

# AI and Automation in Telco Network Security:

## A New Era of Threat Detection & Response

Gaurav Kaushal

*Head – Telecom Business Applications*

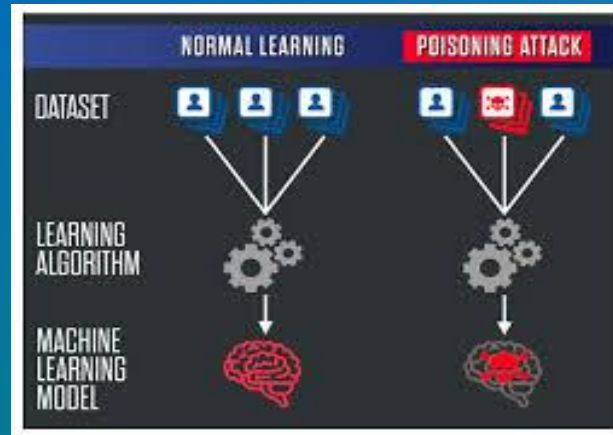
NOKIA

# AGENDA



1. Understanding what AI attacks are
2. Top drivers of cyber risks for Telecom Networks
3. Snapshot of the current telecom cyber battleground
4. Securing Telecom Infrastructure
5. How Nokia can help CSPs

# AI and attack vectors



**SOPHISTICATION**



**Attack Surface**

# Top drivers of cyber risks for telecom networks



**Nation-state actors** threaten mission-critical communications, risking operational continuity



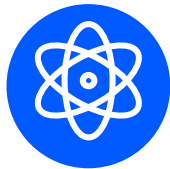
A movement to **cloud-native architectures** with new operational processes and practices



**Governments and new regulations** are imposing stringent directives for critical infrastructure providers



The rise of **Generative AI** enables attackers to increase the speed, scale, and sophistication of their attacks

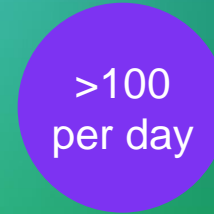


**Quantum computing** enables "harvest now, decrypt later," endangering encrypted data



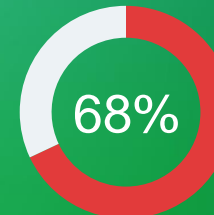
Average cost of **data breach** globally

In 2024, the global average cost of a data breach hit a record \$4.88 million. In the U.S., this figure is nearly double the global average, \$9.36 million.



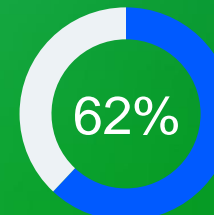
**DDoS attack** frequency surges

DDoS attack frequency has skyrocketed, increasing from 1-2 incidents daily to over 100 per day in many networks.



**Human element** drives breaches

The human element remains a critical factor, contributing to 68% of breaches. This includes errors, phishing, and misuse.



**Ransomware and extortion** lead financial cybercrime


62% of financially driven incidents involved ransomware or extortion, with a median loss of \$46,000 per breach.

# Snapshot of the current telecom cyber battleground




**Salt Typhoon** (October 2024, USA)

- **Motivation:** Espionage, geopolitical advantage.
- **Attack type:** APT, long-term infiltration, data exfiltration.
- **Impact:** Sensitive data at risk, triggered FBI investigations.
- **Remediation:** Endpoint monitoring, patch management, detect evasion tactics.



**AT&T Data Breach** (April 2024, USA)

- **Motivation:** Financial exploitation, data theft.
- **Attack type:** Data breach, exposure of sensitive customer info.
- **Impact:** \$370K ransom paid; 109M customers' data leaked.
- **Remediation:** Access control and least privilege, encryption, security audits.




**Orange Insider Compromise** (January 2024, Spain)

- **Motivation:** Financial and operational disruption.
- **Attack type:** Stolen employee credentials, Raccoon-type infostealer malware.
- **Impact:** Outages, recovery expenses, penalties.
- **Remediation:** EDR for malware detection, MFA, password hygiene, PAM.



