exploit once inside the perimeter, with incident volumes continuing to rise and exposing recurring patterns of access misuse, misconfigurations, and architectural gaps across telecom environments.

VAPT revealed patch neglect as a primary vulnerability source

Quarterly Vulnerability Assessment and Penetration Testing (VAPT) scans across 1000+ IPs showed:

- 76% of vulnerabilities stemmed from missing security patches
- SSL/TLS misconfigurations enabled POODLE, MITM, and DoS attacks
- Unsecured protocols like FTP and HTTP remained in active use
- “End-of-life” systems were still deployed in production environments

Patch latency is an active threat vector. Telcos must treat patching as a frontline defense, not a back-office task.

Application-layer vulnerabilities remain widespread

Application security scans revealed persistent flaws across telecom-facing platforms:

- Broken access control and IDOR enabled unauthorized data access and privilege escalation
- SQL injection and stored XSS exposed backend systems and subscriber data
- Unrestricted file uploads allowed remote code execution and malware deployment

- Outdated open-source components were still present in some environments
- CORS misconfigurations enabled unauthorized cross-origin access

Telecom web apps are not immune to commodity exploits. As operators expand digital services, application-layer security must match infrastructure-grade rigor.

Forensic investigations highlight stealthy attacker behavior

Recent forensic investigations reveal attackers increasingly use “living off the land” tactics, leveraging legitimate tools and processes already present on telecom systems to evade detection. Instead of deploying custom malware, adversaries blend into routine operations to bypass security controls. Observed techniques include:

- PowerShell scripts executed across multiple systems simultaneously
- Root-level modification of security utilities to evade detection
- Remote shell scripts used for crypto mining via SSH ports
- Executable path manipulation mimicked legitimate processes
- Data staging observed across five nodes, aggregating system and user info


These techniques show “living off the land” strategies are now matching traditional APT methods like zero-days and supply chain attacks.

MBSS audits show gaps in baseline hardening

Minimum Baseline Security Standards audits (MBSS audits) run by Nokia Managed Security Services teams across customer networks revealed:

- 35.3% of systems failed compliance checks in June 2024
- Only 25.5% of non-compliant systems were remediated by May 2025
- Common violations included:
 - Nodes not integrated with authorized servers or SNMPv3
 - Idle session and account lockout policy violations
 - HTTP and TLSv1 communications still enabled
 - Weak password complexity, age, and history enforcement

Without consistent hardening, telco infrastructure remains vulnerable to low-effort compromise and the need for frequent MBSS audits is heavily recommended.



SOC telemetry shows the threat surface is expanding from within. Misuse, misconfigurations, and legacy exposure are recurring themes. Telcos must shift from reactive defense to proactive hygiene, visibility, and forensic capability, or risk being breached by what they already own.

Global Title abuse and interconnect risks

Context

Signaling trust assumptions are breaking down. Global Title (GT) leasing, a practice where operators lease their Global Titles to third parties, masks message origins, enabling large-scale fraud, surveillance, and abuse.

Key facts

- [GT leasing banned by Ofcom \(April 2025\) for UK number ranges](#)
- Provisions: No leasing, no sub-allocations, strengthened holder controls
- Risks: Traceability gaps, weakened vetting, cross-border exposure

Impact

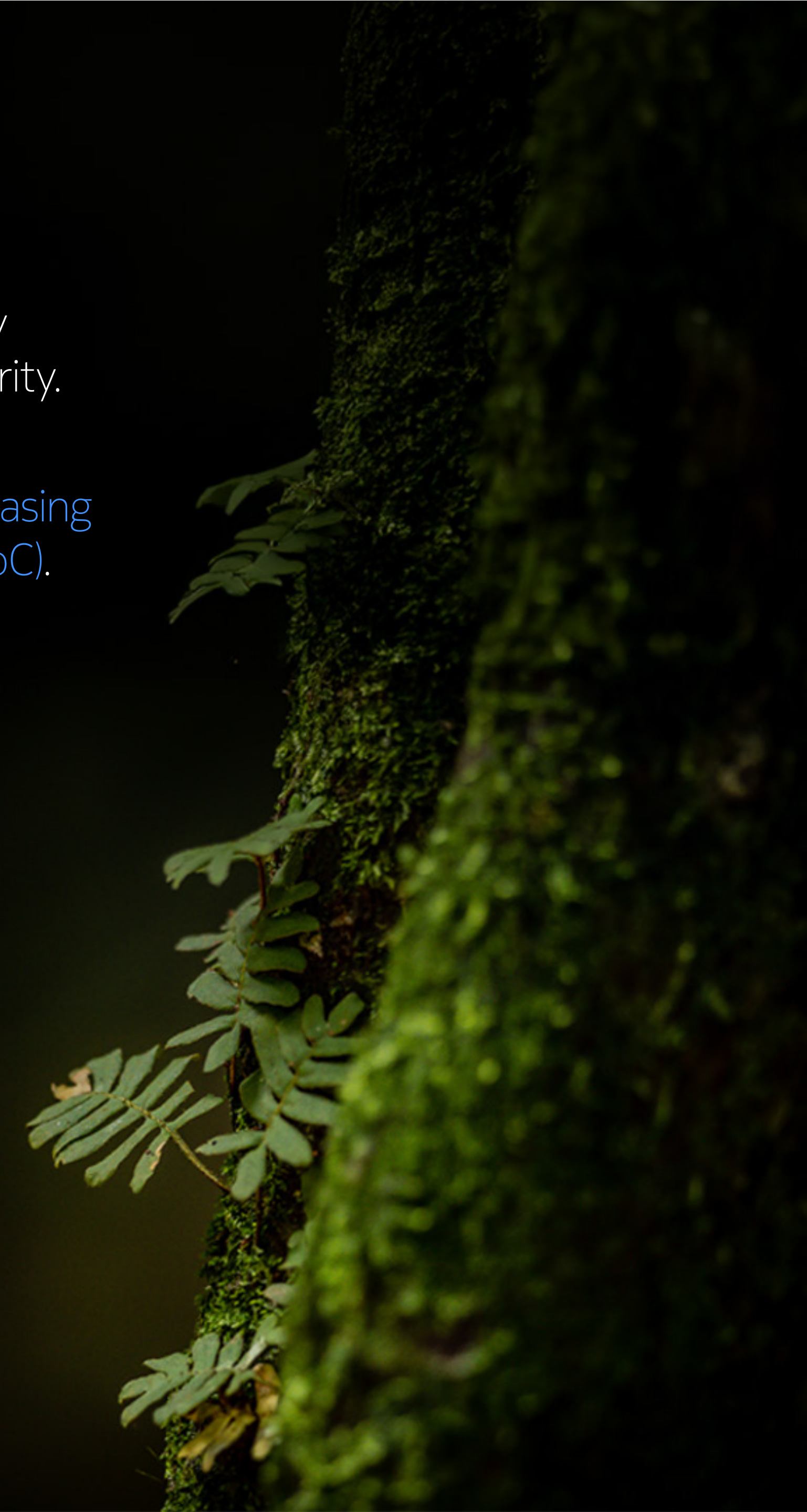
Sets a precedent likely to influence other regulators. Compromised GTs facilitate SMS OTP theft, location tracking, silent surveillance, and DoS.

Recommended mitigations

- Continuously maintaining signaling firewall configurations to keep up with
- Enforce strict GT filtering and transparent ownership
- Vet third-party access rigorously
- Monitor signaling traffic across the network for suspicious patterns, especially on roaming interconnections
- Consider blocking GTs with obvious only malicious traffic
- Conduct proactive signaling threat hunting

Ofcom's GT leasing ban is a global first; expect rising scrutiny of interconnect security.

Consider joining the [GSMA Global Title Leasing Code of Conduct \(CoC\)](#).



Offensive use of AI by threat actors

Context

AI is increasingly influencing the attack lifecycle, accelerating phases such as reconnaissance, exploitation, and persistence. Telecom networks present a broad attack surface - RAN, signaling protocols, core functions, OSS/BSS platforms etc. - all of which could be impacted by AI-enhanced techniques.

Observed trends based on global survey

- Phishing and social engineering are the leading root cause of major incidents globally, cited in **25.6%** of cases
- While credential theft drives just **10%** of major incidents globally, it spikes to 27% in APAC, often linked to SIM swap attacks that enable account takeovers

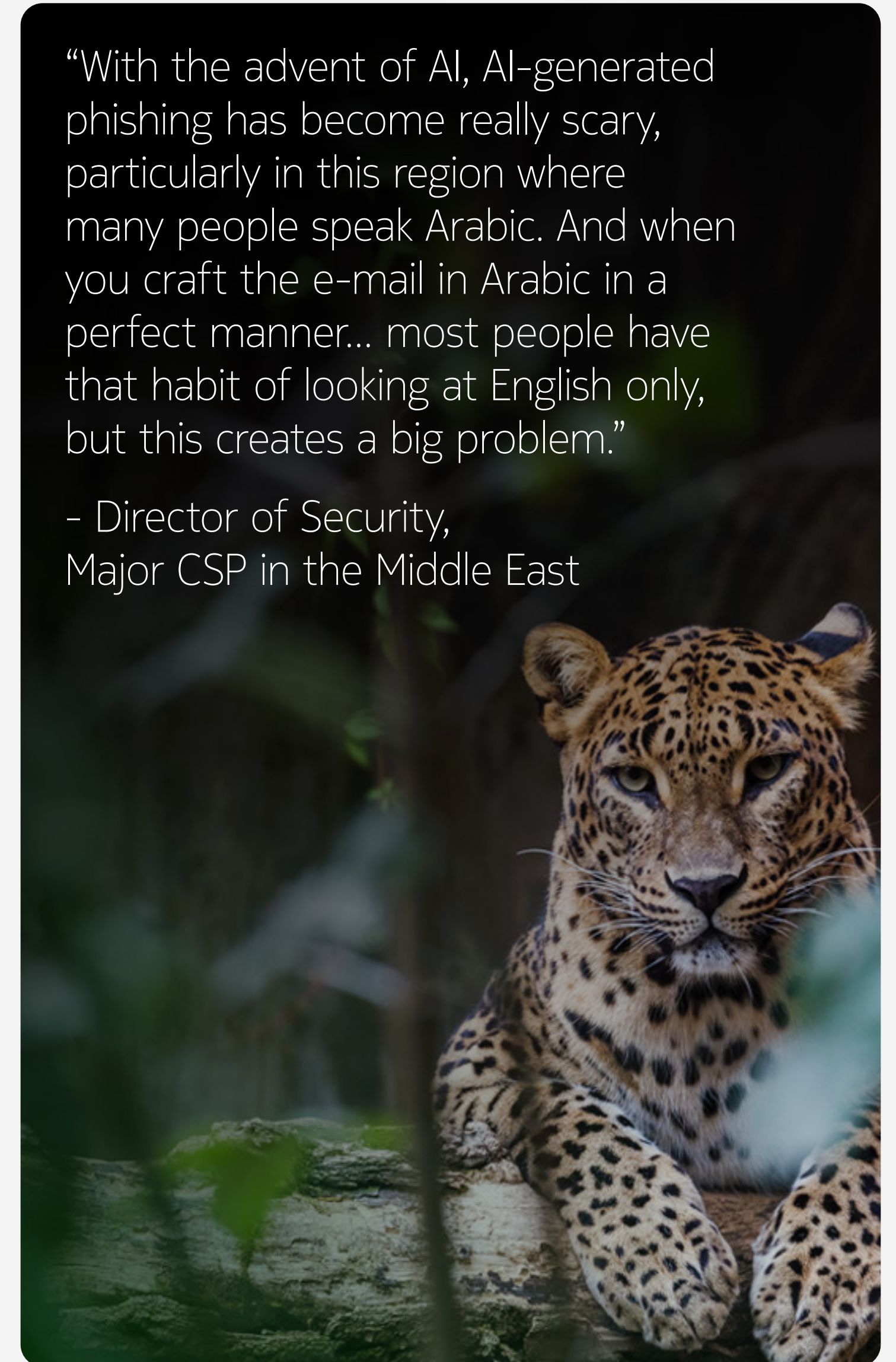
AI attack capabilities

Threat actors are already using AI for phishing and credential attacks, while additional techniques are emerging as generative AI becomes more pervasive:

- **Phishing and vishing:** AI-generated emails and voice cloning are making social engineering more convincing and scalable
- **Credential attacks:** AI models trained on breach data accelerate password guessing and credential stuffing
- **Malware evasion:** Early demonstrations show AI can support polymorphic techniques, enabling dynamic code mutation to evade detection
- **Synthetic identity fraud:** Generative models could create realistic forged documents and synthetic identities for onboarding fraud
- **Reconnaissance and exploit generation:** AI could assist in scanning telecom protocols and generating exploit scripts
- **Adaptive botnets/DDoS:** Future scenarios include reinforcement learning optimizing attack vectors and timing for multi-vector floods

“With the advent of AI, AI-generated phishing has become really scary, particularly in this region where many people speak Arabic. And when you craft the e-mail in Arabic in a perfect manner... most people have that habit of looking at English only, but this creates a big problem.”

- Director of Security,
Major CSP in the Middle East



Telecom-specific risks

While some techniques have been demonstrated in research or limited attacks, others remain emerging scenarios that operators should monitor:

- **Network-resident implants:** AI could adapt implants for vendor-specific VNFs, modify binaries post-update, and mimic legitimate signaling to reduce detection likelihood
- **Signaling exploits:** AI may assist in identifying optimal interception paths across SS7/Diameter/GTP, generating fuzzing sequences for protocol edge cases, and tuning attack parameters to evade anomaly-based detection
- **RAN and endpoint compromise:** AI could automate rogue base station configuration, optimize PCI/RSRP to attract devices, and generate polymorphic firmware variants for different RAN vendors, enabling IMSI harvesting or OTA spyware injection
- **Supply chain:** AI might support reverse-engineering of update formats, embedding malicious code that mimics legitimate functionality and passes automated acceptance tests
- **Manipulation of telecom AI:** Adversarial inputs, model extraction, and data poisoning could target operator AI systems for fraud detection, traffic optimization, or anomaly detection, leading to potential service disruption

“AI-driven bots trying to abuse signaling... it’s really challenging to counter that because we wouldn’t know whether it’s real traffic, malicious payload, or actual signaling itself.”

- Associate Director,
Access Technology Development,
Major CSP in North America



Impact

- Reduced time-to-exploit across all phases of the telecom kill chain
- Increased persistence through adaptive malware and signaling abuse
- Lower barrier to entry via AI-driven ‘cybercrime-as-a-service’ kits

Recommended mitigations

- Real-time threat detection through continuous analysis and correlation of global intelligence feeds
- Automated, adaptive response mechanisms that dynamically adjust security policies to evolving threat contexts
- Just-in-Time (JIT) Security frameworks, which apply targeted protection only when and where necessary, minimizing service disruptions
- Agentic AI architectures capable of cross-domain coordination and continuous learning to anticipate and mitigate sophisticated attacks



Threats to AI/ML models in telecom networks

Context

Telecom operators are embedding AI/ML into every layer of their networks, from OSS/BSS automation and network optimization to fraud prevention and SOC/NOC operations.

These deployments face the same classes of attacks observed in the broader AI ecosystem, with clear parallels for telecom environments:

Threat type	Definition	Industry example	Possible telco scenario
Data poisoning	Adversary injects malicious data during training to corrupt model behavior	In 2016, Microsoft's Tay chatbot was manipulated into producing offensive content (widely reported)	Customer-service bots poisoned to generate harmful or misleading responses
Model extraction	Adversary attempts to replicate or steal a proprietary model by querying it extensively or exploiting API access	Media reports in early 2025 raised concerns about model distillation risks in API-based ecosystems; no official findings announced	Theft of proprietary RIC optimization or fraud-detection models
Evasion attack – Prompt injection	Crafting malicious network traffic patterns or inputs to trick an AI algorithm into misclassifying events or generating false alerts, directly manipulating the model's decision-making pipeline	In 2024, a Canadian tribunal held Air Canada responsible for misinformation provided by its chatbot regarding refunds	Sales bots tricked into granting unauthorized credits or plan upgrades
Evasion attack – Telemetry manipulation	Tampering with network monitoring data such as packet headers, logs, or flow statistics to hide attacker presence or mislead AI-based analytics in telecom systems	Researchers have demonstrated proof-of-concept attacks in O-RAN testbeds where falsified KPIs misled ML-based traffic steering	Spectrum or resource hijacking via falsified RAN KPIs
Evasion attack – Context hijacking	Injecting or altering contextual network data to mislead AI algorithms into treating malicious activity as part of a legitimate operation, exploiting their reliance on sequence or environmental context	Security researchers disclosed scenarios where malicious inputs could influence LLM-based assistants; mitigations were deployed after disclosure	Malicious provisioning or configuration changes triggered by hidden instructions in customer data

Table 3: Attack types targeting AI/ML models in telecom networks



DDoS attack trends



In 2025, DDoS campaigns underwent some fundamental changes. Human orchestration gave way to algorithmic automation. Single-vector DDoS attacks made way to multi-vector campaigns. Attack duration shortened while impact intensity increased dramatically.

Key statistics for the past 12 months:

Terabit-scale DDoS attacks are now a **daily** reality, up from once every five days in 2024, and gigabit residential broadband connectivity is amplifying the dangers.

In September 2025, the first attack over **10 Tbps** was observed. [Learn more](#)

52% of attacks hit multiple hosts simultaneously
(carpet bombing attacks)

58% of attacks combined two or more attack vectors

78% of attacks completed within five minutes compared to **44%** in 2024
(and 37% of DDoS campaigns ended within two minutes in 2025)

If DDoS protection systems cannot detect and mitigate attacks at the network edge within a minute, they miss most contemporary DDoS attacks entirely.

Residential proxies evolved into a complex ecosystem

Residential proxy networks have evolved from tools facilitating minor fraud activities (sneaker scalping, ticket resales, price scraping) to a mainstream infrastructure risk. Based on our 18-month-long measurement campaign, we estimate that more than 100 million IPv4 endpoints covertly retransmit traffic from ordinary consumer devices; roughly a quarter appear to be in Brazil, and just over ten million in the United States.

Global infrastructure distribution

- Brazil: Dominates with approximately 25 million proxy nodes (25% of global capacity)
- United States: Maintains roughly 10 million active endpoints
- Additional concentrations: Russia, Europe, and South Africa host significant node populations

4% of all home internet connections globally are now available for exploits and malicious uses of bandwidth.

Economic control structure

The control of these endpoints is anything but decentralized: a single wholesale broker appears to channel around 70% of the global pool of IP addresses, feeding hundreds of retail-facing 'brands' that share common backend infrastructure while maintaining distinct market identities.

ResHydra dual-monetization model

Nokia Deepfield research points to a systematic exploitation pattern underlying residential proxy networks

- Phase One: Freshly compromised IP addresses are leased as high-value proxy exits, capitalizing on clean reputation scores and geographic diversity for legitimate business operations, including web scraping and content access.
- Phase Two: Once repeated abuse activities degrade IP reputation scores, the same compromised nodes transition to hyper-volumetric DDoS attack roles, transforming yesterday's premium proxy exits into today's attack infrastructure.

ResHydra flips from 'clean' proxy use to a malicious engine for generating giga-floods.

Technical capability enhancement

- Bandwidth scaling: Symmetric fiber rollouts enable gigabit-level uplink capabilities from residential nodes
- Capacity growth: 75% year-over-year increase in peak traffic generated per North American bot node
- Industrial AI integration: Industrial-scale AI scraping operations with multi-hundred-gigabit flows from LLM developers routing through residential 'supernodes' for web scraping operations
- Developers routing through residential 'supernodes' for web scraping operations
- Aggregate attack capacity: Combined bandwidth capability exceeds 100 Tbps, sufficient to strain most national internet backbones

Residential proxies now account for roughly 10% of observed DDoS traffic in hotspots such as Brazil and China, with aggregate capacity exceeding 100 Tbps - more than most national backbones can absorb.



What are residential proxies?

Residential proxies differ fundamentally from virtual private networks (VPNs). Unlike VPNs, which typically use static, data-center-based IP addresses and are predominantly used for privacy reasons, residential proxies can offer constantly rotating IP addresses derived from consumer internet services. This rotation helps attackers bypass conventional security measures.

Initially, residential proxies facilitated minor fraud activities, including sneaker scalping, ticket resales, and price scraping. Recently, however, their use has escalated significantly, especially as major AI companies began leveraging them to bypass data access restrictions on platforms like Reddit, Wikipedia, and YouTube for large-scale web crawling and data scraping.

Anatomy of a residential proxy supply chain

Despite hundreds of seemingly independent residential proxy providers, the ecosystem operates through a surprisingly concentrated control structure.

Three-layer architecture:

Farming layer (Bottom): Ordinary users are drawn into proxy networks through two distinct paths:

- Monetization apps: Users knowingly install apps that promise small financial rewards (often via cryptocurrency or PayPal) in exchange for sharing bandwidth.
- Malware-driven compromise: Up to 40% of endpoints are added without consent, through malicious SDKs bundled in apps or pre-installed on low-cost consumer electronics such as Android TV boxes.

These infections silently harvest bandwidth for resale.

Middleware layer (Consolidation): Centralized infrastructures aggregate bandwidth from millions of endpoints (both voluntary and compromised) creating a wholesale proxy market. Nokia Deepfield research identified about six major entities dominating this layer, channeling traffic to hundreds of retail-facing brands. While these brands appear diverse, most share identical backend infrastructure and differ only in branding.

Retail Layer (Consumer-facing): Between 200-300 brands offer seemingly independent residential proxy services. Despite apparent competition, most utilize the same underlying infrastructure controlled by the middleware layer.

Hyper-volumetric IoT botnet evolution

The Mirai botnet family evolved into devastating potent new variants capable of generating unprecedented attack volumes. **Eleven11bot** (RapperBot) and **AIRASHI** (Aisuru) represent the latest generation of IoT-based attack infrastructure targeting digital video recorders (DVRs), network video recorders, IP cameras, and home/business gateway devices.

