Critical network security in 2025

Threats you can't ignore

Nokia Threat Intelligence Report 2025

Stealthy intrusions, record-breaking DDoS attacks, and rising cryptographic demands are defining network security in 2025. Here's what operators must act on now.

"Salt Typhoon was the most significant cybersecurity incident we faced in the last 12 months… 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

What's putting critical networks under pressure in 2025

Stealthy campaigns hit the telecom core

63% of network operators were hit by "living-off-the-land" attacks (where attackers use legitimate tools and processes to stay hidden)

Long-term compromises bleed data

Multi-year compromises caused major **data exposure** and costly remediation

Insider risk determinates high-cost breaches

59% of high-cost breaches linked to insider actions or mistakes

DDoS floods break records

Terabit-scale DDoS barrages hit **daily** (vs. every 5 days in 2024). Peaks are now over **10 Tbps**; most attacks burn out in under 5 minutes, but can cause significant business losses and damage reputation

Residential proxies amplify attacks

100M+ endpoints brokered globally, expanding the attack surface 100x from ~1M bots

AI becomes the frontline defense

70% prioritize AI-based security analytics

50% plan AI deployment within 18 months

Cyber hygiene gaps persist

76% of vulnerabilities stem from missing patches

Crypto agility moves to the front line

Certificate lifetimes shrink **from 398 days to 47 days** by 2029; automation is no longer optional

"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

Immediate actions to strengthen network resilience

Spot stealthy attacks early
Monitor core systems and enforce behavioral baselines for privileged accounts

Automate DDoS response
Deploy systems that can accurately detect complex multi-vector DDoS attacks and activate sub-60-second mitigation

Kill proxy-driven exposure
Identify and block residential proxy brokers; monitor for abnormal traffic bursts

Close insider and vendor gaps
Enforce least privilege, just-in-time access, and continuous validation for third parties

Get crypto agile
Automate certificate lifecycle management and plan post-quantum migration now

Let AI hunt for you
Deploy AI/ML to flag anomalies, predict attack chains, and auto-trigger playbooks

"This year is completely about upskilling people to use GenAI for telcos."
– Assistant Vice President, Major CSP in APAC

About the report

The Nokia Threat Intelligence Report draws on operational insights from the NetGuard and Deepfield portfolios, real-world data 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 160 telecom security leaders worldwide, providing a nuanced, evidence-based view of the risks and responses shaping the sector.

Your next move starts here

Equip your network with intelligence that drives action. Understand how attackers operate, anticipate their moves, and harden your defenses. Begin building resilience now with the Nokia Threat Intelligence Report 2025.

Download the full report

Talk to Nokia security experts

NOKIA