**NTT Docomo DDoS Attack** (January 2025, Japan)

- **Motivation:** Disruption of telco services.
- **Attack type:** DDoS attack causing network congestion.
- **Impact:** ~12-hour service disruption affecting key platforms (web portal, video streaming, billing, golf-round services).
- **Remediation:** XDR for visibility, DDoS mitigation, improved traffic filtering.



**Sandworm/KillNet** (December 2023, Ukraine)

- **Motivation:** Political disruption.
- **Attack type:** Insider account exploitation, zero-day wiper malware.
- **Impact:** 24M users lost Internet access, damaged infrastructure, financial losses.
- **Remediation:** UEBA, security audits, strong access controls, incident response.

# Attack Objectives /Telecom Crown Jewels

## What Adversaries seek in Telecom networks?

### Charging Data Records (CDR) data

- Who called whom? What is subs geo location?
- Which devices are the individuals using?



### Signaling traffic

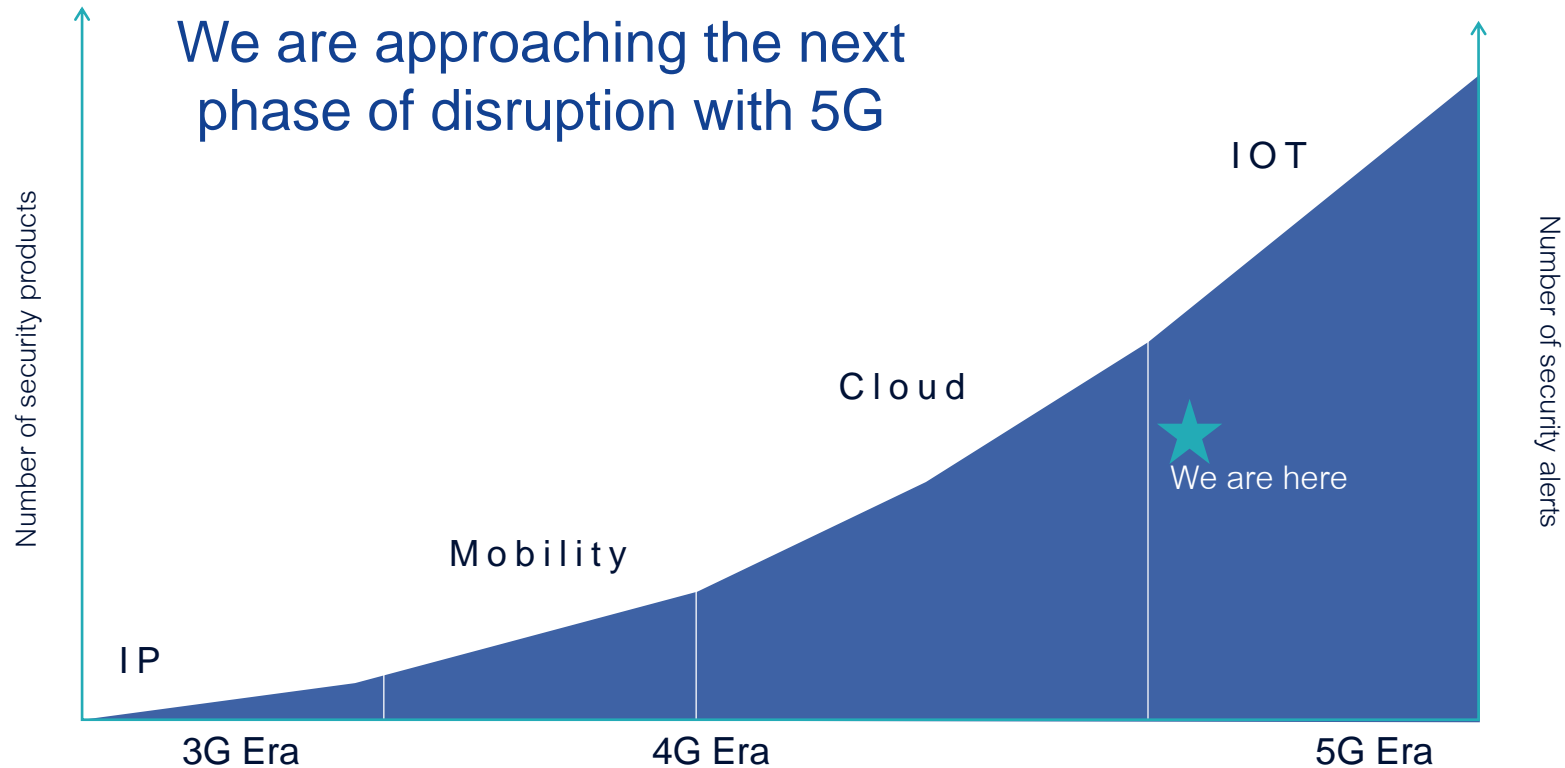
- VIP/dissidents, undercover agents location tracking
- SMS (2FA!) redirection
- Infiltration/impersonation