Eleven11bot campaign analysis

- Discovery timeline: [First observed in late February 2025 by Nokia Deepfield Emergency Response Team \(ERT\)](#), likely indicating exploitation of a new vulnerability by RapperBot.
- Infrastructure scale: Over 30,000 compromised IoT devices with attack operations typically leveraging 3,000-5,000 active bots
- Attack capabilities: Peak attacks exceeding several hundred million packets per second

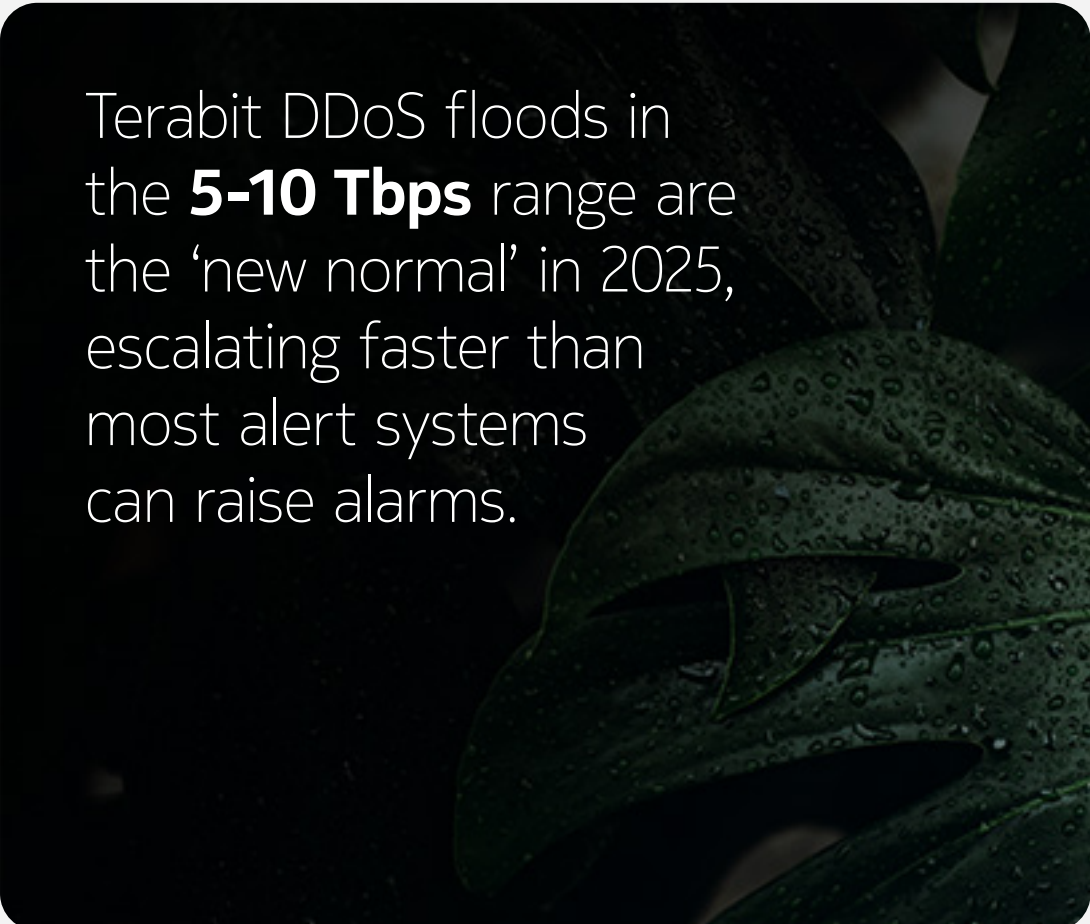
- Geographic distribution: Compromised devices span the United States, the United Kingdom, Canada, Brazil, Japan, Israel, Taiwan, and additional regions
- Operational impact: March 2025 campaign caused multiple multi-hour outages for leading global social media platform
- August 2025: US federal prosecutors make an arrest, taking down the network behind Rapper Bot, effectively shutting down this major source of DDoS. [Learn more](#)
- September 2025: After the disruption of a major botnet network, rival botnet networks compete to seize control of a large number of “freed” devices. [Learn more](#)

Technical attack characteristics

- **Volumetric capacity:** 3-6 Tbps flood generation with peak packet rates typically in the hundreds of Mpps, with occasional spikes approaching 1-2 Gpps
- **Traffic composition:** Blending classic Mirai flooding techniques with SYN-option burst attacks and carpet-bombing UDP across dozens of /24 IPv4 prefixes
- **Time to peak:** Multi-terabit attack peaks typically reached within 1-3 minutes
Operational model: Unlike proxy networks, compromised devices remain permanently armed without monetization phases, enabling attacks with minimal warning

Supply chain vulnerability factors

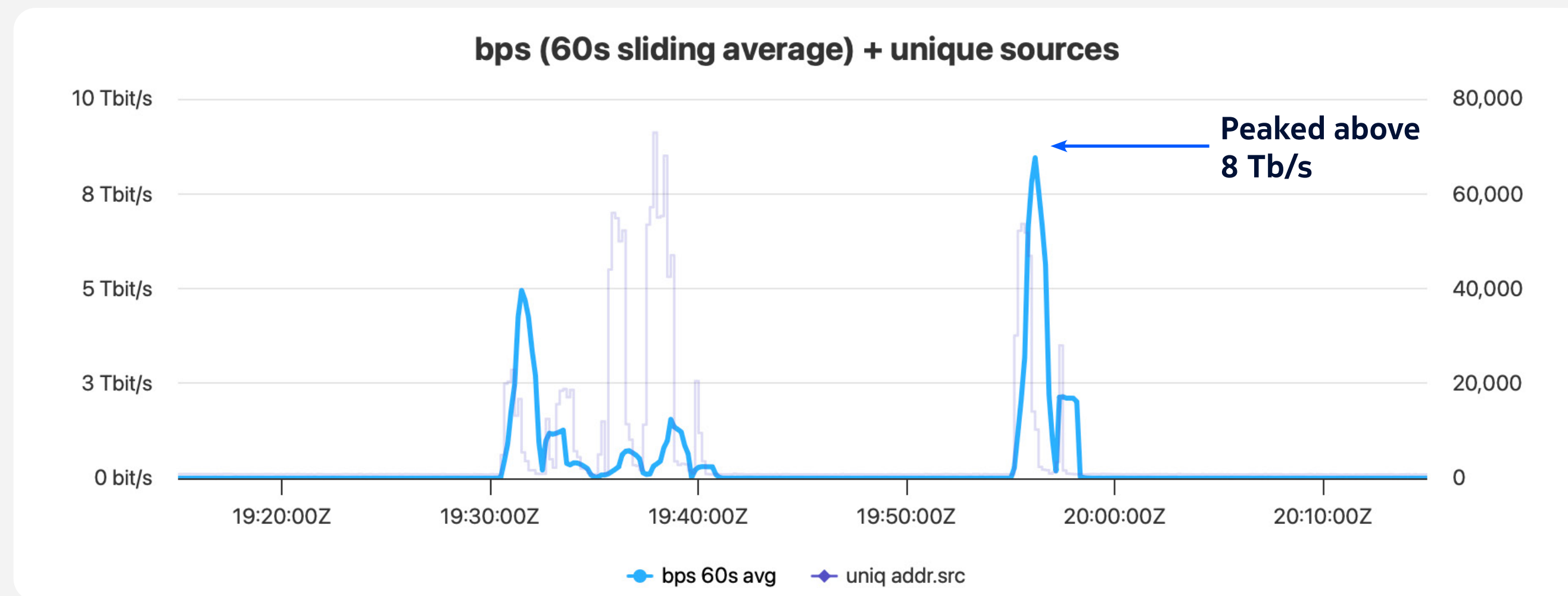
The attack infrastructure exploits fragmented IoT supply chains where responsibility for security updates evaporates across multiple stakeholders. Chipset vendors provide reference SDKs adopted wholesale by white-label Original Equipment Manufacturers. Regional brands apply cosmetic modifications while distributors disable update mechanisms to reduce support overhead.



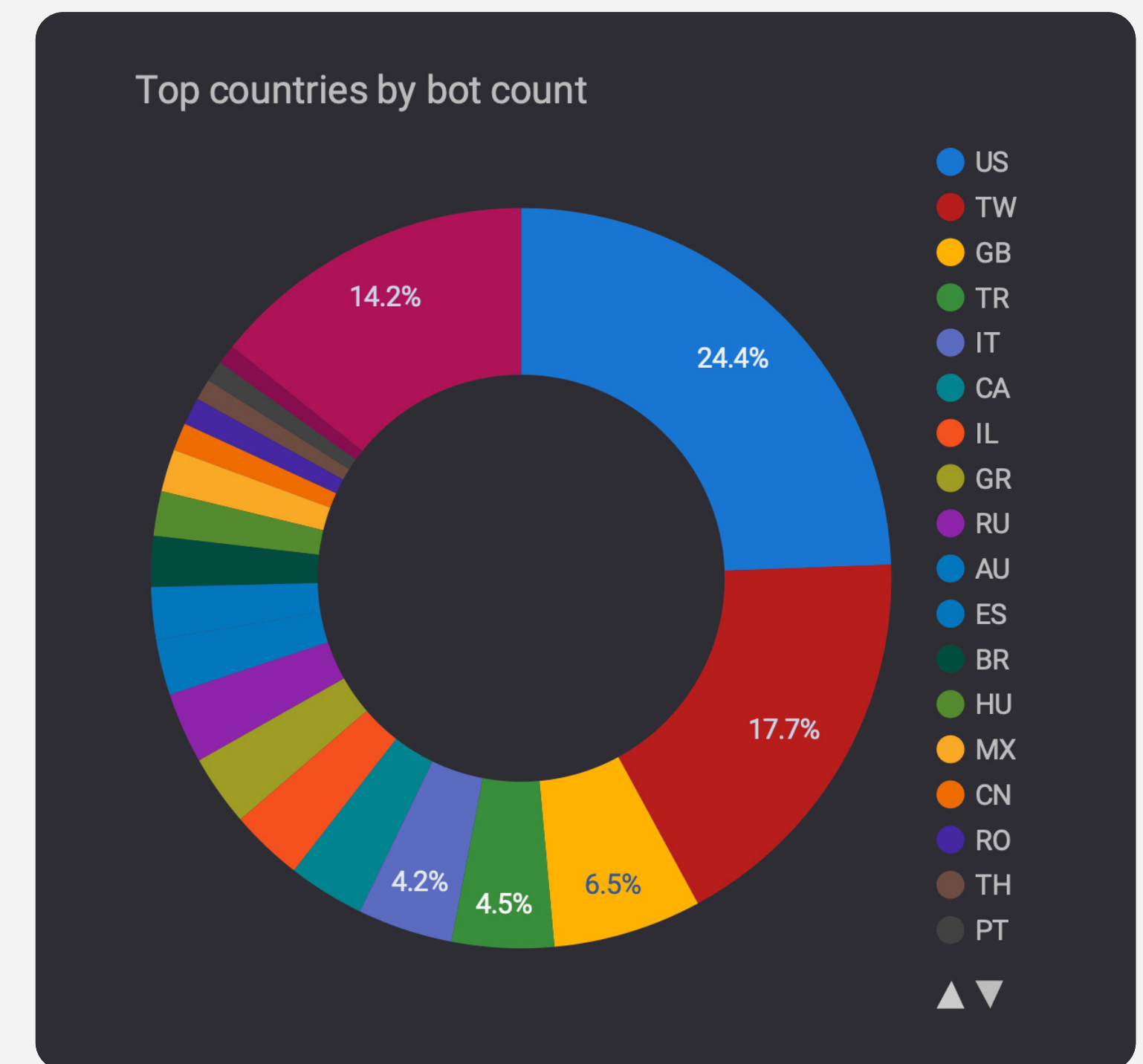
Terabit DDoS floods in the **5-10 Tbps** range are the ‘new normal’ in 2025, escalating faster than most alert systems can raise alarms.

Recent IoT DDoS botnet trends

In early September 2025 the global DDoS record climbed to ~11.5 Tbps, with Cloudflare reporting a short-lived UDP flood sourced from a combination of IoT and cloud providers, consistent with AIRASHI's recent operating profile. Following the August 6 (2025) takedown of RapperBot by the U.S. authorities, Deepfield telemetry shows ex-RapperBot devices appearing in AIRASHI attack sets within days, indicating rapid re-enlistment across botnets.



Graph 2: Two examples of short-lived DDoS attack patterns attributed to the AIRASHI botnet



Graph 3: Geographic distribution of IP addresses engaged by Eleven11, shown as a percentage by country

Algorithmic DDoS orchestration

Attackers deployed sophisticated algorithmic systems for real-time attack optimization. These systems monitor defender response patterns and adjust attack parameters dynamically, similar to high-frequency trading algorithms that respond to market conditions.

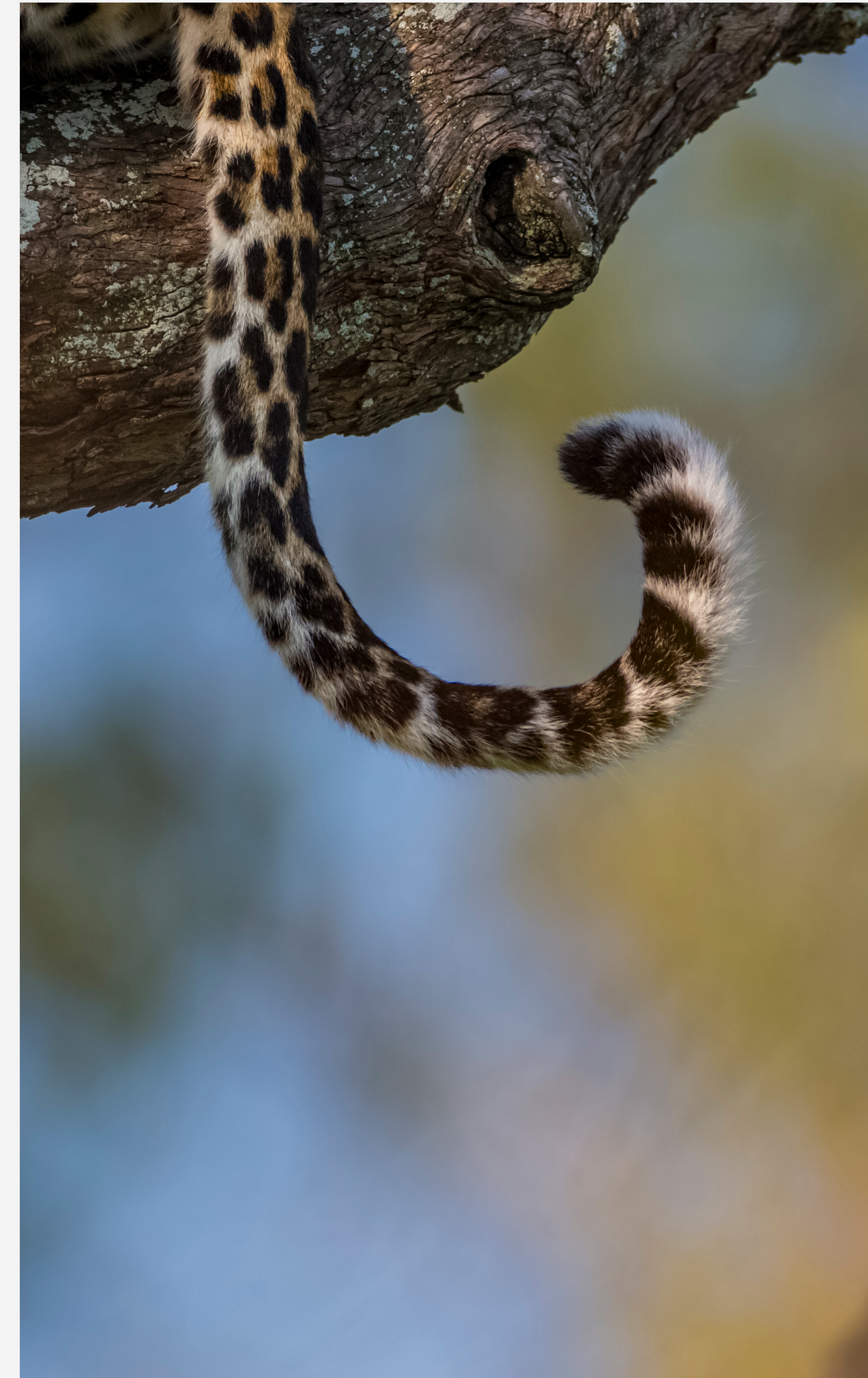
Automated campaign behavior patterns

- **Response measurement:** Systems continuously monitor defender alert thresholds and response timing
- **Vector switching:** Systematic progression through TCP carpet-bombing, UDP flooding, DNS amplification, and SYN flood attacks
- **Threshold detection:** Algorithms identify when security countermeasures are activated and adjust attack vectors accordingly
- **Adaptive escalation:** Bandwidth intensity increases with each vector transition to overwhelm progressive defensive measures
- **Reinforcement learning:** Bot networks re-queue and redirect when countermeasures are detected, threading gaps in defensive coverage

State-sponsored AI integration

Google's Threat Intelligence Group documented evidence of state-sponsored threat actors experimenting with LLMs for reconnaissance automation and attack scripting. These systems don't generate novel attack methods but accelerate the feedback loop between reconnaissance, vulnerability identification, and exploit deployment.

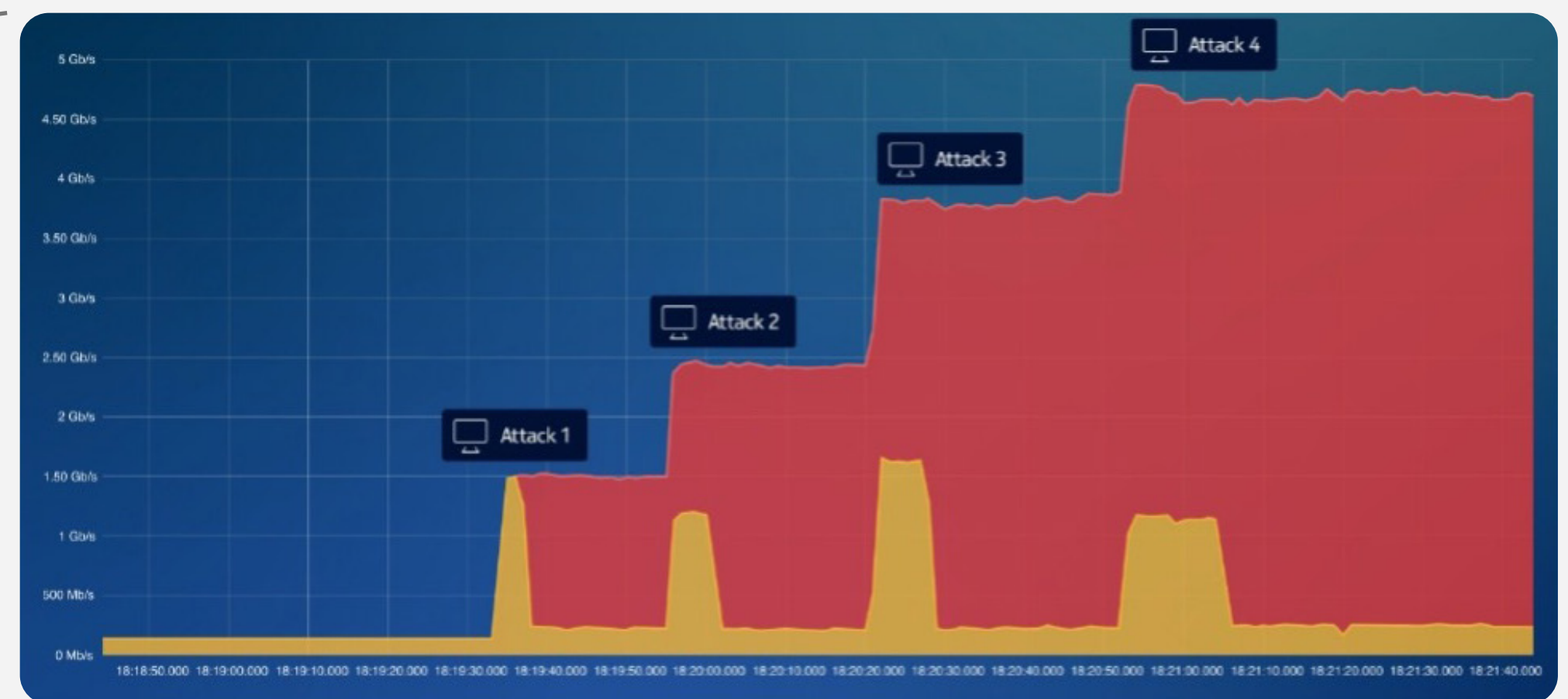
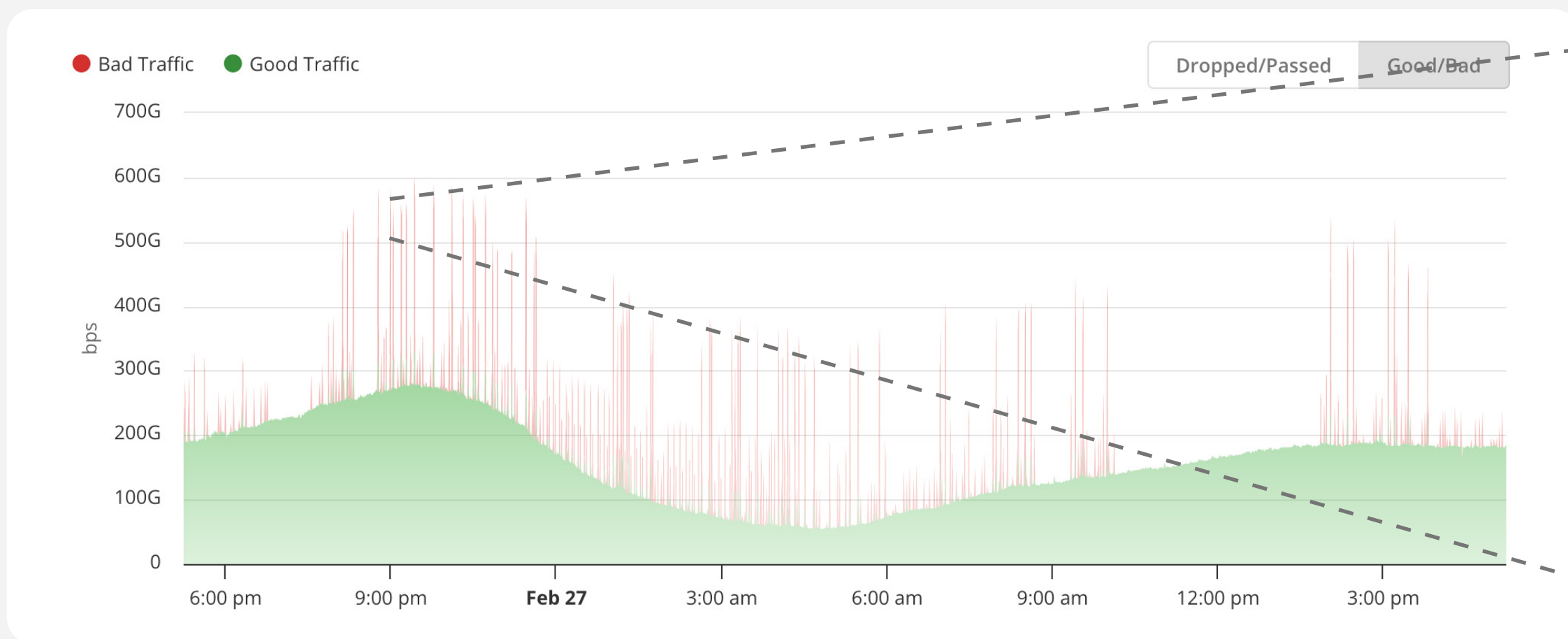
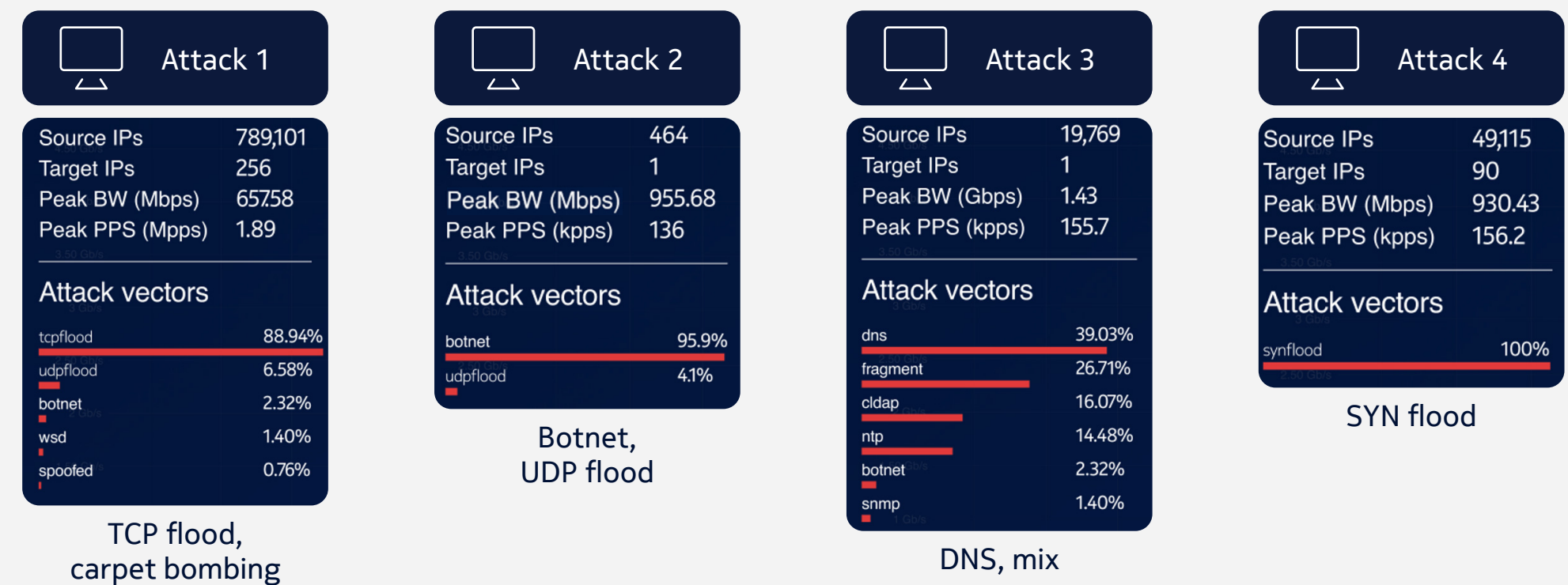
The strategic implication is that DDoS defense must achieve algorithmic response speeds matching those of automated and AI-driven attacks, or attackers will maintain a permanent tactical advantage.



Algorithmic DDoS: Automation takes the wheel

In 2025, DDoS attacks became more automated and adaptive. Attackers used AI-driven tools to launch attacks, monitor defender responses in real time, and rapidly switch tactics and vectors.

A 2025 sample from our DDoS library demonstrates this pattern: within three minutes, four distinct DDoS attacks – TCP carpet bombing, UDP flood, DNS amplification, and high-rate SYN flood – were executed in sequence. Each attack adjusted in response to observed mitigation, with bandwidth increasing at every step. This approach allowed attackers to test and adjust their methods in real time.



Graph 4: Illustration of an AI-driven cascaded DDoS attack

Shadow hacktivism: Operation Eastwood case study

[Operation Eastwood](#), an international law enforcement action in July 2025, disrupted a small hacktivist collective reportedly aligned with pro-Russian interests.

The operation included two arrests, seven additional warrants, raids on two dozen premises, and the seizure or takedown of more than 100 servers used to coordinate activity.

Authorities also issued warnings to a large number of online accounts associated with the group.

Despite these actions, the group remains active and appears capable of restoring its infrastructure.

Key observations from the takedown:

- **Minimal technical sophistication:** Tooling consisted of cut-and-paste scripts deployed on rented VPS nodes and tunneled through free VPN services. No advanced exploits or custom malware were observed.
- **Success through target selection:** Campaigns delivered “good enough” results (brief outages, headlines, propaganda screenshots) by exploiting under-resourced government websites with weak security controls.
- **Persistent motivation:** Law enforcement disrupted infrastructure, but political grievances and gamified incentives remained unchanged. Rebuilding infrastructure is trivial - just a credit-card charge away.
- **Rapid infrastructure replaceability:** Command-and-control takedowns caused temporary disruption, but new infrastructure could be spun up quickly using commercially available services.

Well-funded and well-prepared organizations can outsource DDoS scrubbing and deploy anycast to defend against attacks. Understaffed regional portals cannot do the same, so they ‘go dark’ and attackers claim victory. Reducing the impact of hacktivism requires collective action and investment in better protection of the targets that make the best headlines, not just botnet takedowns.



Real-world operational data: Bite Latvija case study

Bite Latvija, one of Latvia's leading telecommunications providers, [published comprehensive DDoS security data](#) based on telemetry supplied by [Nokia Deepfield Emergency Response Team](#). The operational dataset cuts through threat intelligence hype to reveal attack reality.

2024 operational statistics

- Total attack events: Just under **4,000 DDoS attempts** detected and blocked
- Peak attack intensity: Maximum observed attack reached **280 Gbps**
- Attack duration patterns: Average duration under **15 minutes**; the longest event lasted nearly three days
- Timing analysis: Peak frequency on **Sundays** during 16:00–20:00 hours
- Vector combination: **69%** of attacks combined multiple vectors
- Source diversity: Significant volume of **previously unseen source IP addresses**



Graph 5: 2024 DDoS security snapshot from Bite Latvia

Bite Latvija's data aligns with worldwide DDoS patterns

- Frequency over spectacle: 4,000 annual events reinforce rising attack counts. Globally, **38%** of floods never exceed 5 Gbps, **82%** stay below 50 Gbps. Disruption, not raw capacity, drives modern DDoS campaigns.
- Multi-vector dominance: 69% of attacks combined multiple methods versus **58%** globally. Automation clearly favors blend-and-pivot tactics over single-vector approaches.
- Speed over scale: Most attacks stayed under 50 Gbps, matching global findings. The decisive metric remains tempo: **37%** of floods end within two minutes, **78%** within five. Manual intervention becomes post-incident analysis.

Operational implications

DDoS capacity provides breathing room. Automation ensures continuity. When regional carriers rely on AI-driven telemetry and sub-minute edge enforcement against thousands of attacks, peer networks must also evaluate and step up their defensive capabilities.

DDoS defense evolution

The threat landscape evolves at both extremes: frequent gigabit-level targeted attacks and hyper-volumetric multi-terabit campaigns. Both can overwhelm unprepared networks.

Legacy defenses fail against modern campaigns. Static, manual approaches cannot match multi-terabit peaks and billion-packet-per-second rates. Attacks strike with minimal warning.

Effective protection requires adaptive, automated, and high-capacity mitigation integrated with real-time intelligence.

Nokia Deepfield Defender addresses this challenge by combining AI-driven big data analytics for early detection with the terabit-class filtering capabilities of next-generation routing and mitigation platforms, enabling networks to absorb and neutralize attacks across the full spectrum.

DDoS resilience depends on automation, scale, and intelligence. Networks must evolve from reactive, manual processes to proactive, self-defending architectures capable of absorbing and mitigating attacks without impacting services and customers.



A close-up photograph of various tropical leaves, including large monstera leaves with characteristic holes and long, thin palm fronds, set against a dark green background. The lighting is soft, highlighting the textures and colors of the foliage.

Zero-day attacks

Context

Zero-day exploits are increasingly tailored to telecom-native protocols, platforms, and management systems. While a zero-day attack is defined by its use of an unknown vulnerability, it is crucial to recognize that in a multi-stage attack, a zero-day exploit often serves as a tactical component. Threat actors, such as the Salt Typhoon APT group, frequently employ these exploits as an initial access vector, blending them into the early stages of a larger campaign to achieve a persistent foothold before transitioning to other tactics, techniques, and procedures (TTPs) for lateral movement and data exfiltration.

Generic detection tools miss many of these sector-specific threats. The need for telecom-aware defenses has never been greater.

Targeted threats are rising. **55%** of telecom operators surveyed report malware tailored to telecom infrastructure; **45%** have encountered custom-built toolkits.



Detection gaps and the protocol problem

Telecom networks increasingly carry not only SS7, Diameter, SIP, and 5G SBA (HTTP/2, service APIs), but also industrial/SCADA traffic that rides over operator backbones for connectivity. When these protocols sit outside the scope of generic tools, blind spots appear with critical-infrastructure implications.

Where generic IDS/IPS fall short:

- **Signature bias:** Heavy reliance on known IOCs and patterns fails against telecom-specific zero-days and vendor-specific differences.
- **Scalability issue:** Signature-based IDS cannot keep up with rule explosion, encrypted traffic, and zero-day variants (e.g., Log4Shell, ProxyShell, Mirai).
- **Opaque payloads:** Limited inspection of encrypted or proprietary control-plane exchanges.
- **“Living off the land”:** Poor detection of fileless activity that blends with legitimate administrative tools and workflows.

Critical infrastructure dependency adds urgency. Industrial systems and SCADA protocols increasingly rely on telecom networks for connectivity, yet these traffic patterns also fall outside the scope of generic security tools, creating high-stakes blind spots.

Operational reality in the SOC:

- **Unknown traffic dominates:** Significant portions of traffic do not map to known classes, driving false positives/negatives; labeling at scale is expensive, so ground truth is limited

- **Analyst overload:** Massive PCAPs and event volume make it hard to find pivot points quickly; even after filtering “known good,” the residual unknown remains large

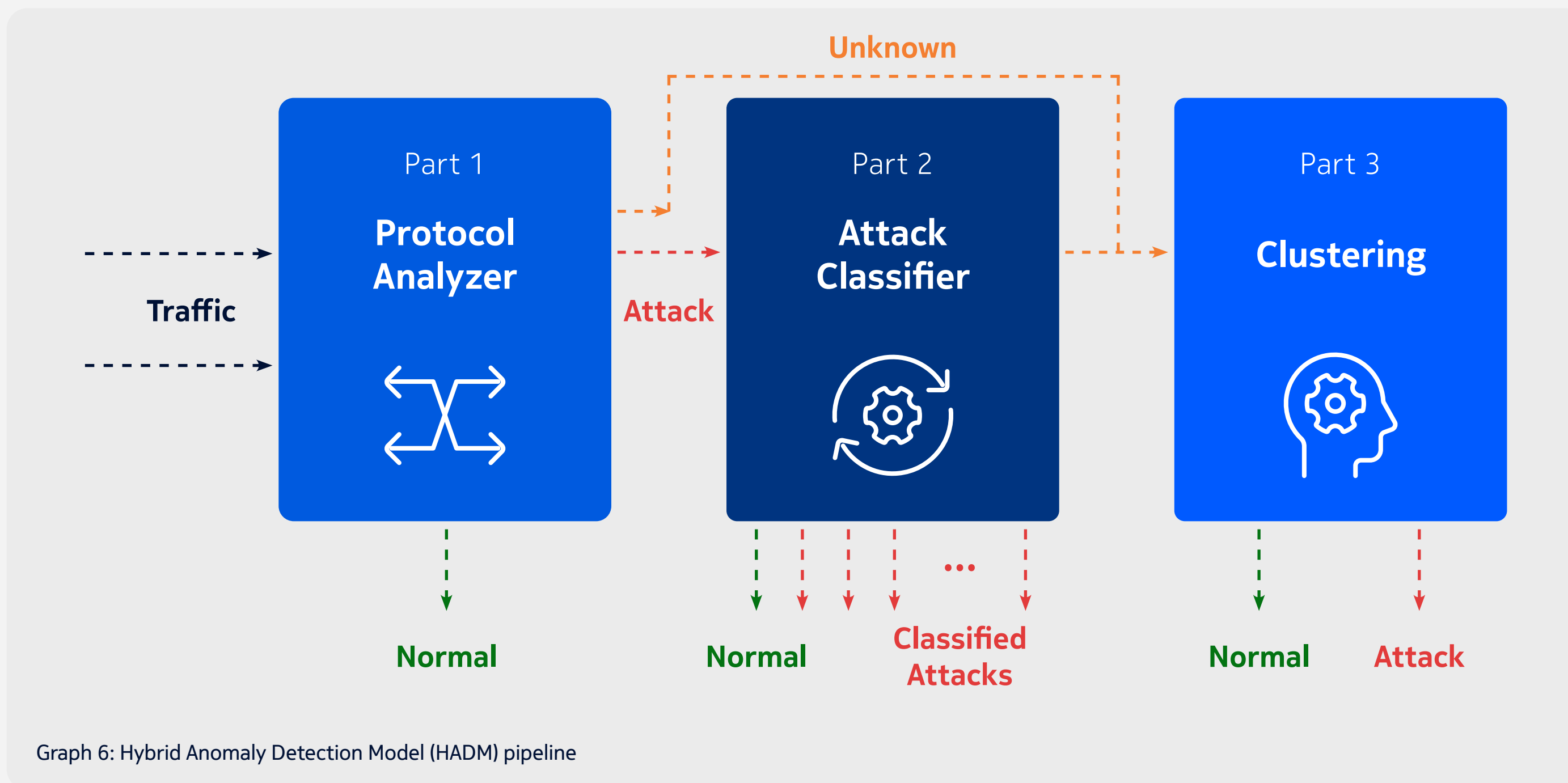
Closing this gap requires telecom-aware, behavioral analytics rather than static signatures. Models that understand signaling/context, operate near real time, and handle unknowns. Semi-/unsupervised ML (e.g., clustering) can group similar packets/flows to shrink analyst workload and surface true anomalies without exhaustive labeling, critical as industrial/SCADA traffic over telco also falls outside generic coverage.

Hybrid Anomaly Detection Model (HADM)

Nokia Bell Labs developed the Hybrid Anomaly Detection Model (HADM), an IDS approach that combines protocol-aware filtering with both supervised and unsupervised machine learning. The architecture is optimized for telecom’s distributed, latency-sensitive environments.

HADM consists of three layers:

- 1. Protocol Analysis Layer:** Filters and categorizes network traffic by protocol risk profile, directing suspicious flows for deeper inspection. Continuously updates its protocol threat knowledge from detection feedback.
- 2. Supervised ML Detection Layer:** Trained on labeled datasets of known threats, including modified or fileless variants, to detect threats resembling past attack families.
- 3. Unsupervised ML Detection Layer:** Identifies novel or unknown threats by detecting deviations from established network baselines and clustering anomalous activity patterns.



Advantages and operational relevance for telecom

- Higher detection of zero-day/novel threats in signaling and management planes
- Near real-time analysis to reduce detection delay and dwell time
- Lower false positives via behavioral and entity-baseline assessment
- Adaptive learning from live traffic, reducing manual signature churn
- Transparent/explainable outputs to accelerate investigation and compliance reporting

Optimized for telecom deployment, HADM detects campaigns like Salt Typhoon and Volt Typhoon, flagging malformed protocol commands and stealthy lateral movements even in latency-sensitive segments such as RAN, MEC nodes, and interconnect points.

[NetGuard Endpoint Detection and Response \(NEDR\)](#) delivers telco-grade security by combining host-level visibility with network traffic intelligence and HADM's advanced analytics. It continuously monitors dynamic workloads across VNFs, CNFs, and bare-metal nodes, while remaining invisible to real-time operations to ensure uninterrupted performance in mission-critical network environments.

Telco-specific TTP prevalence noticed by surveyed telecom security professionals



Case study: Threat hunting in 5G RAN to pre-empt zero-day exploits

Proactive threat hunting in an Asian telecom's 5G RAN uncovered systemic weaknesses that could have enabled zero-day exploitation. Nokia security consultants found repeated authentication failures on SSH/RDP interfaces, suspicious process execution, and critical logging gaps in Radio Access and Management Networks that limited SIEM visibility. These blind spots, if left unaddressed, could allow attackers to move laterally in the network and deploy zero-day malware, by exploiting unknown vulnerabilities without detection.

The operator's structured response, including root cause analysis, log collection and ingestion improvements, and enhanced detection use cases, demonstrates how proactive hunting mitigates zero-day risk in highly distributed 5G environments.



Operational threats and technical shifts

Context

Telecom's trust and authentication layers are undergoing major changes from 2024 to 2029. Mismanaging these shifts risks outages as severe as cyberattacks, affecting core systems, APIs, IoT, and service discovery.

Key shifts

- **TLS certificate lifespan reduction:** Certificate validity is shrinking from 398 days today to just 47 days by 2029, with intermediate steps at 200 days (2026) and 100 days (2027). Manual renewals across APIs, IoT, OSS/BSS, and embedded devices become unworkable. Without automation, expired certs will cause outages and cascading failures.
- **DNSSEC enforcement:** Regulations like NIS2 and rising DNS hijacks are driving DNSSEC adoption. DNSSEC protects critical 5G, MEC, and IMS service discovery from silent redirection or outages. Lack of DNSSEC increases regulatory risk and operational failures.
- **mTLS ECU removal:** Public CAs will stop issuing clientAuth ECU certificates by 2025, breaking mutual TLS authentication in some device onboarding and B2B integrations. Legacy systems with hidden dependencies are at high risk of unexpected failures.

Watch for

- Hidden legacy certificate dependencies
- Unsecured subdomains without DNSSEC
- Vendor gear with hard-coded trust settings

Risks and actions

Infrastructure change	Risk if unmanaged	Required telecommunications actions
TLS certificate shortening	Expired certificates causing widespread service outages	Automate certificate lifecycle via ACME protocol; integrate expiration alerts into NOC workflows
DNSSEC implementation	DNS hijacking redirecting critical network traffic	Sign all DNS zones; monitor DNSSEC validation status; include DNS security in service health monitoring
Mutual TLS evolution	Authentication failures in automated network systems	Inventory certificate dependencies; migrate to internal PKI infrastructure; update partner trust relationships

Table 4: Infrastructure changes, risks, and required actions for telcos



Certificate validity is shrinking from **398 days** today to just **47 days** by 2029. Manual renewals are no longer viable, and if operators can't adapt quickly, disruptions will hit as hard as cyberattacks.



Quantum computing threats, PQC standards and crypto agility

Quantum computing is shifting from theory to reality, creating systemic risks for today's cryptographic systems. RSA (Rivest–Shamir–Adleman) and Elliptic Curve Cryptography (ECC), which secure most digital communications, are expected to be vulnerable to quantum computing attacks.

Regulators have set clear timelines:

- The U.S. National Institute of Standards and Technology (NIST) calls for RSA and ECC deprecation by 2030 and full disallowance by 2035.
- The European Union's Network and Information Systems (NIS) Cooperation Group requires Member States to define national strategies by 2026, with high-risk sectors fully adopting Post-Quantum Cryptography (PQC) by 2030.

Key considerations

- **Immediate urgency:** According to Mosca's theorem, if the sum of data security lifetime and migration time exceeds the quantum breakthrough timeline, organizations are already exposed. This is especially critical in scenarios like:
 - Harvest-Now-Decrypt-Later: Adversaries intercept encrypted data today, waiting for quantum capabilities to decrypt it in the future.
 - Trust-Now-Forge-Later: Digital signatures on contracts and certificates could be forged retroactively, undermining long-standing trust.
- **Defense-in-depth strategy:** Multiple cryptographic layers reduce single-point failure risk. This includes:
 - Post-Quantum Cryptography (PQC): Resistant to quantum computing attacks, ideal for ephemeral

connections like TLS and SSH.

- Symmetric Key Infrastructure (SKI): Less impacted by quantum computing threats, suitable for persistent connections such as data center interconnects. Increasing key sizes mitigates Grover's algorithm.
- Quantum Key Distribution (QKD): Uses quantum mechanics for secure key exchange, immune to computational compromise.

These layers ensure that if one technique is compromised, others remain intact. Hybrid cryptography (combining classical and quantum-safe algorithms) is also gaining traction during transition phases to ensure interoperability and gradual migration.

- **Practical implementation:** Nokia [Quantum-Safe Networks](#) (QSN) adopt a defense-in-depth approach, with crypto-agility and crypto-resiliency, to deliver quantum-safe cryptography solutions today across our IP and optical portfolios, enabling organizations to adapt, scale, and evolve defenses for both short-term and long-term quantum safety.