### Other

- Ransom
- Inflict communication damage (wipers)
- IMEI and IMSI (4 sim swap)
- Cyberespionage/Technology Theft
- Computing power stealing (crypto currency mining)
- Pivoting to more secure networks (eg national regulators)

# Why aren't threats detected?

Security personnel are drowning from a deluge of data



Sources: Ponemon, Cisco, HPE, ESG

- Security becomes unmanageable by conventional means
- Security Operations Must become Adaptive & Automated
- Only 30% of alerts are investigated
- 72% of investigated alerts are false
- 54% of legitimate alerts are not remediated
- 53% of time is spent on detection

# Securing Telecom Infrastructure

## Lessons from recent attacks



Advanced threat detection (XDR, EDR)

Correlate alerts across systems to detect LotL tactics, lateral movement, and malware



Privileged access management

Enforce strict access controls for privileged accounts and lawful interception tools



Certificate & key management

Rotate, revoke, and audit certificates to block misuse and mitigate MITM risks



Security consulting & collaboration

Leverage telecom threat intelligence, conduct assessments and follow CISA/NSA guidelines

AI

Advanced automation



Security observability

Network topology aware



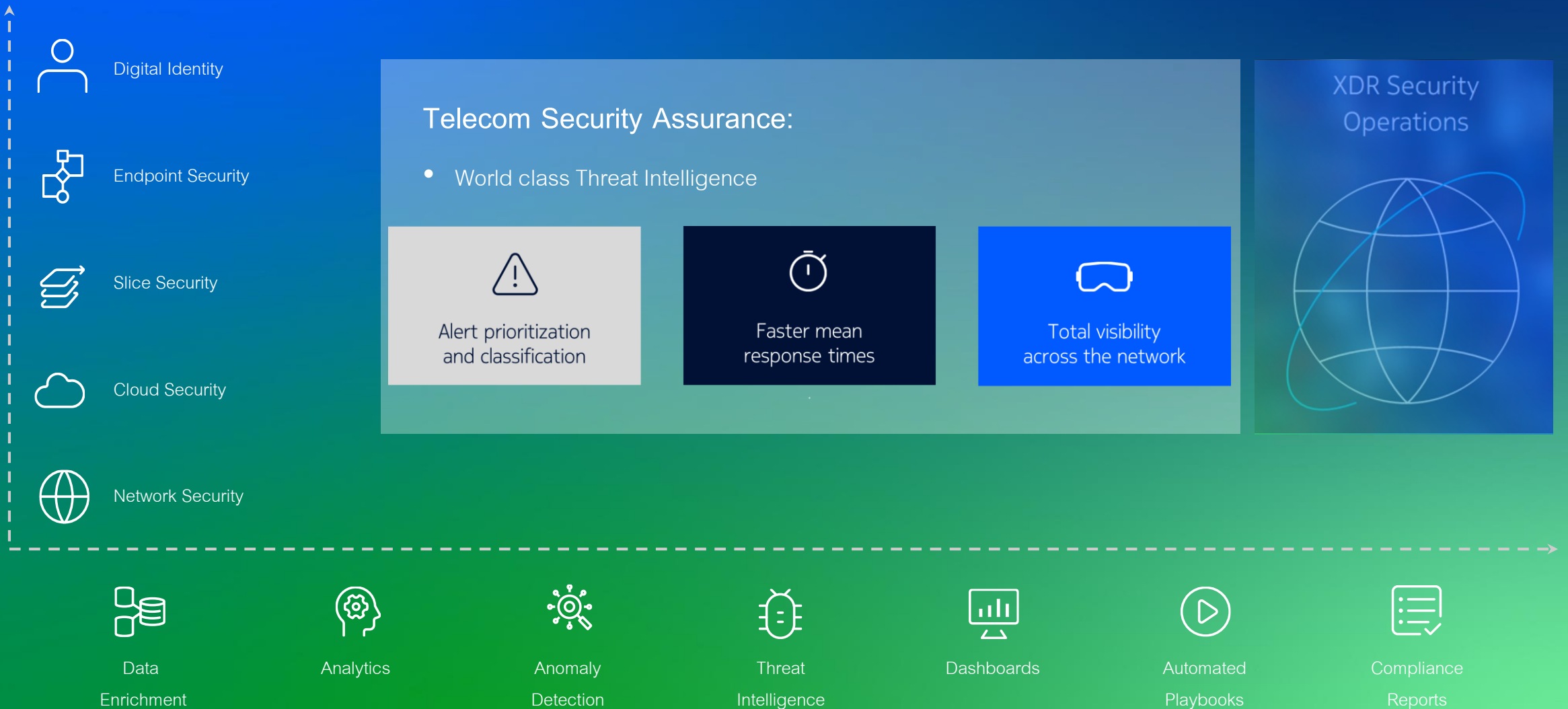
Telecom use cases

Threat scoring





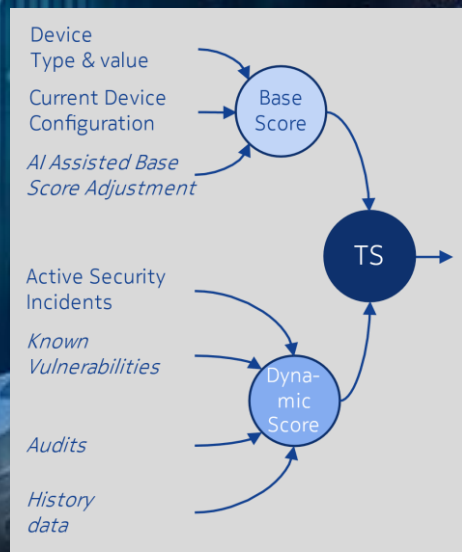
# The security functions at the heart of a trusted CSP network



# Nokia CyberSecurity Dome (NCYD) – XDR Platform

Gen AI based XDR platform for security observability and incident Lifecycle management

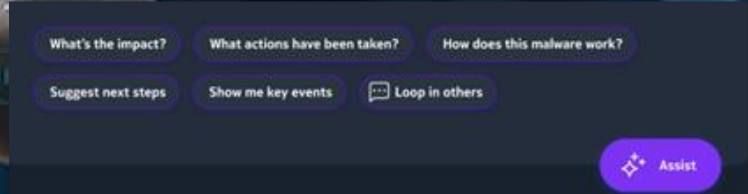
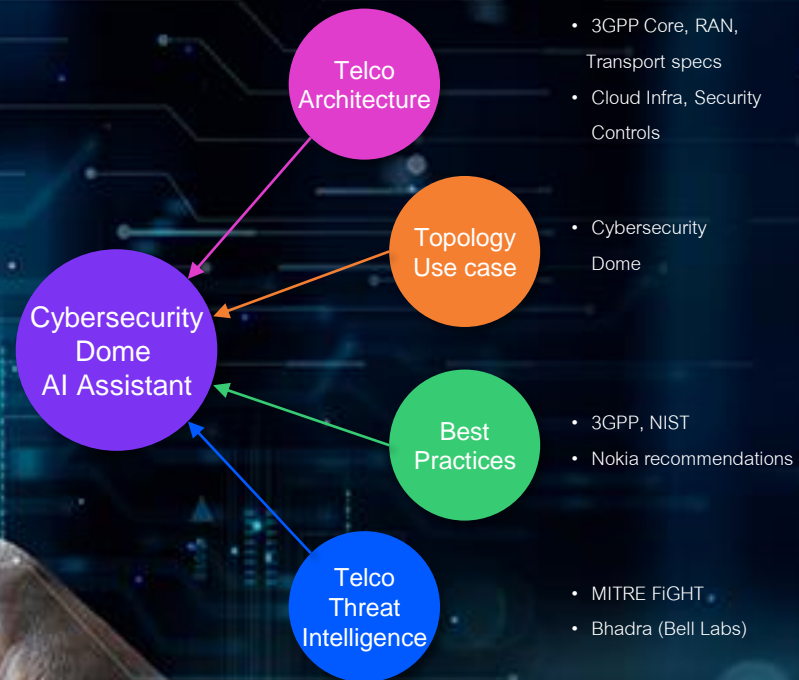
- XDR Platform ( incl. SOAR, SIEM & Threat Intel)
- AI/ML based Threat Scoring for Users and Network Elements
- Gen AI SOC analyst assistant trained in Telco Stds
- Network Topology aware
- Ready use case catalog for Telco Security Assurance
- SaaS and Open development Ecosystem