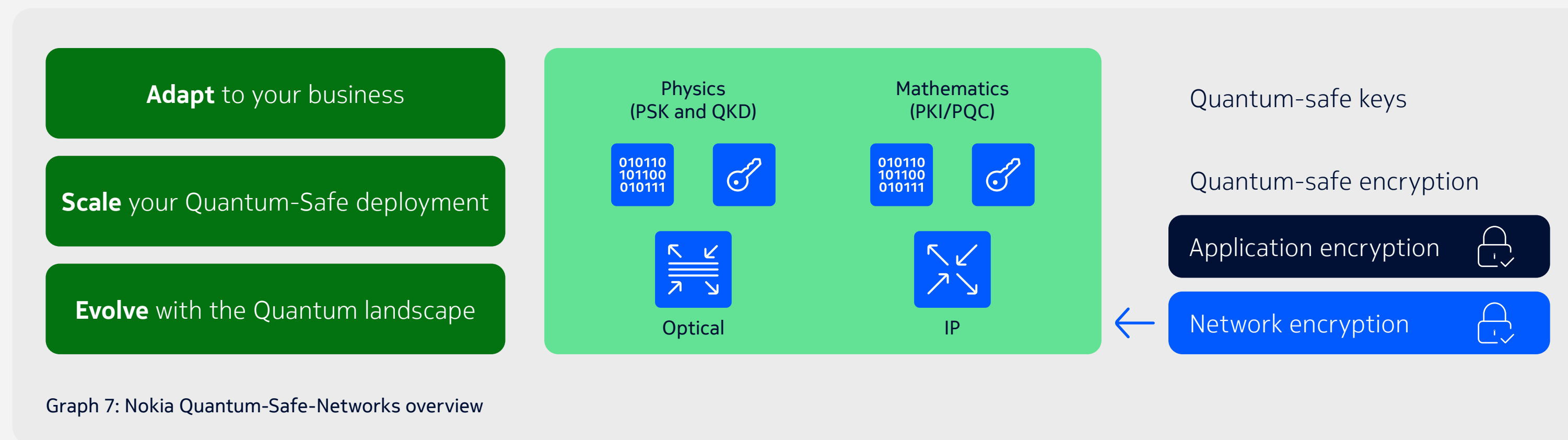
PQC standards in motion

Organizations worldwide are waking up to the reality that current cryptographic foundations won't survive post-quantum capabilities. The shift toward PQC is accelerating, moving from theory to practical transformation.

2025 status:

- ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA: Officially standardized
- FALCON (FN-DSA): Now entering public draft review, with final standardization expected by 2026–2027
- HQC: Selected in the round 4 standardization after close competition with BIKE
- Classic McEliece: Under consideration based on ISO version

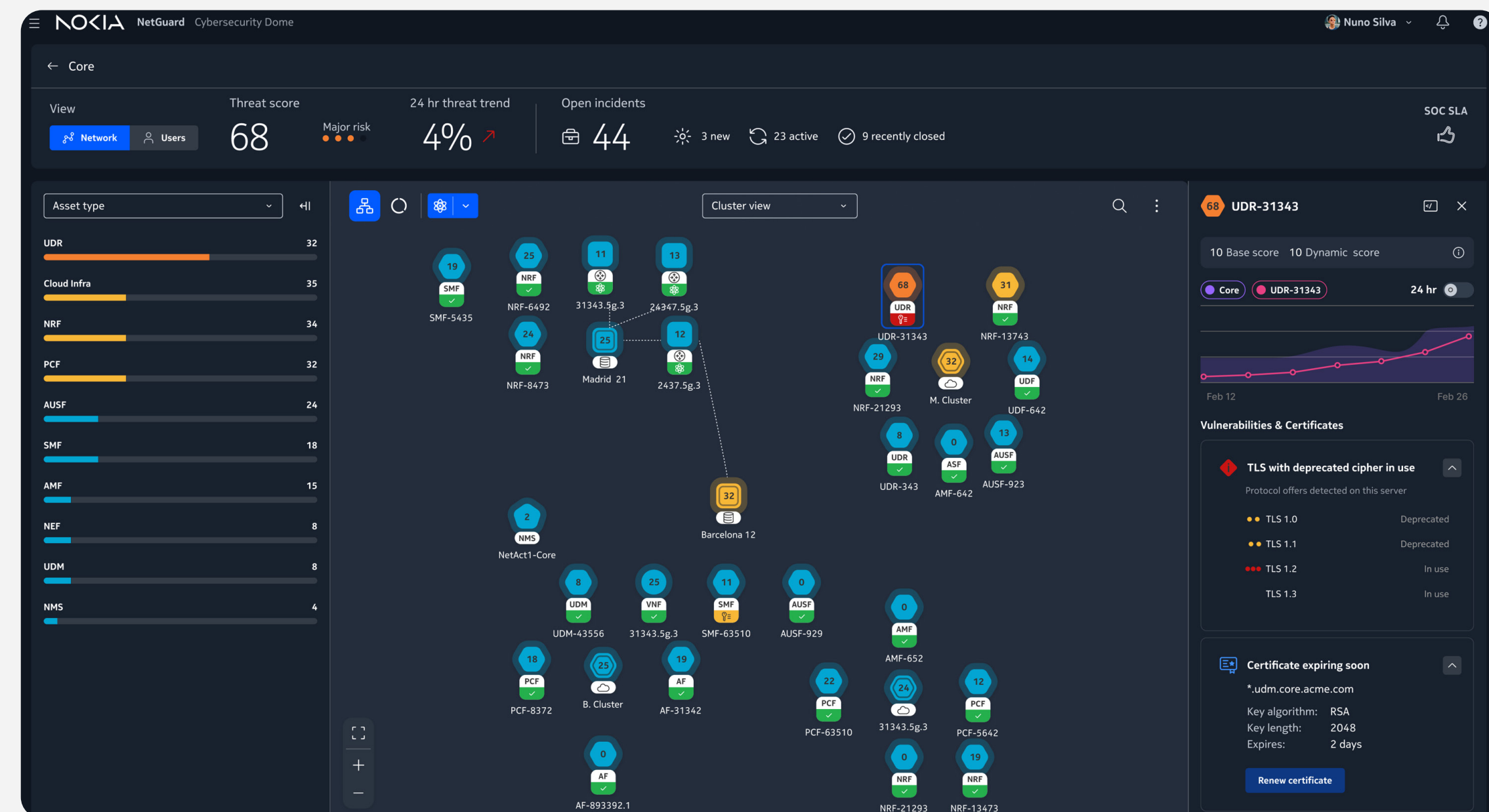
NIST is also advancing its PQC signature On-Ramp initiative to evaluate additional digital signature schemes, especially those not based on structured lattices. There are no current plans for a KEM on-ramp.



Nokia's role in building quantum-resilient infrastructure

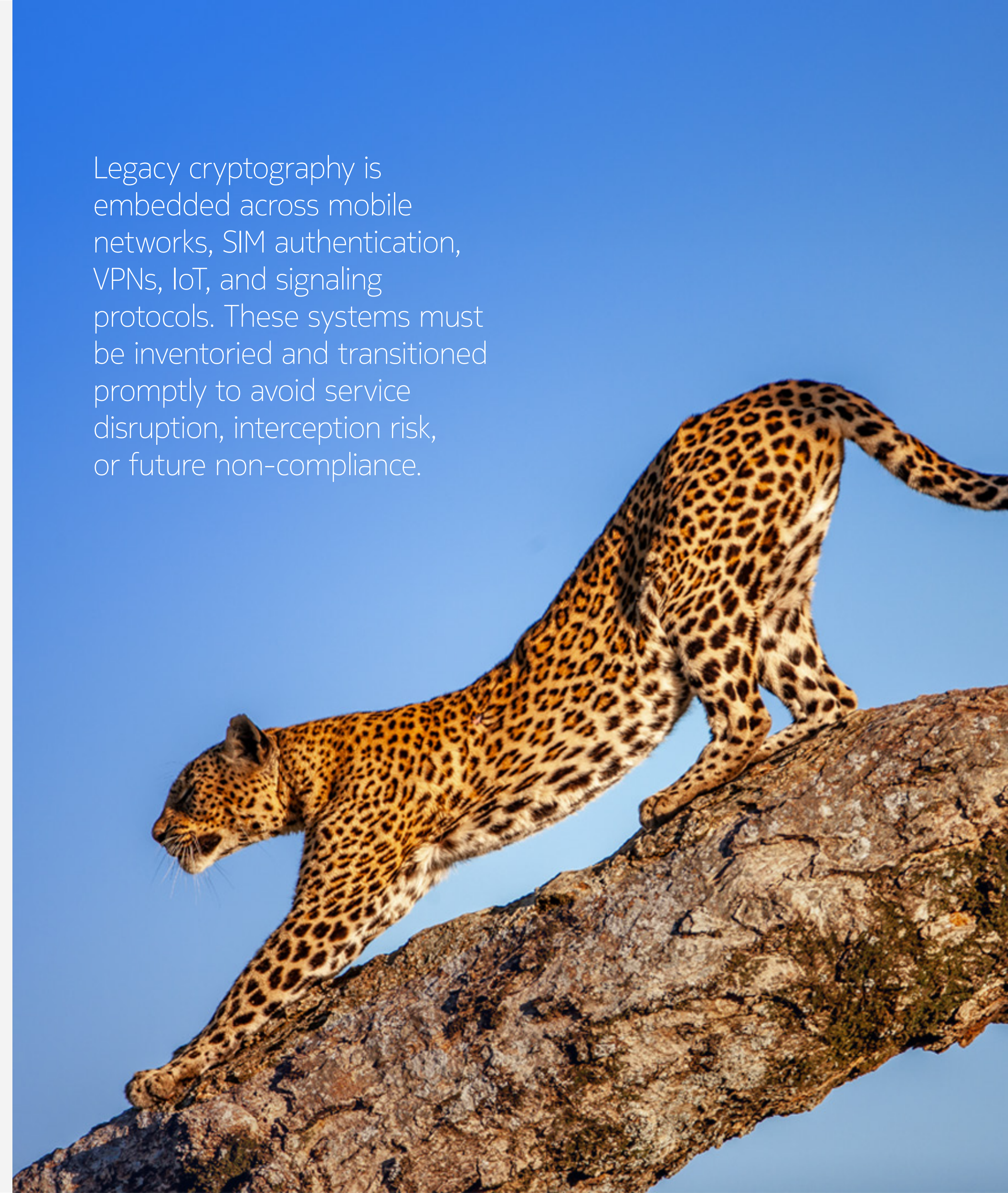
Nokia actively supports quantum-safe transformation through:

- Cryptographic inventory and risk assessment to identify vulnerable algorithms
- Phased migration plans aligned with policy timelines
- Flexible quantum-safe key distribution via manual, automated, and QKD-supported methods
- End-to-end integration across IP and optical networks for campus, data center, and cloud environments
- Extension of [NetGuard Cybersecurity Dome](#) to support quantum-safe readiness by providing visibility into cryptographic protection across network layers. This includes monitoring encryption methods, identifying legacy protocols, and combining cryptographic posture insights with threat modeling to help SOC teams prioritize quantum-safe upgrades based on risk exposure



Graph 8: NetGuard Cybersecurity Dome core network topology view

Legacy cryptography is embedded across mobile networks, SIM authentication, VPNs, IoT, and signaling protocols. These systems must be inventoried and transitioned promptly to avoid service disruption, interception risk, or future non-compliance.



Quantum safety for Intent-Based Networks

6G network evolution positions intent-based networking (IBN) as crucial for managing complexity through automation, flexibility, and intelligence. IBN translates business intents into concrete network configurations, bridging gaps between operator requirements and network delivery capabilities.

Intent-based networking represents SDN evolution allowing operators to define functional requirements while networks automatically determine achievement pathways. IBN handles initial deployment (intent fulfillment) plus continuous monitoring and adjustment (intent assurance) maintaining business objective alignment.

Security advantages of IBN

- Enables security-related intents with automated translation and assurance
- Facilitates multi-domain security through standardized interfaces
- Provides continuous monitoring and adaptation to maintain security posture
- Can be applied to security itself, allowing operators to express security-related intents
- Plays important role in securing multi-domain networking through standardized interfaces

At the same time, cryptographic agility (seamless crypto-algorithm updates without infrastructure disruption) becomes essential in the post-quantum era [2].

The intersection of IBN and cryptographic agility creates new opportunities and challenges. However, implementing agility within complex IBN frameworks requires careful security implication consideration.

Embedding quantum-resilient cryptography into IBN is the only way to ensure that automation doesn't become a single point of cryptographic failure.



Security challenges in IBNs

IBN security challenges arise from their core strengths: abstraction between network intentions and implementation methods. This creates semantic gaps between high-level intents and low-level implementation, leading to novel complex security threats. IBN security challenges divide between inherited enabling technologies (SDN, AI/ML) and inherent IBN paradigm issues.

Inherited security challenges include SDN-related threats (teleportation, DoS attacks, unauthorized control plane access) and AI/ML vulnerabilities (data poisoning, inference attacks, model stealing). Threat impact depends on unified or separate IBN and SDN controller implementations.

IBN operations span two core phases: intent fulfillment (design and deployment) and intent assurance (validation and adaptation). These categories represent concrete vulnerabilities confirmed through real-world CVEs [1]:

Fulfillment-stage threats

- T1. Faulty Compilation Pipelines: Bugs in translating intents into network instructions, silently leading to incorrect configurations (CVE-2021-38363)
- T2-T3. Composability Issues: Conflicting intents causing resource exhaustion; adversaries can infer network state through crafted intents (CVE-2022-29944)
- T4-T5. Unintended Pathways: Emergent behavior from overlapping intents allowing unauthorized flows; exploitable through link failures or spoofed sources

- T6-T7. Over-Permissive Intents: Excessive access provisions enabling lateral movement due to lack of fine-grained scoping
- T8. Cross-App Abuse: Poor application sandboxing leading to privilege escalation through indirect intent manipulation
- T9. Conflict During Deployment: Shared configurations resulting in partial overwrites or policy violations (CVE-2021-38364)

Assurance-stage threats

- T10-T11. Rule-Intent Inconsistency: Failure to adapt to network changes causing integrity violations (CVE-2022-24035)
- T12-T13. Intent State Corruption: Misleading status information leading to misconfigured networks (CVE-2022-29607)
- T14-T15. Network Degeneracy: Forwarding loops or resource exhaustion exploitable by attackers (CVE-2022-29608)
- T16-T17. Telemetry Poisoning: Compromised data skewing optimization decisions, potentially creating adversary-favorable policies

IBN presents opportunities to simplify network operations radically, but high-level abstraction reliance introduces new, non-obvious risks. These threats are grounded in actual vulnerabilities disclosed in widely used platforms. IBN represents new programmable infrastructure classes with dedicated threat models and failure modes rather than safer SDN replacements.

Research communities must prioritize intent verification frameworks, telemetry integrity validation, and formal policy composability models to make IBN truly secure by design.

For CSPs, these threats translate to real-world risks of network outages, data leaks, and SLA violations. Ensuring security at the intent layer is as critical as securing the transport layer.



Sources:

[1] J. Kim, H. Okhravi, D. Tian, and B. E. Ujcich, "Security challenges of intent-based networking," *Commun. ACM*, 2024.

[2] E. Barker et al., *Considerations for Achieving Cryptographic Agility: Strategies and Practices*, NIST CSWP 39, 2025.

Crypto-agility challenges in IBNs

In addition to the above, the introduction and evolution of post-quantum cryptography and quantum-safe connectivity in general makes crypto-agility essential in the IBNs of the post-quantum era. This new interplay may pose several challenges such as:

Lack of crypto-agility governance can undermine security of IBNs during PQC transition. The result: exposed traffic, silent downgrade attacks, or even regulatory penalties.

Inconsistent cryptographic policies	Downgrade attacks during transitions	Intent misinterpretation due to algorithm variability	Verification drift	Supply chain exposure
Threat				
Differing cryptographic policies across network components may lead to inconsistent enforcement of security, violating business intent.	An attacker exploits weak transitional cipher suites by forcing nodes to negotiate down to deprecated algorithms.	A high-level security intent (e.g., “use strong encryption”) may be interpreted differently when algorithm agility mechanisms allow dynamic algorithm changes.	Intent verification mechanisms may become outdated or blind to newly added algorithms.	Frequent updates to cryptographic libraries (for agility) increase the attack surface for compromised or malicious updates.
Impact				
Broken authentication chains, incompatible cipher suites, and service outages.	Breach of confidentiality or integrity.	Violation of compliance and security SLAs.	False positives in policy enforcement; undetected weak cryptographic usage.	Remote code execution or backdoors.



Crypto agility provides essential long-term resilience but introduces nuanced network risks where security requirements must be reliably enforced across dynamic, automated environments. Addressing this requires clear policies, strong cryptographic assurance, continuous monitoring, and secure supply chains. The role of IBN controllers should be revisited to support cryptographic agility by design.

Quantum computing introduces paradigm shifts in cybersecurity risk. The threat is real, timelines are defined, and delays carry significant consequences. Organizations must act now to secure digital foundations, protect stakeholder trust, and ensure continuity in the quantum era. Embedding quantum-safe technologies into broader resilience strategies supports risk management, regulatory compliance, and long-term digital confidence.

For IBNs, crypto agility is underexplored. At Nokia Bell Labs, we are advancing research in this area with [UNEXT](#), our intent-based, OS-like network controller designed to provide native, agile cryptographic support in tomorrow's networks.

The background of the slide is a close-up photograph of various green leaves and grasses, creating a dense, textured pattern. The colors range from dark forest green to bright, almost neon green, with some leaves showing prominent veins. The lighting is dramatic, with some areas being brightly lit while others are in deep shadow.

Current regulatory landscape

Over the past year, telecom operators have experienced an increase in cybersecurity-related regulations driven by rising cyber threats, rapid digitalization, and geopolitical instability. Four core priorities define the current regulatory landscape:

01 | Rapid incident response and disclosure mandates

02 | Software supply chain and vendor risk management

03 | Adoption of standardized cybersecurity frameworks

04 | Stronger threat intelligence sharing requirements

These developments are raising compliance costs and complexity, especially for multinational CSPs navigating inconsistent rules across jurisdictions.

“You can have your standards and controls on a piece of paper, but how well you really enforcing this in the real-world scenario, that’s the most important thing.”

- CISO, Leading CSP in North America



Key cybersecurity regulations shaping the telecom sector today

European Union (EU)

- NIS2 Directive (Deadline: October 17, 2024): Applies to CSPs and their suppliers, enforcing baseline cybersecurity requirements, mandatory incident reporting, and supply chain security controls. Non-compliance can lead to penalties of up to 2% of annual turnover. As of June 2025, only 14 EU countries (Belgium, Croatia, Cyprus, Denmark, Finland, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Romania, Slovakia and Slovenia) have adopted national legislation to transpose the directive. ENISA published implementation guidance in June 2025, offering non-binding best practices for digital infrastructure and managed service providers.
- Cyber Resilience Act (CRA): Entered into force on December 10, 2024. Reporting obligations for exploited vulnerabilities and severe incidents start September 11, 2026, and full compliance (including CE marking and conformity assessment) applies from December 11, 2027. It complements telecom regulations by requiring stronger software supply chain security, continuous monitoring, and secure lifecycle management of products with digital elements.
- Digital Operational Resilience Act (DORA): Became fully applicable on January 17, 2025 and requires ICT service providers, including CSPs supporting financial institutions, to comply with strict cybersecurity and operational resilience standards, including third-party risk management, continuous monitoring, incident reporting, and business continuity controls.
- EU Radio Equipment Directive (Delegated Act): Introduces cybersecurity and privacy requirements for certain wireless devices and is applicable from August 1, 2025.
- Upcoming Digital Networks Act (DNA): First proposal planned to be published at the end of 2025. Aims to modernize EU telecom regulation. It will focus to enhance connectivity, incentivize infrastructure investment, and strengthen network security and European technological sovereignty. Other broadly related initiatives include the planned EU Cloud and AI Infrastructure Act (2025) and the Quantum Act (2026).
- EU AI Act: Imposes strict obligations on high-risk AI systems, including those used in telecom. General-purpose AI (GPAI) obligations apply from August 2, 2025, requiring transparency, technical documentation, and systemic risk mitigation for large models.

United Kingdom

- Ofcom Global Title Leasing Ban: Ofcom has banned new Global Title leases from 22 April 2025 and requires all existing arrangements to end by 22 April 2026, with limited exceptions extended to 22 October 2026.
- Offensive Cyber Doctrine: The UK has declared its intention to retaliate against cyberattacks, highlighting growing risks in geopolitical cyber operations.

Germany

- IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) requires telecom operators to use only BSI-approved components. German authorities have announced plans to phase out untrusted 5G core components starting in 2026, with a target of full removal by 2029.

France

- LOI de Programmation Militaire and ANSSI Audits: Telcos must obtain ANSSI approval for critical infrastructure components, including 5G Core, Radio or Legal Interception features.

Spain

- Esquema de Seguridad de Redes y Servicios 5G: Spain's 5G cybersecurity framework, established by Royal Decree 443/2024 and in force since April 2024, mandates supply chain risk assessments, incident reporting, and evaluation of high-risk components in line with EU and international standards.

India

- Indian Telecom Security Assurance Requirements (ITSAR) mandates security testing and certification of telecom equipment in accredited Indian labs under the Mandatory Testing and Certification of Telecom Equipment (MTCTE) framework.

United States

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) requires reporting of substantial cyber incidents within 72 hours and ransomware payments within 24 hours.
- FCC: Expanding telecom cybersecurity oversight, including mandatory security measures and proposed risk management plans.
- Executive Orders: Recent updates mandate secure software development, post-quantum cryptography transition, and AI-driven cyber defense across federal systems.

Australia

- Cyber Security Act (2024) & Critical Infrastructure Amendments (2025) mandate ransomware payment reporting within 72 hours and risk management programs for critical telecom assets.

Regulatory fragmentation and strategic response

Telecom operators are navigating not only a growing volume of regulation but also varying requirements across jurisdictions. Even shared frameworks, such as the EU's NIS2 Directive, are implemented differently in each country, creating practical challenges for multinational compliance.

This complexity is compounded by overlapping regimes. Rules on AI, cloud, IoT, and telecom increasingly intersect, often requiring CSPs to address multiple obligations for the same system or product. Effective compliance now depends not only on understanding the rules but also on applying them consistently in dynamic, evolving environments.

How leading operators are responding:

- Investing in compliance automation and real-time regulatory mapping
- Building centralized risk and compliance functions with legal, policy, and engineering input
- Proactively engaging regulators to shape interpretations and avoid enforcement surprises

“The biggest challenge is translating the regulation to your environment... There’s no silver bullet for that. Each point of the regulation has to be translated.”

– Cybersecurity Manager,
Major CSP in Latin America

“[NIS2 and other new regulations] in the short run, it’s a headache because you think, oh, now I have to completely shake up the way that things are done... But in the long run that short-term pain is worthwhile. It can be a wake-up call for organizations. You think, why did we never do that before?”

– Security Strategy Lead,
Major CSP in Europe

The geopolitical context and its impact on telecom security

The international security environment is characterized by a period of “radical uncertainty,” marked by assertive actions from authoritarian regimes, the erosion of established international norms, and the increasing prevalence of cyber-enabled conflict. These dynamics significantly affect telecommunications security by amplifying risks to critical infrastructure, supply chains, and the resilience of cross-border networks.

Key observations:

- The UK National Security Strategy 2025 highlights intensifying great-power competition and hybrid threats, and sets out a goal of raising national security spending to 5% of GDP by 2035
- At the July 2025 NATO Summit, Allies agreed raising defense spending toward 5% of GDP by 2035, including greater emphasis on protection of critical infrastructure
- Government and industry advisories continue to report state-sponsored cyber activity directed at the communications and telecom sectors worldwide



“People’s Republic of China (PRC) state-sponsored cyber threat actors are targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks.”

- Joint Cybersecurity Advisory from western security services¹



¹ Australia, Czech Republic, Finland, France, Germany, Italy, Japan, New Zealand, Poland, UK, USA

Regional developments (illustrative examples)

- Iran and Israel/US tensions: In Q2 2025, brief escalations between Iran and Israel (with U.S. involvement) were accompanied by government alerts about potential retaliatory cyber activity against critical infrastructure. While no confirmed widespread disruption to CSPs materialized, heightened readiness persisted across several nations.
- UK offensive cyber policy: UK officials have publicly committed to maintaining offensive cyber capabilities as a deterrent, with the National Cyber Force and Cyber & Electromagnetic Command named as responsible entities.
- India’s expanding role: India is continuing to develop mandatory domestic testing regimes for telecom equipment and digital infrastructure. At the same time, international reports have raised concerns over hack-for-hire operations linked to actors in India, leading to greater monitoring and cooperation with allied nations.
- 5G security and High-Risk Vendors (HRVs): Security concerns around certain vendors remain central to EU, UK, and US policies. The European Commission has signaled it is preparing binding measures to restrict HRVs in critical infrastructure.
- EU initiatives in 2025 include funding large-scale “AI factories” (compute and data infrastructure positioned to accelerate trustworthy AI adoption) which underscore the link between secure digital infrastructure and competitiveness.
- The awareness of economic losses due to theft, industrial espionage or sabotage is growing. German companies lost almost 15 Billion Euro in 2024 because “Patent infringements, even before filing” according to [BITKOM, the German digital tech association](#).

- The Australian Security Intelligence Organisation, AIC, calculates espionage cost the Australian economy \$12.5 billion in 2023–24. This includes the direct impact of espionage - for example, intellectual property theft: [The cost of espionage](#)

“We have observed a lot of DDoS attacks, serious DDoS attacks happening across [the Middle East] due to political instability around the region.”

- Director of Security, Major CSP in the Middle East

Regulatory frameworks are expected to expand further into AI, quantum technology, and post-quantum cryptography. As geopolitics and cybersecurity become increasingly intertwined, many industry analysts suggest that CSPs will need to evolve from compliance-driven approaches to more intelligence-led, risk-adaptive strategies.

“We are entering a new era that will be characterised by radical uncertainty. The international order is being reshaped by an intensification of great power competition, authoritarian aggression and extremist ideologies.” - UK National Security Strategy, 2025





Key strategic directions of CSPs

Telecom operators are no longer just service providers. They're becoming banks, AI platforms, and sovereign cloud hosts, all while defending against more specialized threats.

AI and digital sovereignty

For leading CSPs, AI is strategic infrastructure. They're positioning as sovereign AI partners, delivering locally controlled, compliant AI solutions that are based on trusted technology and address strict data localization mandates.

Investment priorities reflect this ambition: 72% of telecom operators rank AI/ML-based threat analytics as a high priority, with Asia Pacific leading among regions.

Over half of operators (55.7%) plan to use AI for threat detection and anomaly identification in the next 12-18 months, with predictive threat intelligence and pattern recognition close behind (48.5%).

The best performers combine AI governance frameworks with sovereign cloud platforms, making AI adoption safer and faster.

“This year is completely about upskilling people to use GenAI for telcos.”

- Assistant Vice President,
Major CSP in APAC

“About a year ago, we built an internal AI governance team and partnered with an external company to support the practice. This team governs AI and automation requests across the company, not just in cybersecurity. For example, we've deployed use cases like an external threat intelligence tool that uses AI and automation to extract key insights from daily reports that span hundreds of pages, and no one has time to go through this.”

- CISO, Leading CSP in North America

Security assurance in autonomous networks

Current state

Security must be integral to any investment and strategy for fully autonomous networks. From physical infrastructure to cloud-based applications, every layer should incorporate advanced threat detection, encryption, and authentication. This enables CSPs to shift from reactive defense to predictive security, identifying and mitigating vulnerabilities before they impact operations. These are networks that can sense, think, and act, and to reach this level of operations, operators must start with a targeted and secure automation strategy.

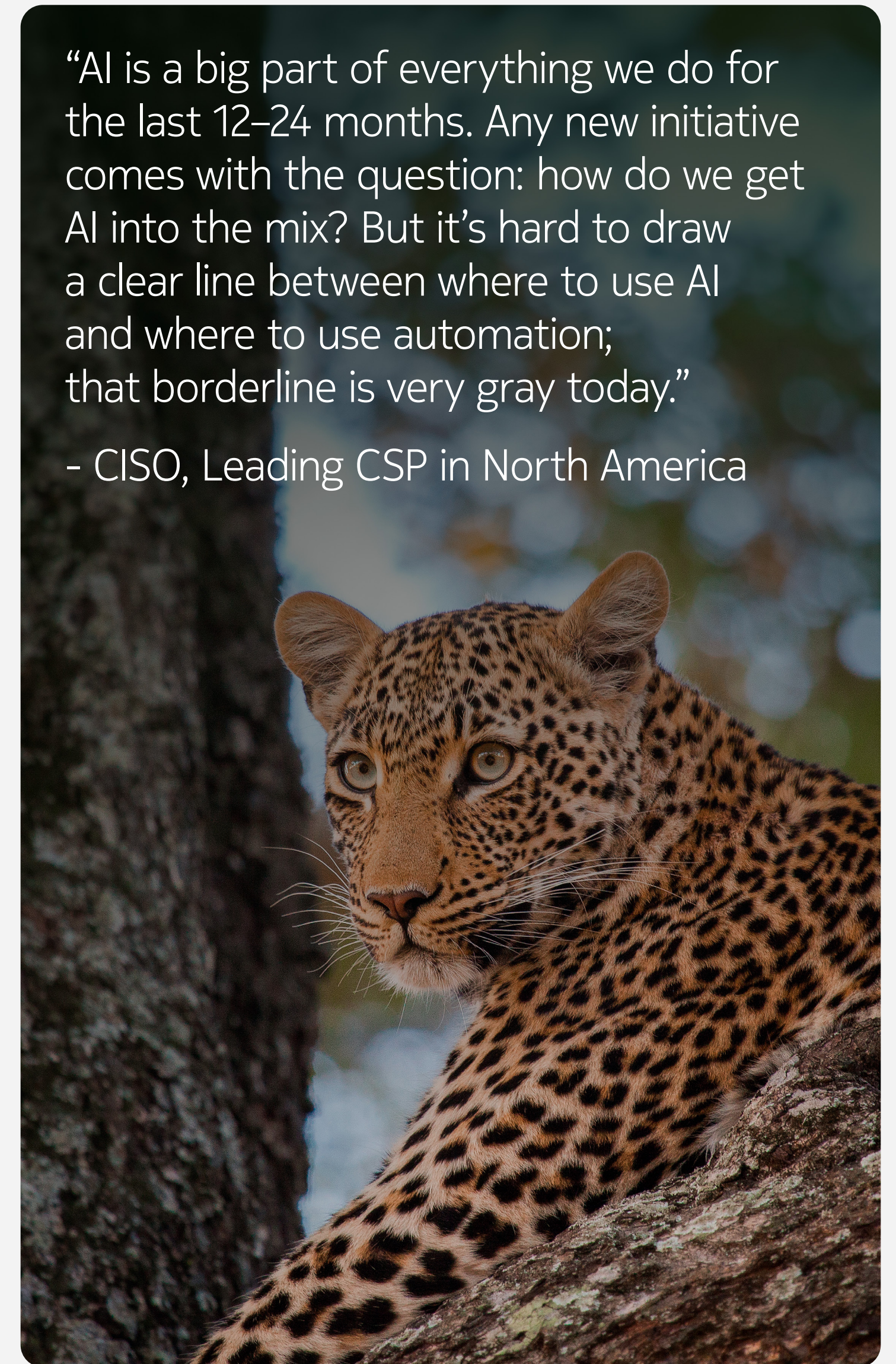
Telecom operators are moving up the automation curve: Level 3 (conditionally autonomous) is the largest cohort today at 38.1%, while assisted (18.6%) and partially autonomous (26.8%) still account for 45.4% combined.

Short-term ambition

Within 12 months, highly autonomous SOCs are expected to almost double (from 11.3% to 21.6%).

“AI is a big part of everything we do for the last 12–24 months. Any new initiative comes with the question: how do we get AI into the mix? But it's hard to draw a clear line between where to use AI and where to use automation; that borderline is very gray today.”

- CISO, Leading CSP in North America

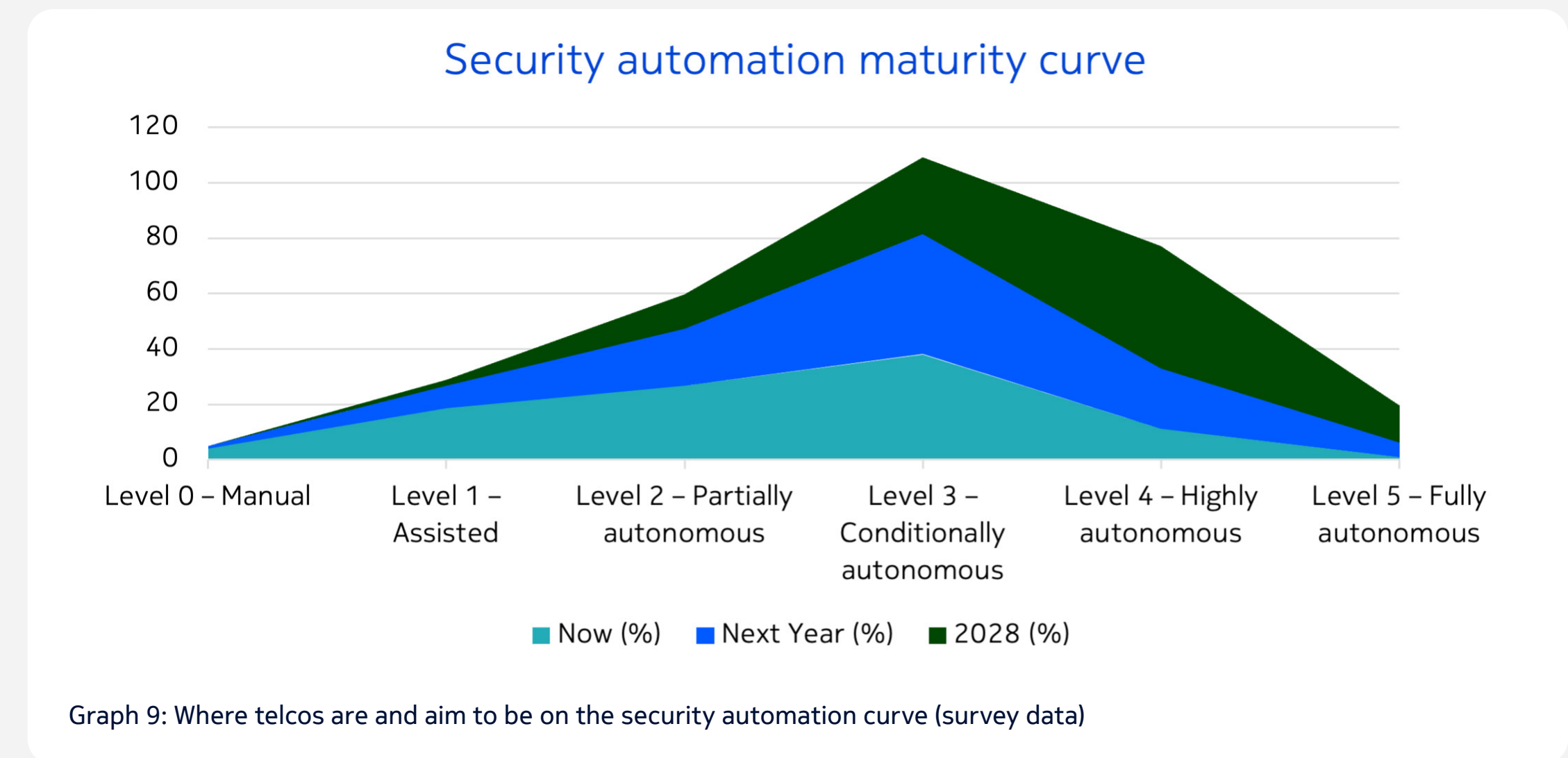




By 2028, over **half** of telecom operators (57.7%) expect to run highly or fully autonomous security operations.

Looking to 2028

- 44.3% highly autonomous (AI predicts security incidents and autonomously creates detection rules. Proactive threat hunting and scenario modeling based on security telemetry and threat intelligence)
- 13.4% fully autonomous (The SOC is run by autonomous AI agents that collaboratively manage incidents and crisis responses in real time with minimal human input)
- Manual and assisted operations almost gone



This reflects rising confidence in automation technologies to reduce human error, accelerate detection and response, and handle the scale and complexity of telecom security.

Network security assurance in this context means embedding intelligent, self-correcting protection directly into the network fabric. Following a “sense-think-act” framework, autonomous security systems should:

- Sense: Constantly scan for anomalies and malicious patterns.
- Think: Correlate, assess, and decide the right countermeasure.
- Act: Contain the threat before human intervention is needed.

Supply chain exposure and third-party risk

Supply chain dependencies now span hardware, cloud providers, managed services, and software components, making vendor assurance a frontline security challenge.

Survey results reflect the tension: operators ranked vendor/third-party risks as second major challenge in achieving strong 5G security (following complex integration of legacy and 5G systems). Security leaders are recalibrating how they assess and monitor partners. Many now enforce stricter contracting terms, cut ties with noncompliant suppliers, and scrutinize subcontractor arrangements that expand exposure.

“Our big area of focus is third party risk management. Some of the vendors, as a result of this due diligence, may not be our partners anymore.”

- CISO, Leading CSP in North America

CSPs are beginning to treat vendor ecosystems with the same rigor as their own networks. The leaders will be those who embed continuous monitoring and zero-trust principles into third-party relationships, reducing the risk of invisible compromises propagating across critical infrastructure, and of geopolitically motivated exploitation.

“We thought suppliers and professional companies were more mature on security, but we found weaknesses across the whole supply chain... Some vendors still prefer to fix a vulnerability first before telling us, but we need them to inform us immediately, even before they patch.”

- Global Business Security Officer, Leading CSP in Europe

Business model evolution and service expansion

Telcos are moving beyond connectivity into financial services, IoT ecosystems, and enterprise platforms. As one Cybersecurity Manager at a Brazilian operator explained:

“Telecommunication companies are turning into a bank platform too.”

This expansion brings new regulatory obligations and threat models. Telecom-bank hybrids now face both SIM swap fraud and banking malware.

The winners will be those who merge telco-grade security with fintech-grade compliance, building trust across both domains.

Network infrastructure modernization

The 5G rollout is colliding with legacy systems, and the collision is costly. 54% of operators struggle with legacy-5G integration, and 31% still have vulnerabilities in user plane function (UPF) components.

This is not only a performance problem but can also become a security liability. CSPs investing in self-healing, AI-driven networks are pulling ahead, using predictive maintenance and automated mitigation to shrink downtime windows.

31.1% of respondents observed SIM lifecycle abuse in the past year, with Europe showing the highest share among regions.

“Telecom networks are moving into cloud environments. That means open protocols and open systems which may be open for attacks. For operators used to proprietary hardware, this is a big shift and we must ensure detection, protection and recovery in the cloud.”

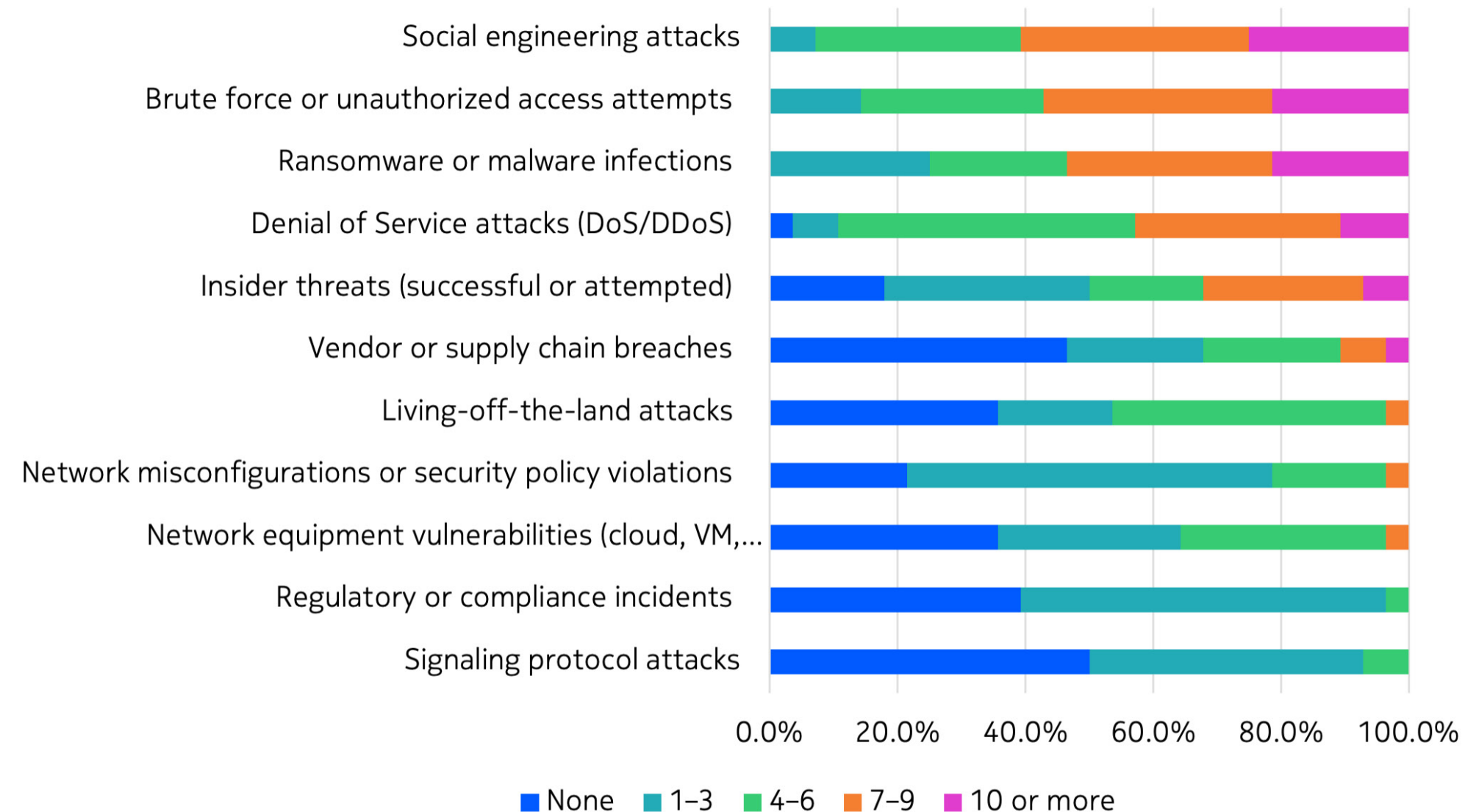
- Global Business Security Officer,
Leading CSP in Europe

Regional threat adaptation

According to our recent threat survey, threat patterns and priorities vary by region. Regional findings are based on subsamples of approximately n≈28–38 per region (directional).

Middle East & Africa shows elevated brute-force and unauthorized access attempts, with about 6 in 10 operators experiencing seven or more incidents last year. SIM lifecycle abuse is a notable concern (36%). Zero-trust implementation is a top investment focus, prioritized by roughly three-quarters of respondents.

Incident frequencies in Middle East & Africa



Graph 10: Security incident frequencies by type in Middle East & Africa (survey data)

Latin America leads in telecom-adapted malware exposure (64%) and custom toolkits targeting telco platforms (50%). Fake base station deployments are common (32%). The vast majority of operators in the region prioritize network security operations.

Europe reports the highest social engineering severity, with 30% of operators experiencing 10 or more incidents in the past year. SIM lifecycle abuse (46%) and covert data exfiltration (38%) are also prominent. Nearly three-quarters of operators prioritize AI/ML-based threat analytics.

“The riskiest incident was a malicious software package put on an old-fashioned server in our network. Nothing happened for many months, but at the end this software package started to move to other, more sensitive servers... What was really interesting for me was to understand that some attacks don’t act immediately; they wait and make the problem months later.”