Threat score

**Meaning**  
A measure for the likelihood of a network function to being the victim of a successful damaging attack

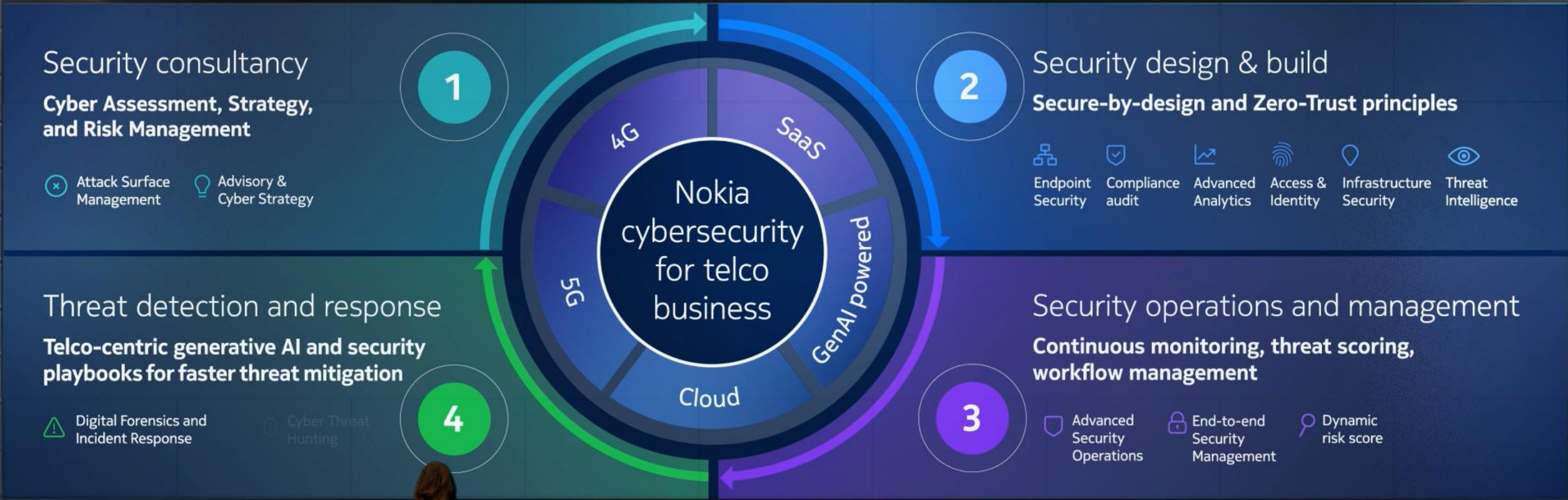
**Purpose**  
Prioritize actions of the system operator and trigger (automated) actions when appropriate



**Gen AI Assistant Features**

- Smart Summary
- IoC / IoA Analysis
- Chat: Guided Resolution
- Chat: Report Generation

# Nokia Security helps you in all phases to protect your network



NOKIA