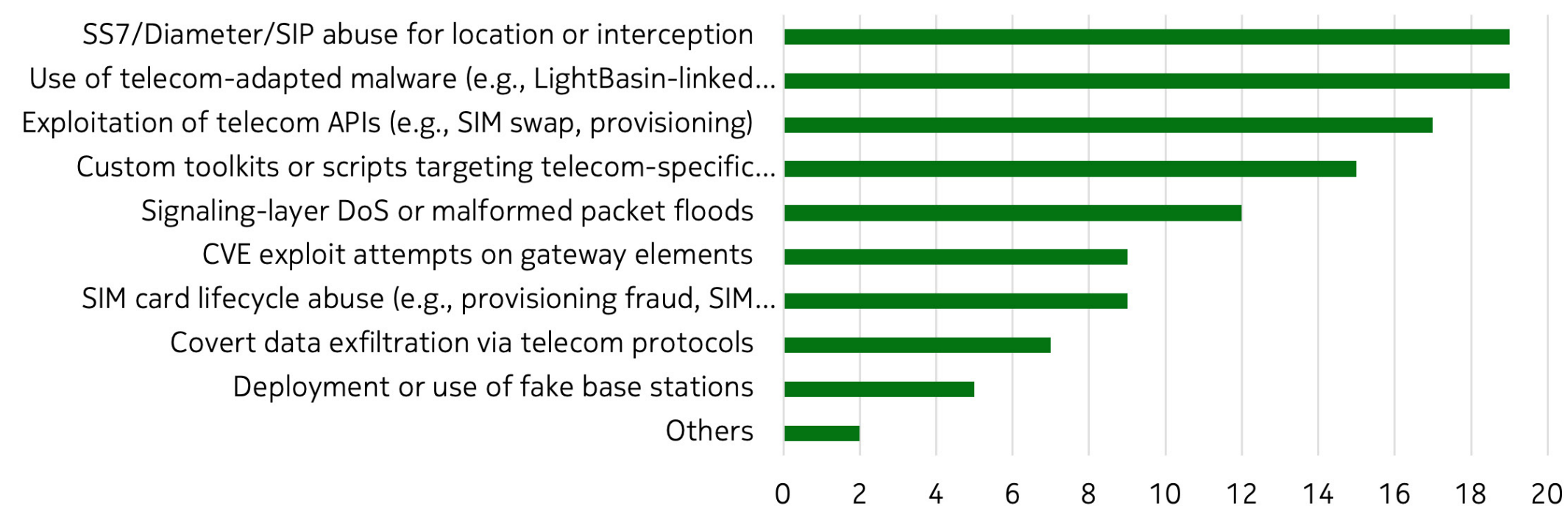
- Engineering and Implementation Director,
Leading CSP in **Latin America**

“The fraud and scam attempts, both on voice and SMS and also on email, have exploded the last years. In a fairly small country like Norway, with 5 million people, last year we blocked more than 2.2 billion scams.”

- Global Business Security Officer,
Leading CSP in **Europe**

Asia Pacific shows the highest rates of SS7/Diameter/SIP abuse (58%) and the use of telecom-adapted malware (58%). Integration of legacy and 5G systems is the most cited security challenge (67%). More than 8 in 10 operators in the region prioritize AI/ML-based threat analytics.

Attack behaviors observed in Asia Pacific



Graph 11: Attack behaviors observed in Asia Pacific (survey data)

North American operators report higher preparedness for ransomware ($\approx 4.18/5$) and DDoS attacks ($\approx 4.11/5$) than for zero-day ($\approx 3.29/5$) or nation-state threats ($\approx 3.24/5$). AI/ML-based threat analytics is a high investment priority for nearly two-thirds of respondents.

“Anything new that hits you, you’re immediately running into two challenges: dollars and resources. First you deal with the dollars, then you deal with how to quickly respond with the right people.”

- CISO, Leading CSP in **North America**

Operational resilience and leadership alignment

Recovery times are slow: 63% of major incidents take more than a week to fully recover, long enough to hurt uptime, revenue, and trust. In this climate, CSPs must balance rapid containment with uninterrupted service – a tension acknowledged by operators and security leaders.

Leadership alignment is critical. Without executive support, security actions that inconvenience internal teams or customers risk being deprioritized. As one security strategy lead in Europe notes, “Our senior executives understand security and appreciate that we may need to inconvenience people at times.” Another leader in APAC observes, “Security has started finding space in quarterly presentations... strengthening the network from a security perspective has increased.”

Resilience is not only about speed of recovery; it also depends on visibility. Operators often inherit infrastructure from prior acquisitions, creating potential blind spots that attackers can exploit. As a North American CISO puts it, “One of the biggest gaps we discovered was in infrastructure from prior acquisitions, what we call shadow IT and shadow networking.”

Downtime remains the most tangible risk. For many operators, every minute offline halts critical financial flows: “Availability is the first thing. Every minute our network doesn’t operate, it stops all the money that flows through,” says an Access Technology Director in North America.

Conclusion

The telecom threat landscape has entered a phase of persistent, and highly specialized attacks. From lawful interception compromises to AI-driven exploits and post-quantum risks, adversaries are targeting the very foundations of trust and availability in telecom networks. Operators are responding with automation, AI-enabled defenses, and stronger regulatory alignment, but resilience will hinge on how well they integrate security into every layer of infrastructure, operations and governance. The challenge is not just to keep pace with threats, but to ensure that the networks society depends on will remain resilient, trusted, and available.

“From telecom perspective, availability is priority number one. If we are not available, financial institutions, retail stores, and transactions come to a standstill.”

- Associate Director, Access Technology Development, Major CSP in North America





Nokia's cybersecurity expertise

NetGuard Portfolio

Nokia NetGuard Security is a comprehensive suite of cybersecurity solutions tailored for mission-critical telecom networks, with over 500 security projects delivered globally. It includes:

- [Cybersecurity Dome](#) - A centralized intelligence platform that correlates data across telecom domains, users, and security controls to expose hidden threats and automate response. It delivers unified, real-time visibility and assurance across the network.
- [Endpoint Detection and Response](#) - Telco-grade protection for critical network functions, combining host-level telemetry and network traffic analytics to detect and respond to both known and novel threats with precision and speed.
- [Identity Access Manager](#) - A telecom-specialized PAM solution that controls and audits privileged access, automates credential handling, enforces role-based policies, and secures sessions to prevent misuse and ensure compliance.
- [Certificate Manager](#) - Automates the full lifecycle of digital certificates, from issuance to renewal and revocation. It prevents outages from expired certificates, and supports compliance across complex, multi-vendor telecom environments.

These solutions empower CSPs and mission-critical enterprises to detect and respond to cyber threats efficiently, while strengthening Security Operations Centers with intelligent automation, deep visibility, and resilient protection.

AI-Powered DDoS Protection

[Nokia Deepfield Defender](#) leverages AI-driven big data and real-time analytics, enriched with detailed network context ([Deepfield Genome®](#)), to detect and block DDoS attacks. When deployed in a full solution, with Nokia advanced IP routers based on [Nokia FP processors](#) and/or with a dedicated FP5-based [7750 Defender Mitigation System](#) featuring advanced DDoS countermeasures, Deepfield Defender drives full-spectrum protection against both inbound (external) and outbound (internal) threats, covering botnet, volumetric and application-layer attacks.

Our advanced expertise is extended to our customers via the [Deepfield Emergency Response Team](#), which supports CSPs in minimizing the impact of DDoS incidents.

Managed Security Services

[Nokia Managed Security Services](#) (MSS) deliver a wide range of security services targeting multi-vendor telecom networks and critical infrastructure, including 24x7 SIOC (Security Intelligence and Operations Center) services, GRC (Governance & Risk Management) services with vulnerabilities management, security configuration management (MBSS), penetration testing boosted with specific telco expertise, and Security Infrastructure Management. Our teams carry out proactive and reactive operations to protect networks serving hundreds of millions of users worldwide. Insights from these operations provide a global view of critical security incidents, application vulnerabilities, and VAPT trends.

Quantum-Safe Networks

[Nokia's Quantum-Safe Networks](#) (QSN) use a defense-in-depth strategy with multi-layered cryptography to deliver security across all layers. Tailored to specific business needs, QSNs enable CSPs to scale quantum deployments securely. In collaboration with Nokia Bell Labs, the QSN team is pioneering the future of quantum-safe networking.

Advanced Research in Security

[Nokia Bell Labs](#), the 100 years old research lab with 10 Nobel prizes and 5 Turing awards, focuses a significant amount of its research on security and privacy technologies, as well as other foundational research that supports security applications and deployment. From Post-Quantum Cryptography to pioneering AI/ML anomaly detection, Bell Labs shapes the future of Security Research and sets the future standards of what are secure and private networks.

Advanced Cybersecurity Consulting

[Nokia Cybersecurity Consulting](#), part of our Advanced Consulting Services, offers deep expertise in 3G, 4G, and 5G security. We help CSPs assess risks, processes, and designs to secure their networks and comply with global cybersecurity regulations. With end-to-end 5G security capabilities built on in-house research and products, we support critical infrastructure providers in navigating complex security landscapes.

Methodology

Nokia has been producing threat intelligence reports for many years. The 2025 edition is the most comprehensive report to date, including a greater emphasis on cybersecurity trends and emerging technologies that impact the telecom industry.

The report is based on analysis 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
- DDoS traffic and attacks by the Nokia Deepfield Emergency Response Team (ERT)
- Cybersecurity regulation trends by Nokia's Strategy & Technology and Government Relations teams
- Quantum security by Nokia's quantum-safe networks security experts and Nokia Bell Labs
- Other emerging telecom security trends by the Nokia Bell Labs, Cybersecurity Consulting and Product Management teams

New in this year's report is a comprehensive survey, conducted between June and August 2025, blending quantitative and qualitative insights to capture telecom operators' cybersecurity priorities, preparedness, incident experiences, and investment plans. These survey findings are woven throughout the report, grounding every chapter in real-world perspectives.

- Audience: Security and network professionals from telecom operators and service providers globally, including both practitioners and decision-makers (e.g., CISOs, SOC leads, network architects).
- Quantitative survey: The study engaged 160 participants across all global regions through an online questionnaire of 12 questions. Questions Q1–Q4 were posed to all respondents, Q5–Q8 targeted decision-makers, and Q9–Q12 focused on practitioner perspectives. Detailed survey outcomes are in the Appendix.
- Qualitative survey: 10 participants across all regions interviewed using a 10-question guide to provide deeper context and validate quantitative findings.
- Analysis: Rankings were converted into weighted scores; preparedness ratings aggregated into percentage distributions; incident data grouped by frequency and cost ranges; and AI/ML adoption trends analyzed globally and by region.



Disclaimer

This report is based on public resource data, for example, real-world data, industry research, and documented case studies. The information provided herein is for informational purposes only and does not constitute legal advice, nor should it be considered a substitute for professional judgment, legal advice, or independent verification. While every effort has been made to ensure the accuracy and reliability of the information presented, no warranty, express or implied, is given as to its completeness, accuracy, or suitability for any particular purpose.

The author and the provider of these information are not responsible or liable for any loss or damage arising from reliance on the information contained herein. The reader is solely responsible for its use or interpretation of the information provided herein, and shall conduct its own risk assessment, seek qualified and independent legal and cybersecurity professional advice before making any decisions or taking any actions based on the information in this report.



Glossary of abbreviations

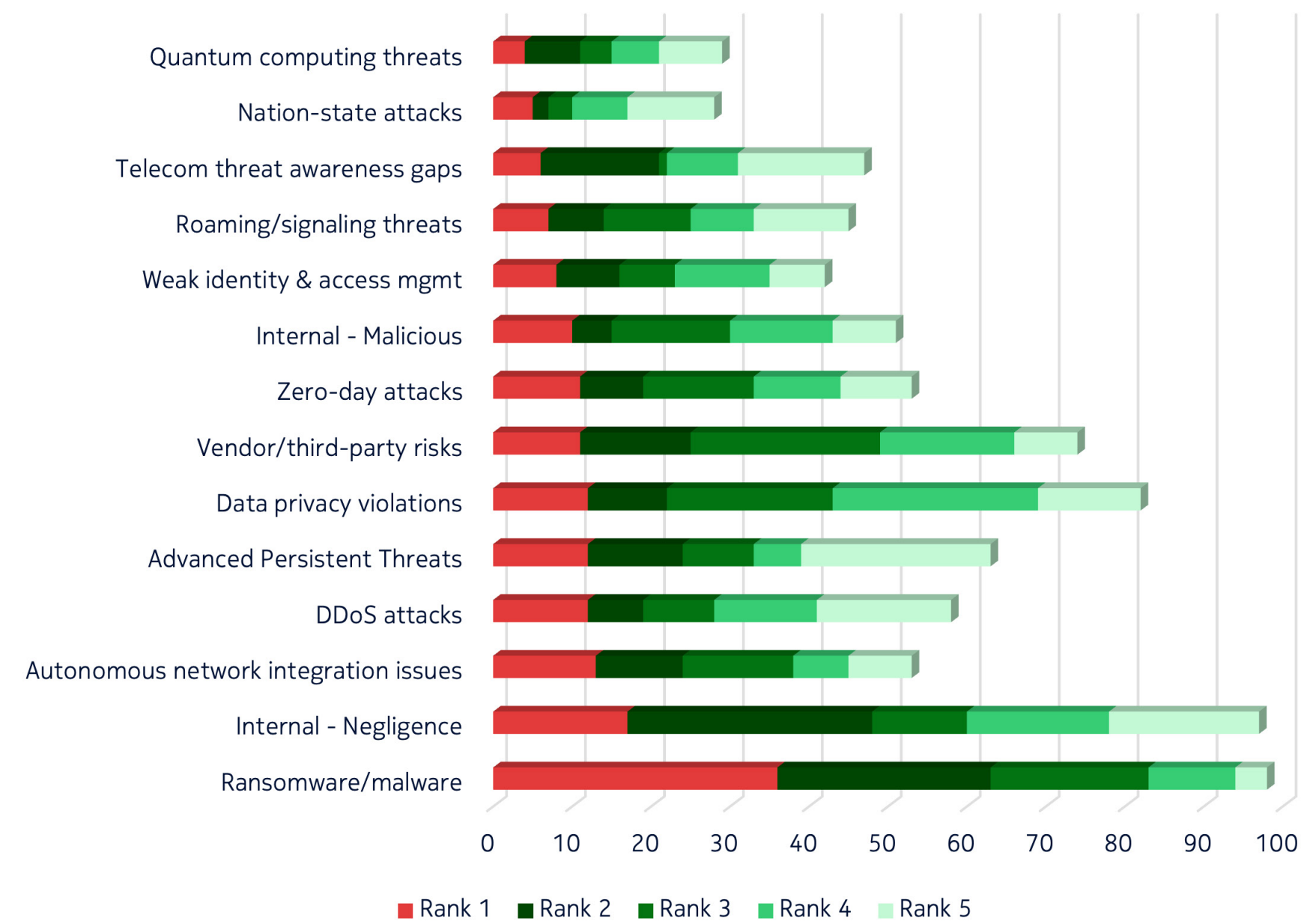
- AI – Artificial Intelligence
- AMF – Access and Mobility Management Function
- ANSSI – French National Cybersecurity Agency
- APATE – Adversarial Perturbation Against Traffic Efficiency
- API – Application Programming Interface
- APT – Advanced Persistent Threat
- BIKE – Bit Flipping Key Encapsulation (PQC candidate)
- CA – Certificate Authority
- CALEA – Communications Assistance for Law Enforcement Act
- CISA – Cybersecurity and Infrastructure Security Agency
- CORS – Cross-Origin Resource Sharing
- CVE – Common Vulnerabilities and Exposures
- DNS – Domain Name System
- DNSSEC – DNS Security Extensions
- DSA – Digital Signature Algorithm
- ECC – Elliptic Curve Cryptography
- ECU – Extended Key Usage
- EPC – Evolved Packet Core
- FALCON – Fast Fourier Lattice-based Cryptography (PQC candidate)
- FCC – Federal Communications Commission
- FTP – File Transfer Protocol
- GTP – GPRS Tunneling Protocol
- HLR – Home Location Register
- HQC – Hamming Quasi-Cyclic (PQC candidate)
- HSS – Home Subscriber Server
- ICMP – Internet Control Message Protocol
- IDS/IPS – Intrusion Detection/Prevention System
- IMS – IP Multimedia Subsystem
- IMSI – International Mobile Subscriber Identity
- ISO – International Organization for Standardization
- KEM – Key Encapsulation Mechanism
- KYC – Know Your Customer
- LLM – Large Language Model
- LOI – Law of Information (France)
- MEC – Multi-access Edge Computing
- MFA – Multi-Factor Authentication
- MITM – Man-in-the-Middle (attack)
- MME – Mobility Management Entity
- NATO – North Atlantic Treaty Organization
- EDR/NDR/XDR – Endpoint/Network/Extended Detection and Response
- NIS2 – Second EU Directive on Network and Information Security
- NIST – National Institute of Standards and Technology
- NOC – Network Operations Center
- NSA – National Security Agency
- OTA – Over-the-Air
- OTP – One-Time Password
- PCI – Physical Cell Identity
- PGW – Packet Gateway
- PII – Personally Identifiable Information
- POODLE – Padding Oracle On Downgraded Legacy Encryption
- RDP – Remote Desktop Protocol
- RIC – RAN Intelligent Controller
- RSA – Rivest-Shamir-Adleman
- RSRP – Reference Signal Received Power
- RTP – Real-Time Transport Protocol
- SBA – Service-Based Architecture
- SCADA – Supervisory Control and Data Acquisition
- SDN – Software-Defined Networking
- SIEM – Security Information and Event Management
- SIP – Session Initiation Protocol
- SLA – Service-Level Agreement
- SLH – Signature Lattice-based Hash (PQC candidate)
- SNMP – Simple Network Management Protocol
- SOC – Security Operations Center
- SQL – Structured Query Language
- SS7 – Signaling System No. 7
- SSH – Secure Shell
- SSL – Secure Sockets Layer
- SUCI – Subscription Concealed Identifier
- SYN – Synchronize (TCP flag)
- TCP – Transmission Control Protocol
- TLS – Transport Layer Security
- UDM – Unified Data Management
- UDP – User Datagram Protocol
- UEBA – User and Entity Behavior Analytics
- UPF – User Plane Function
- USIM – Universal Subscriber Identity Module

Appendix

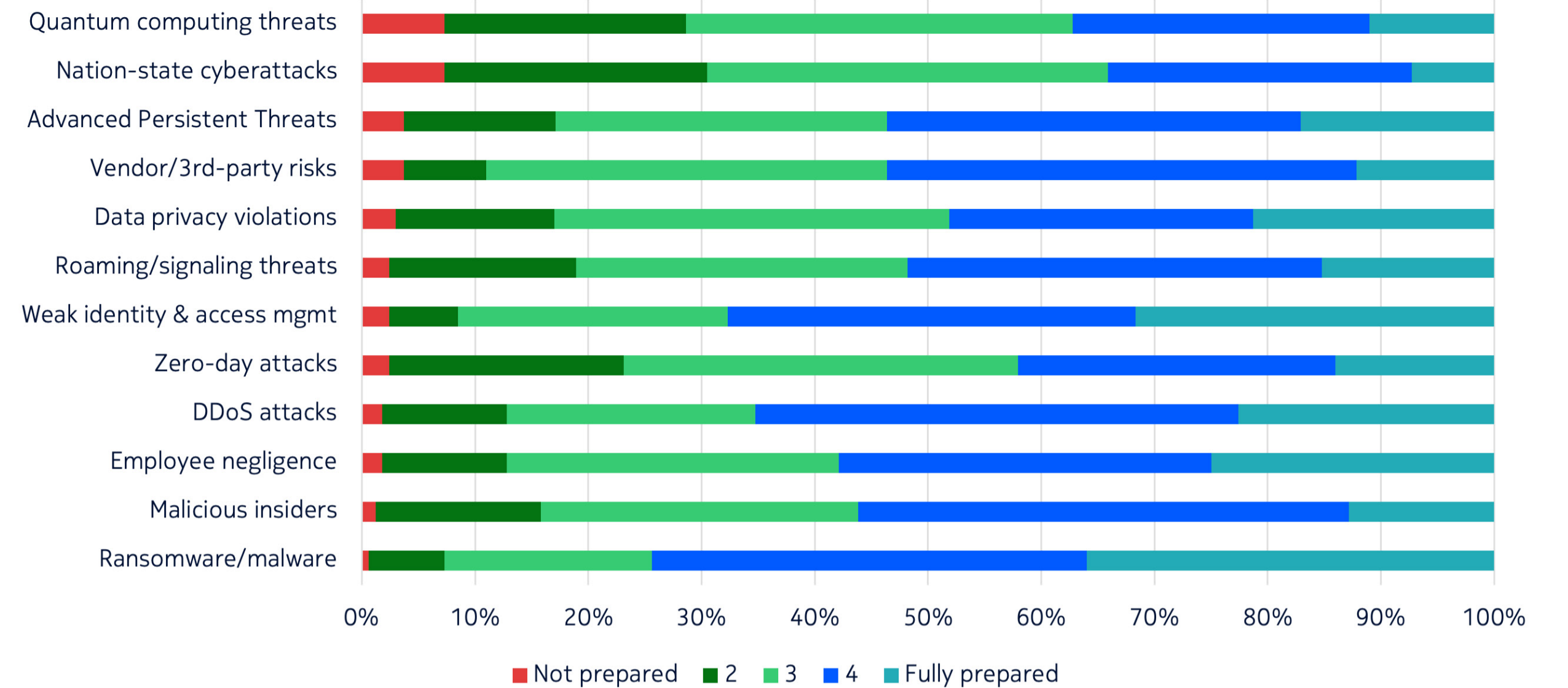
Please rank your organization's top 5 cybersecurity concerns, with 1 being your biggest concern and 5 being your fifth biggest concern. Consider potential business impact, likelihood of occurrence, and difficulty of mitigation.

How well prepared are you to handle each one? Preparedness refers to your team's current ability to detect, respond to, and recover from the listed risks; this includes having the right tools, technologies, skilled personnel, processes, and vendor support in place. Rate your team's current preparedness for the following risks

Top cybersecurity concerns

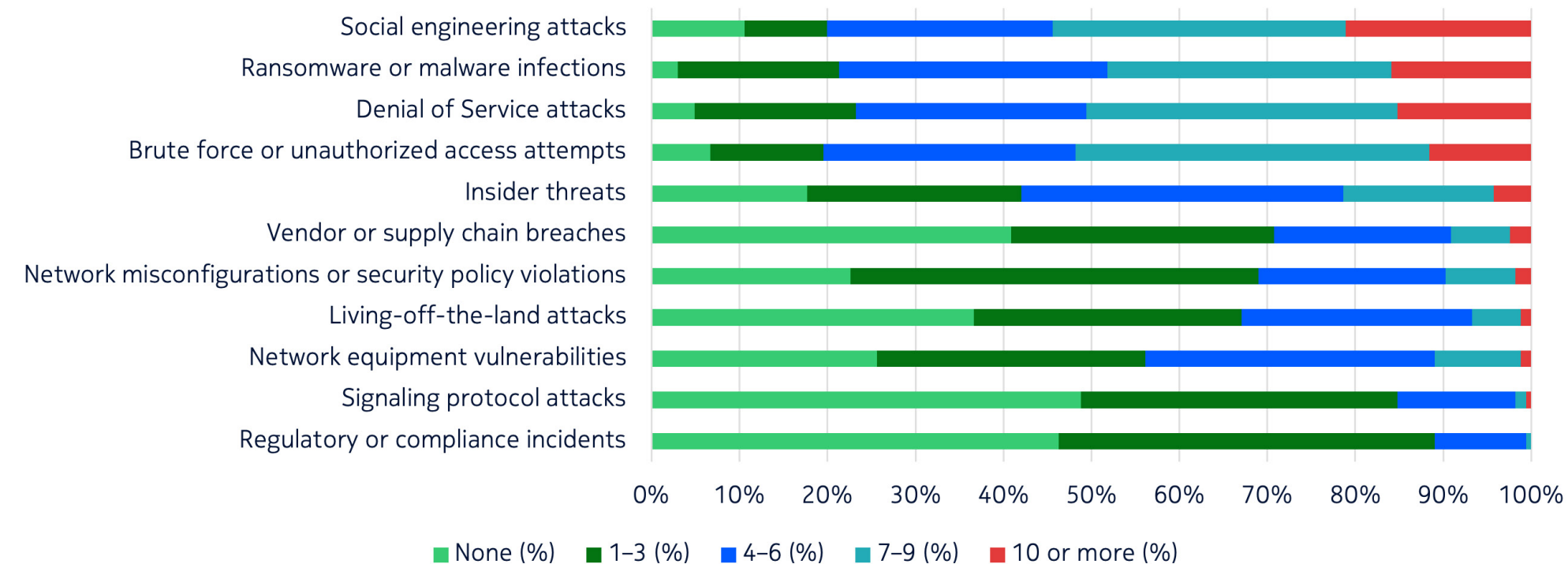


Preparedness



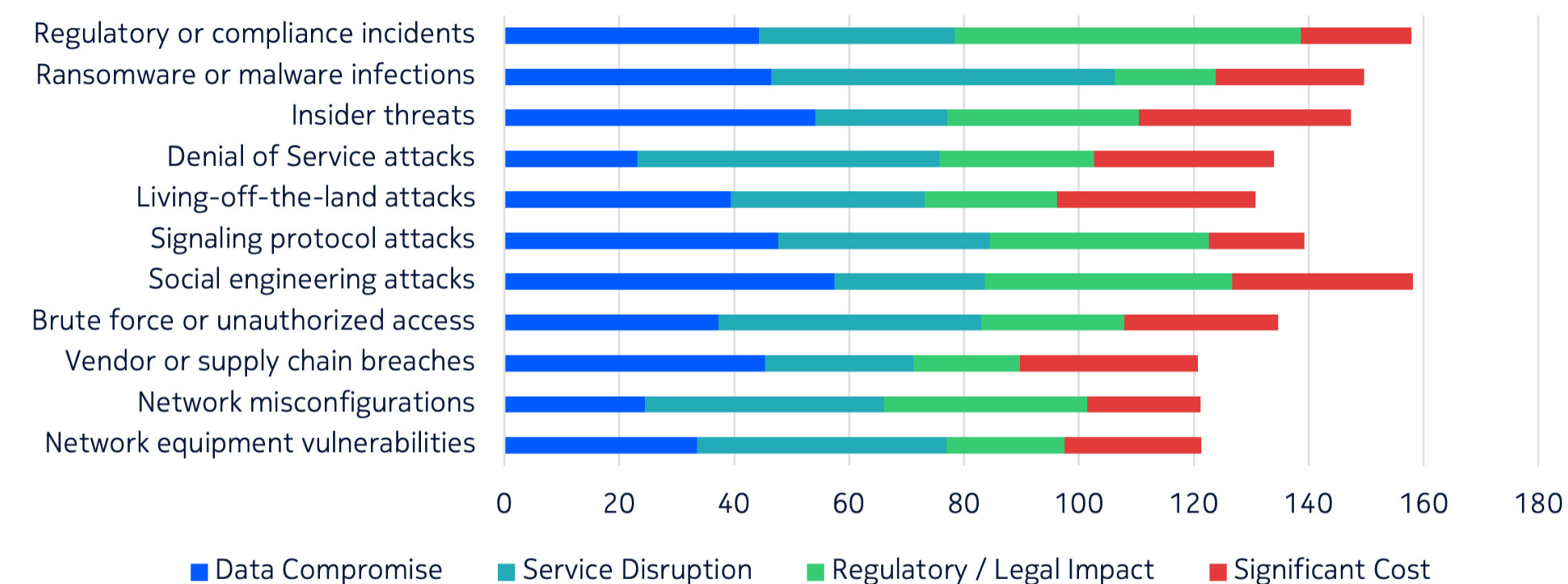
In the last 12 months, how many incidents has your company experienced of the following types?

Incident frequencies



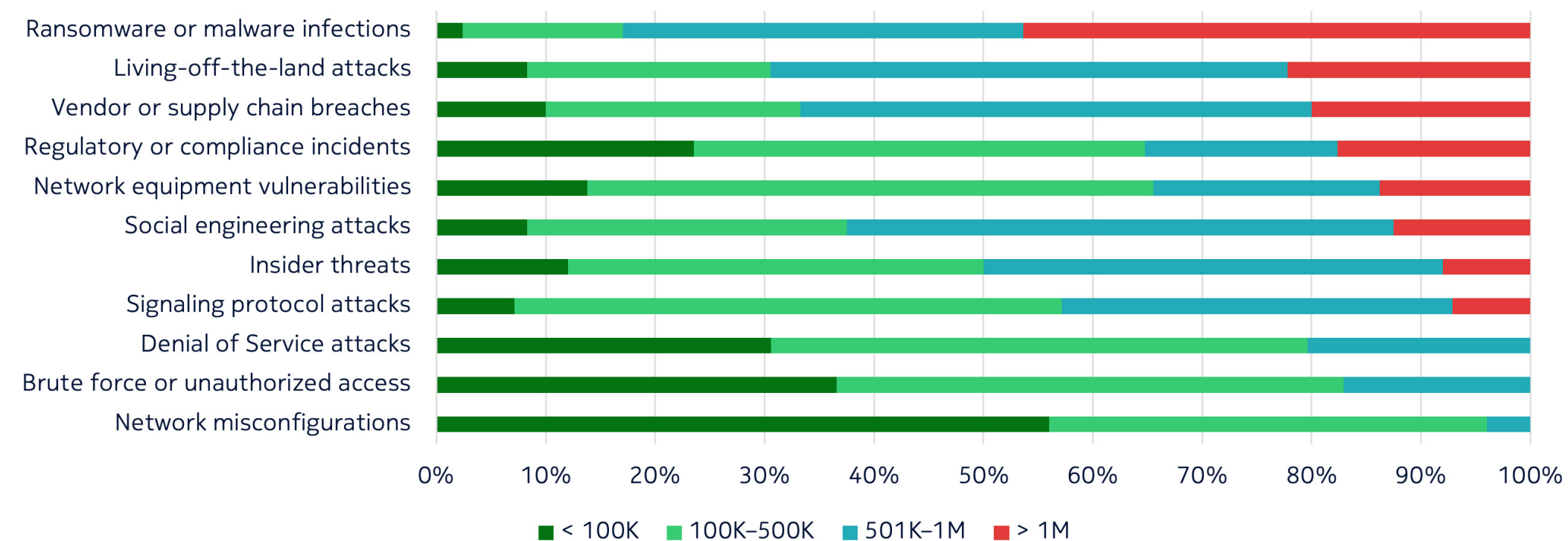
For the incident types your organization experienced, what were the actual consequences?

Incident consequences



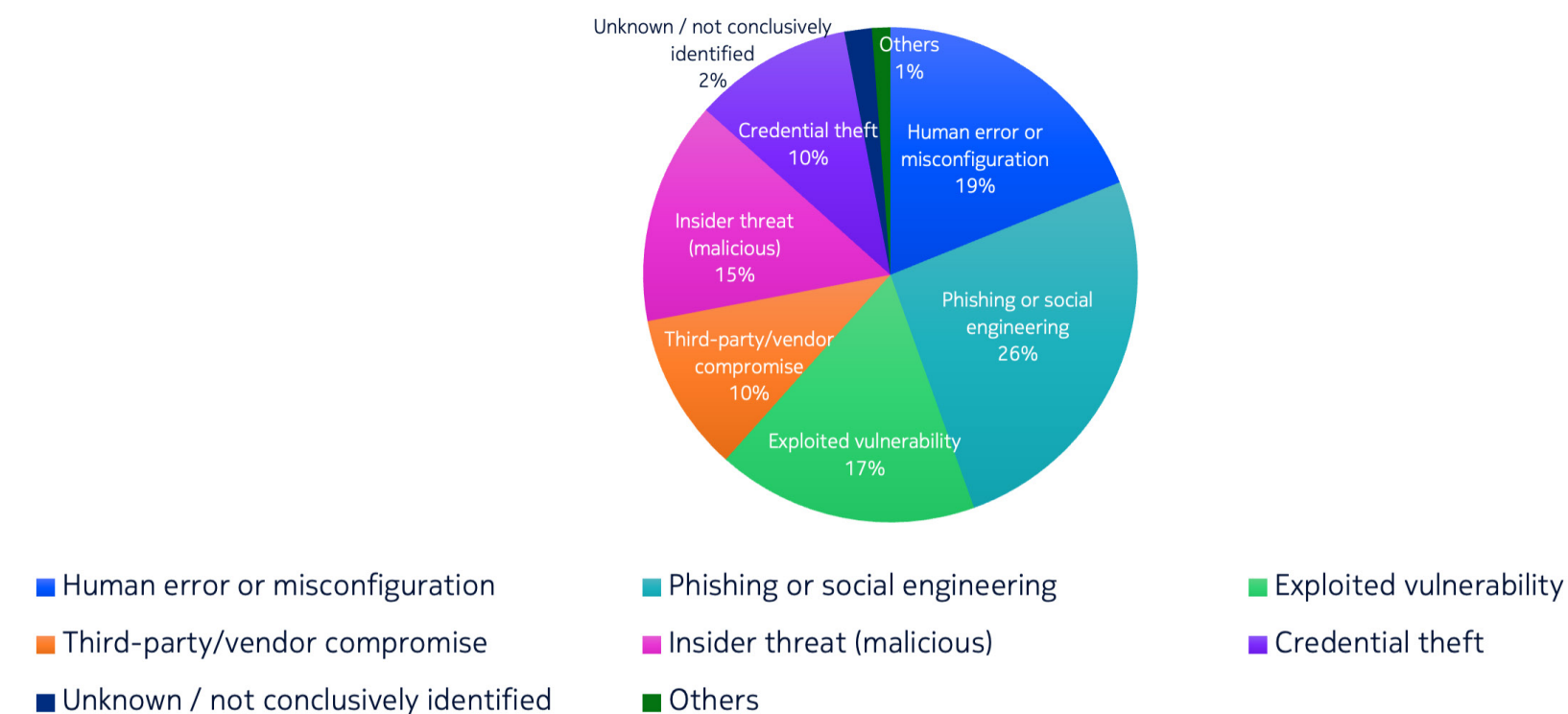
For each incident type that resulted in significant cost, please estimate the approximate cost range.

Costs of incidents

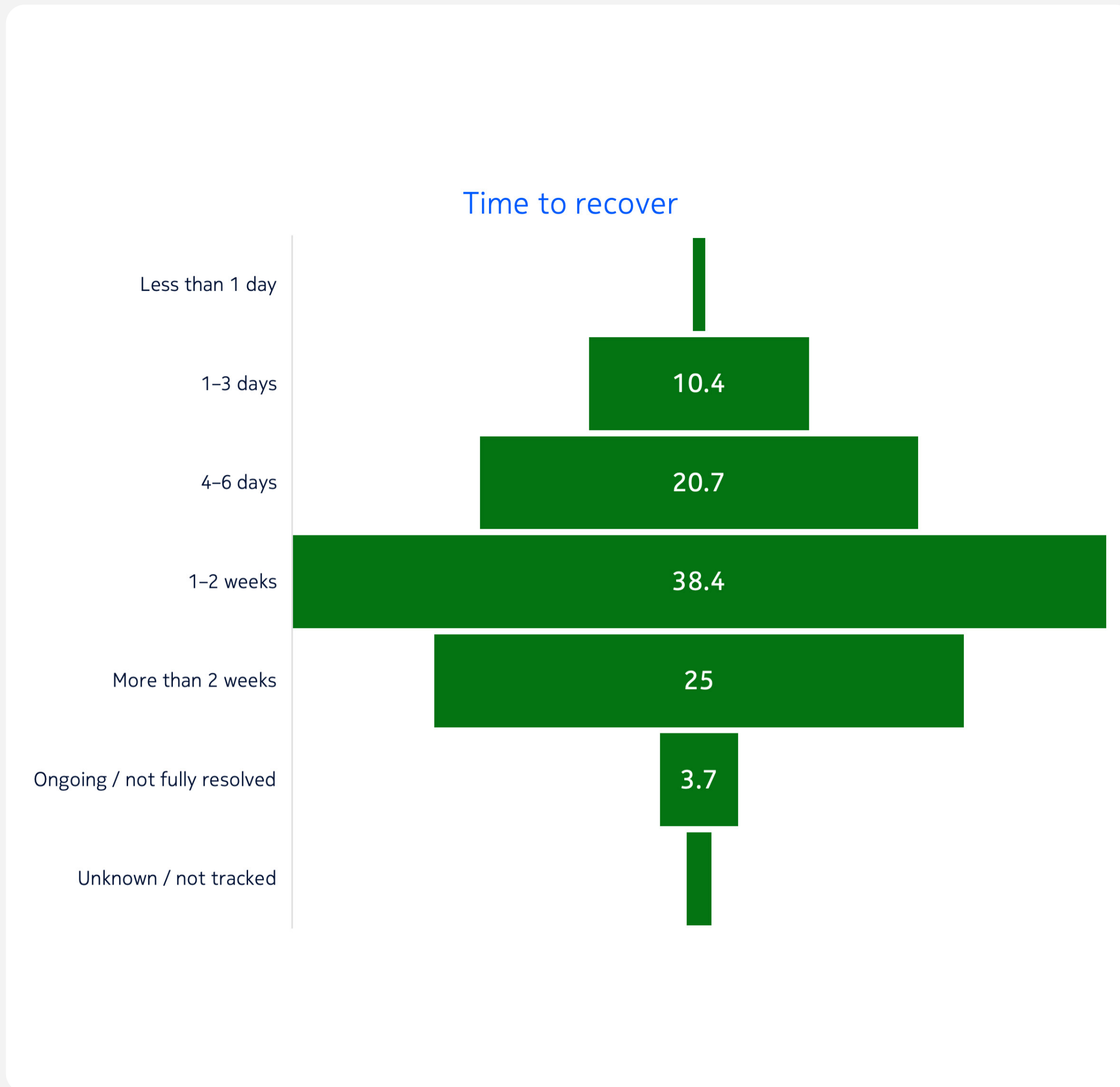


Thinking about the most impactful cyber incident your organization experienced in the past year (regardless of type) what was the primary cause of the incident?

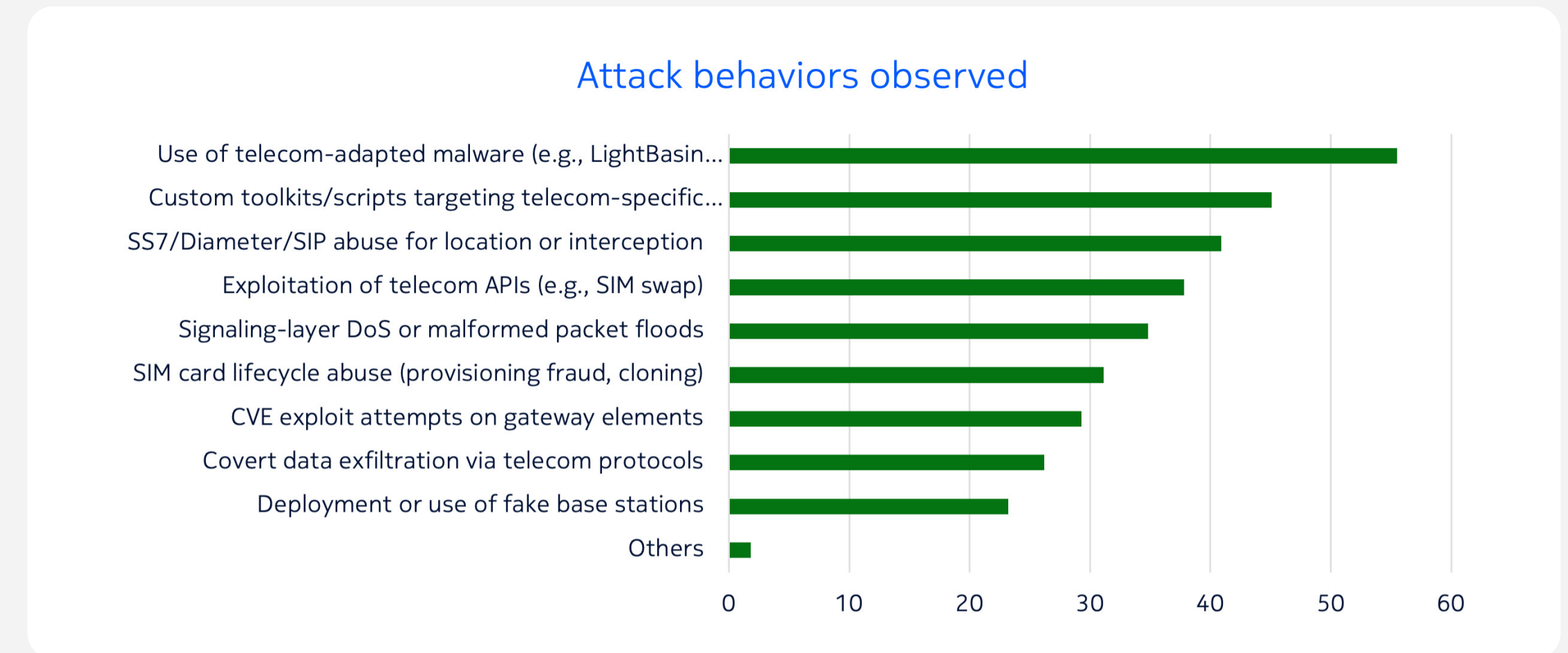
Root Causes of significant cost incidents



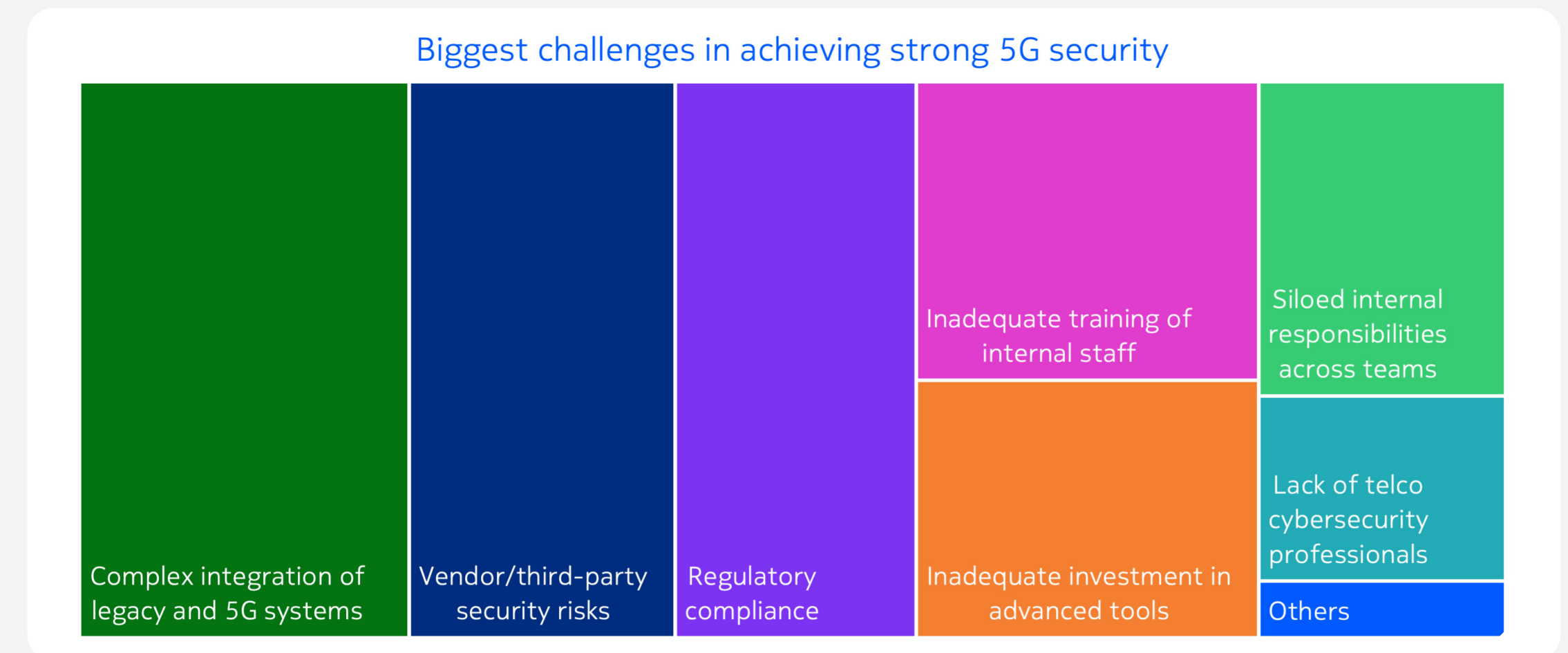
How long did it take your organization to fully contain and recover from it?



Which types of attacker behaviors or techniques have you observed targeting your telecom infrastructure in the past year?

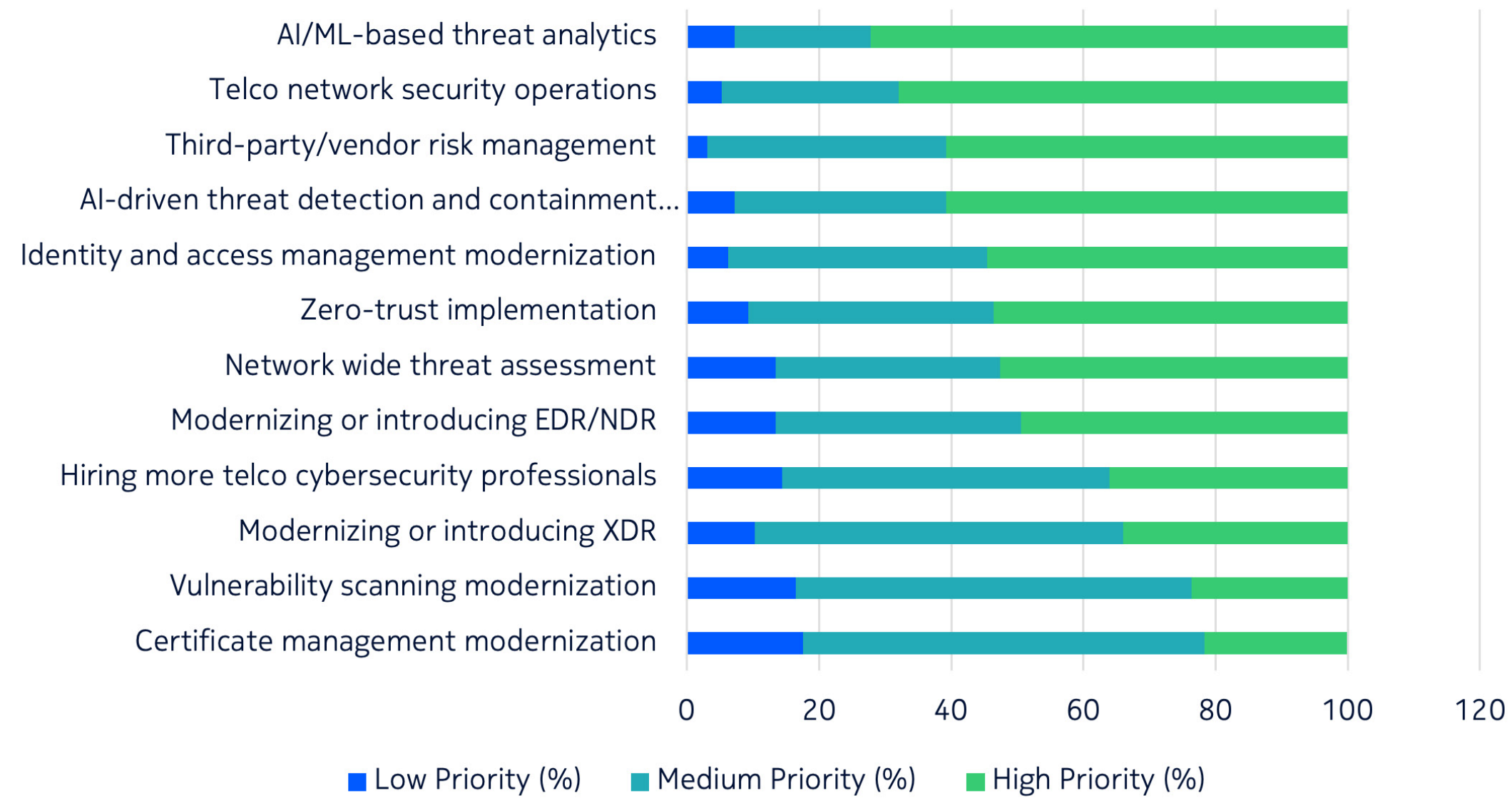


What are the biggest challenges your organization faces in achieving strong 5G security?



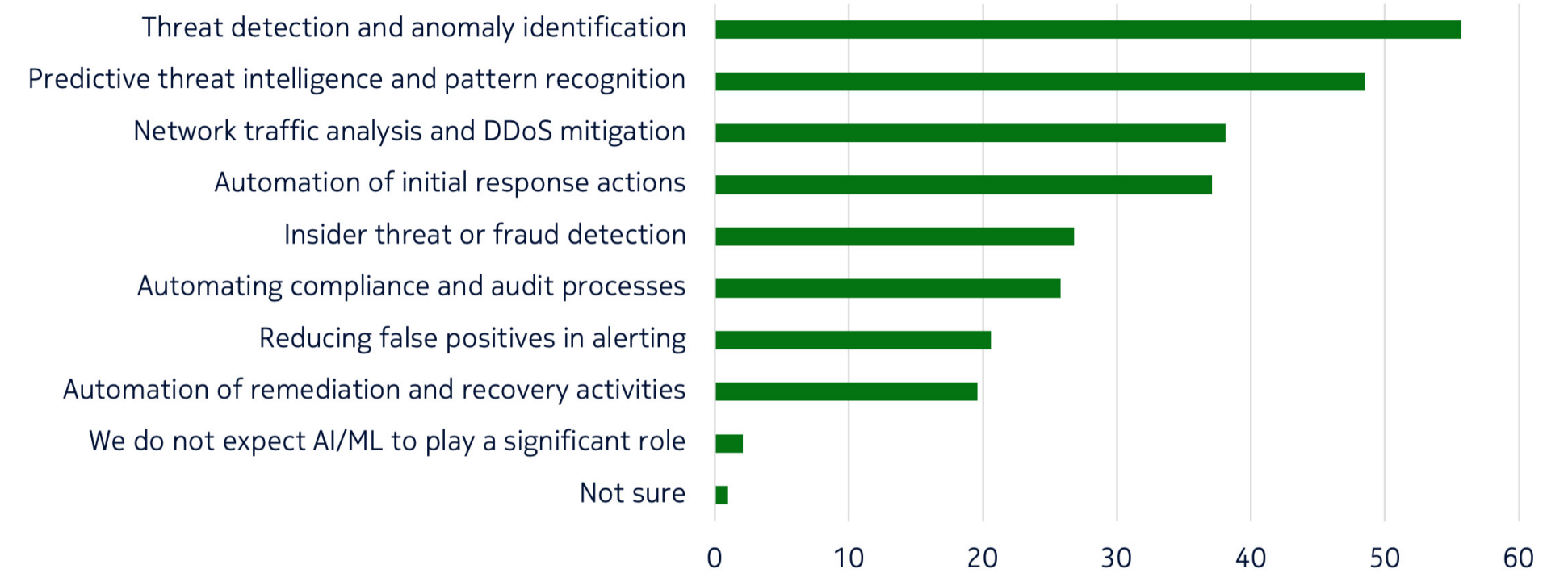
What investment priority are you assigning to the following security areas in the next year?

Investment priorities



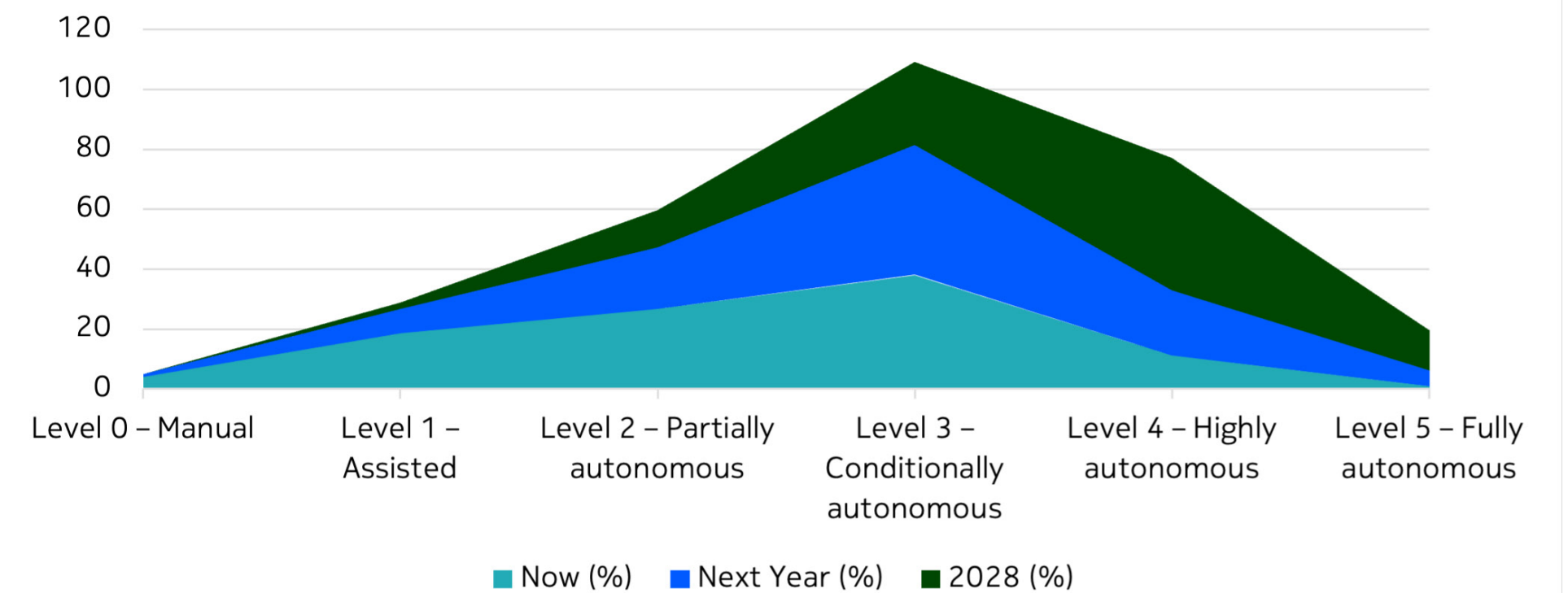
In which of the following areas do you see AI/ML playing a meaningful role in your 5G security operations over the next 12-18 months?

Expected role of AI/ML in 5G security operations



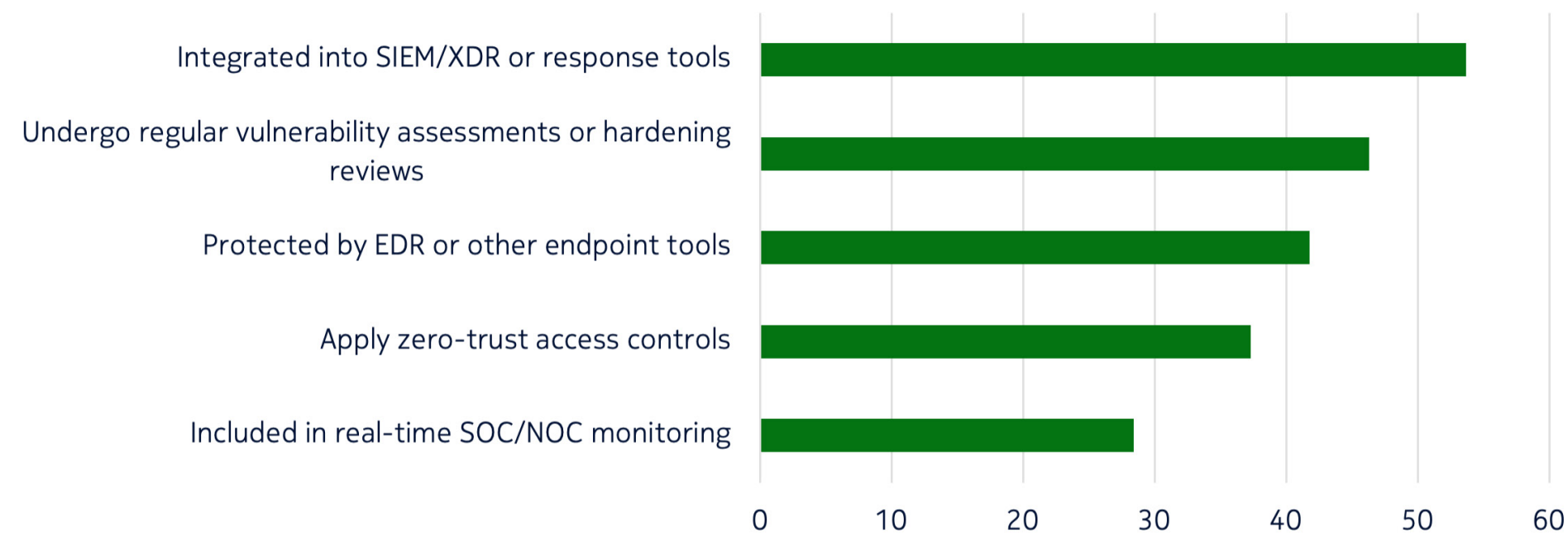
Where is your organization on the security automation maturity curve today, where do you aim to be next year, and where do you aspire to be by 2028?

Security automation maturity curve



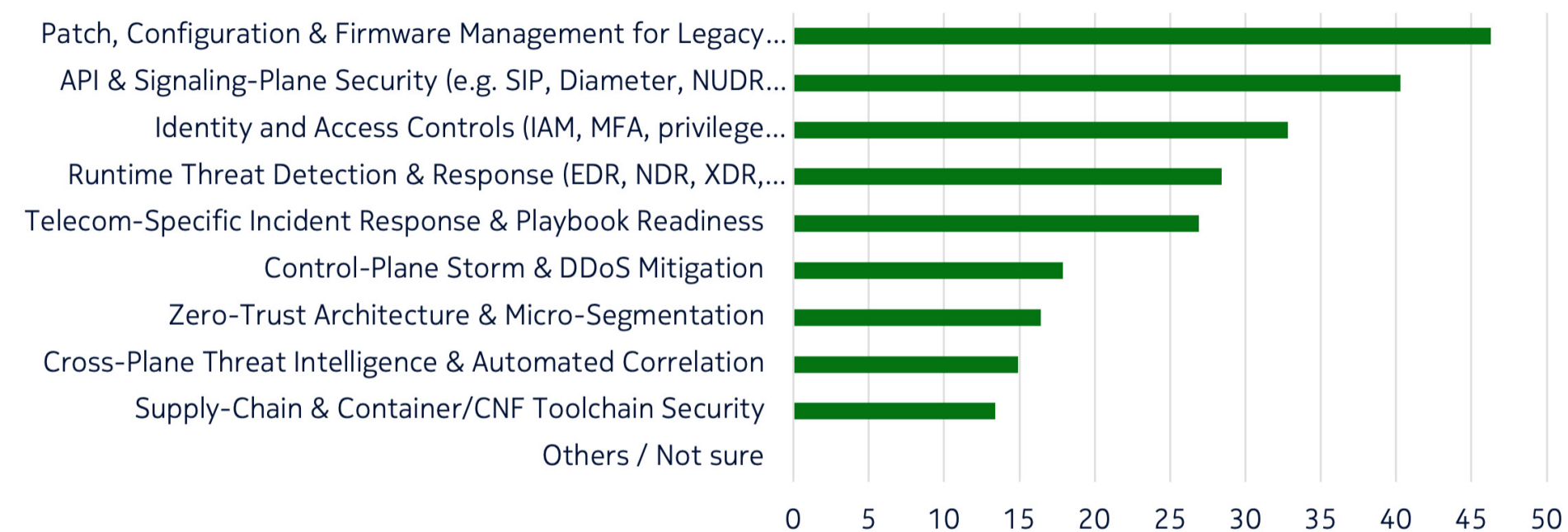
Which of the following statements best reflect your current security posture for your network's subscriber-data repositories and session-control elements (e.g., HLR, UDM, SDL, S-CSCF, AMF)?

Current security posture for subscriber-data repositories & session-control elements



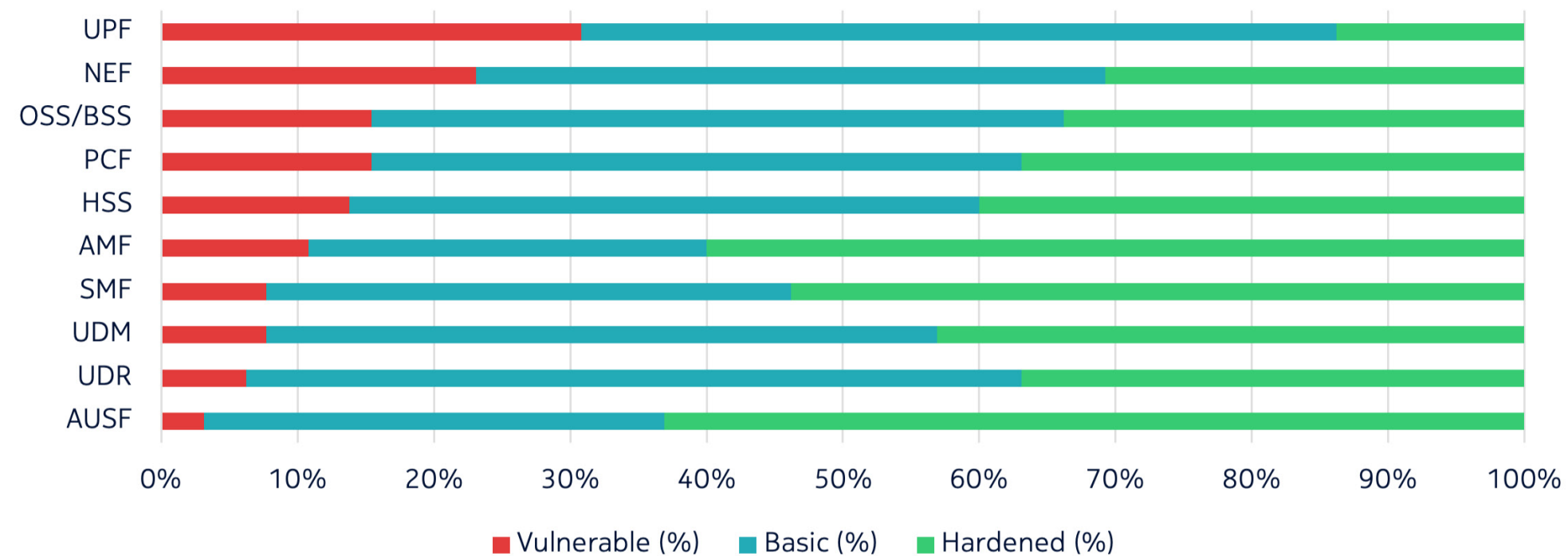
Based on your experience or observations of recent telecom-targeted cyber incidents (e.g. Salt Typhoon), which security controls do you believe are most commonly underperforming or failing to prevent impact?

Underperforming security controls in the industry based on recent telecom attacks



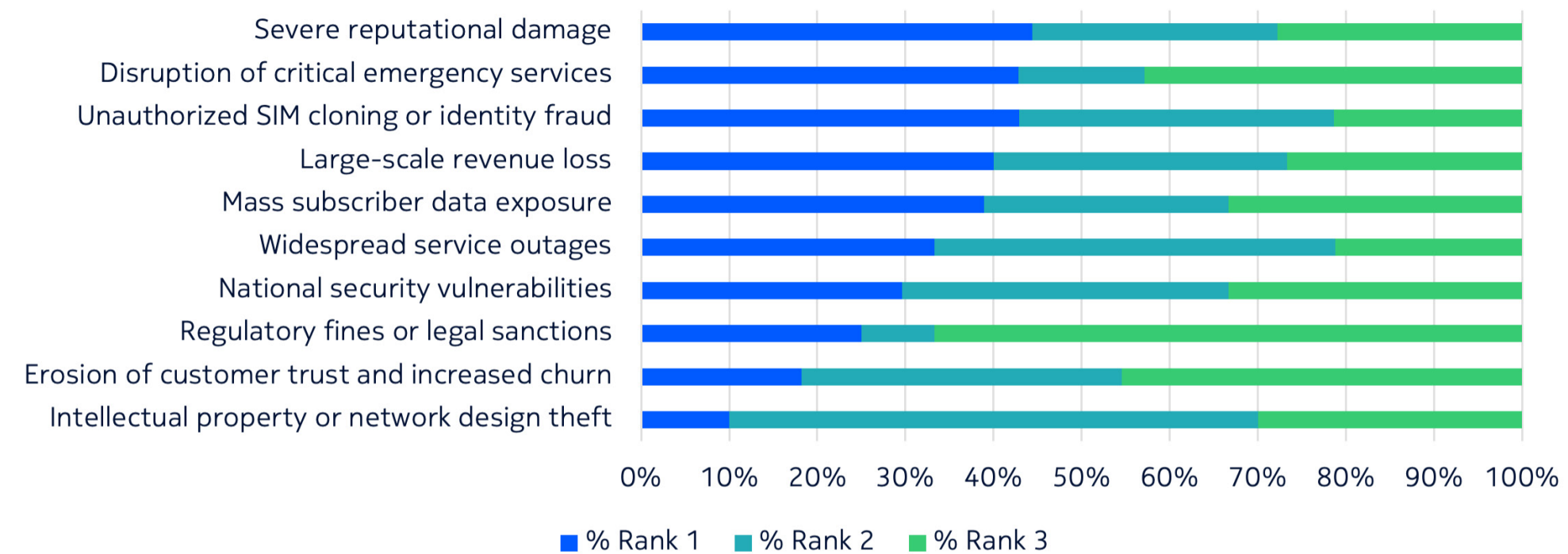
How would you rate the current security posture of the following 5G core components in your network?

5G core component security posture



What do you consider the 3 most serious consequences of a breach in your telecom network?

Most serious consequences of a breach in telecom networks



Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 215118

nokia.com

NOKIA

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.

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

© 2025 Nokia