

ENHANCING THE PROTECTION OF NEXT GENERATION NETWORKS WITH GENERATIVE AI

Whitepaper

December 2025



The Global Cybersecurity Forum (GCF) is a global, non-profit organization that seeks to strengthen global cyber resilience by advancing international multi-stakeholder collaboration, purposeful dialogue, and impactful initiatives. It serves as a platform where the world's cybersecurity stakeholders exchange knowledge and collaborate in tackling critical issues around Cyberspace.

GCF aims to catalyze socioeconomic change, push the boundaries of knowledge on critical cybersecurity topics and build the foundations for global co-operation on key challenges and opportunities in Cyberspace. By uniting decision makers and thought leaders from around the world, GCF aligns with international efforts to build a safe and resilient Cyberspace that is an enabler of prosperity for all nations and communities.



stc, as the leader in ICT services in the Middle East, has grown beyond telecommunications to connect the world, enrich lives, and drive digital transformation. Through world-class infrastructure, emerging technologies, and a strong commitment to sustainability, stc empowers communities, businesses, and industries in Saudi Arabia, the region, and beyond. stc's investments are pivotal in establishing Saudi Arabia as a major digital hub, enabling the digital ambitions that are redefining industries and enhancing lives in society. Guided by its values of drive, devotion, and dynamism, stc addresses environmental and social challenges while upholding strong governance, ensuring a secure, sustainable, equitable, and digitally empowered future for all.



Foreword



Mazen Alahmadi

stc;
Chairman of the 'Safeguarding
Future Networks and Emerging
Technologies' Knowledge Community

As we progress towards an advanced digital future, it is critical to ensure that the mobile infrastructure we rely on is secure and resilient.

We aim to spark a global policy discussion on protecting the often-overlooked layer of mobile signaling before threats outpace our ability to respond.

I would like to thank all our contributors for their expert and valuable input to this work. It is through the inclusion of diverse experiences that we can ensure our interconnected world is built on trust and openness.

Authors

- **Vinod Nair**, Nokia
- **Thomas Foerster**, Nokia
- **Joern Mewes**, Nokia

Contributors

- **Zaki Alowini**, stc
- **Nauman Khan**, stc
- **Abdulmajeed Aleid**, stc
- **Islam R. Swelam**, stc
- **Abdulrazzak, A. Shaikh**, stc
- **Mohammed Y. Uddin**, stc
- **Abdulaziz Hameda**, stc
- **Khalid Aljuhani**, stc
- **Mohammed Tawfik**, stc
- **Malak Almutairi**, sirar by stc
- **Adil A. Mirza**, Aujas
- **Rashad Bakleh**, Cellusys
- **Saad Abu Hlayel**, Orange
- **Yousef Alkhulaif**, Netwitness
- **Cu Nguyen**, POST Luxembourg
- **José Sobreira Martins**, Unitel

Knowledge Community: Safeguarding Future Networks & Emerging Technologies

In an increasingly interconnected world, the evolution of next generation ICT technologies such as 6G wireless technology has emerged as a powerful catalyst. The profound implications and transformative power of this next wave of ICT technologies demand immediate attention – both to navigate its complexities and to harness its capabilities for the benefit of society. The Knowledge Community 'Safeguarding Future Networks & Emerging

Technologies' is committed to promoting and safeguarding today's ICT networks, bringing together a diverse array of expertise from multiple stakeholder groups. The community welcomes ICT providers, telecom companies, telecom industry players, cybersecurity research organizations, infrastructure operators, reputable think tanks, academia, and all stakeholders with a vested interest in the security of ICT networks.

Contents

| | |
|--|-----------|
| Foreword | |
| Useful Acronyms | 05 |
| Executive Summary | 09 |
| Introduction | 10 |
| Methodology | 11 |
| Key Findings | 11 |
| 1. The Signaling Domain | 12 |
| 1.1 The signaling threat landscape | 12 |
| 1.2 SS7, Diameter and GTP vulnerabilities | 14 |
| 1.3 5G roaming vulnerabilities | 16 |
| 1.4 SIP vulnerabilities | 17 |
| 2. Using Gen AI For Defense | 19 |
| 2.1 Industry perspectives | 21 |
| 2.2 Use case 1: Accelerating SOC operations | 23 |
| 2.3 Use case 2: Proactive threat hunting | 27 |
| 2.4 Use case 3: Self-defending autonomous networks | 31 |
| 2.5 Gen AI safety and governance | 34 |
| 2.5.1 Responsible and ethical AI | 34 |
| 2.5.2 Regulatory compliance | 36 |
| 2.6 Enablers for AI-driven telecom security | 38 |
| 2.6.1 High-quality data pipelines | 38 |
| 2.6.2 Real-time network observability | 38 |
| 2.6.3 Purpose-built AI/ML models | 39 |
| 3. Conclusion | 40 |
| 4. Recommendations | 41 |
| Endnotes | 42 |
| Bibliography | 44 |

Disclaimer

This document has been published by the Global Cybersecurity Forum (GCF) in collaboration with Knowledge Partners as part of their efforts to promote thought leadership in cybersecurity. While GCF and the knowledge partners have made every effort to ensure the accuracy and reliability of the information provided, neither party assumes any responsibility for errors, omissions, or inconsistencies in the content, nor for any consequences arising from its use or interpretation. The content is provided for general information purposes and may be subject to change without prior notice at the discretion of GCF. This publication is protected by copyright law. No part of this report may be reproduced, distributed, or transmitted in any form or by any means—whether electronic or mechanical—without prior written permission from both GCF and the Knowledge Partners. All requests for such permissions should be directed to KC@GCFForum.org.

Useful Acronyms

| Abbreviation | Definition |
|--------------|--|
| AI | Artificial Intelligence |
| AMF | Access and Mobility management Function |
| API | Application Programming Interface |
| C2 | Command and Control |
| CAMEL | Customized Applications for Mobile networks Enhanced Logic (see SS7) |
| CNF | Containerized Network Function |
| CSP | Communications Service Provider |
| DDOS | Distributed Denial Of Service |
| DL | Deep Learning |
| DNS | Domain Name Server |
| DOS | Denial Of Service |
| EDR | Endpoint Detection and Response |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| Gen AI | Generative Artificial Intelligence |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| GRX | GPRS Roaming Exchange |
| GSMA | Global System for Mobile Communications Association |
| GT | Global Title |
| GTP | GPRS Tunneling Protocol |
| GTP-C | GTP Control Plane |
| GTP-U | GTP User Plane |
| GTPDOOR | Telecom-Oriented Malware Exploiting GTP |
| HLR | Home Location Register |
| HPLMN | Home Public Land Mobile Network |
| HSS | Home Subscriber Server |
| HTTP/2 | Hypertext Transfer Protocol Version 2 |
| IoA | Indicators of Attack |
| IoC | Indicators of Compromise |
| IoT | Internet of Things |
| I-SBC | Interconnect Session Border Controller |
| IMS | IP Multimedia Subsystem |

Useful Acronyms

| Abbreviation | Definition |
|--------------|--|
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| IPSEC | Internet Protocol Security |
| IPX | Internet Protocol Exchange |
| I-SBC | Interconnect Session Border ControllerLogic (see SS7) |
| ISDN | Integrated Services Digital Network |
| ISUP | ISDN User Part |
| JIT | Just-In-Time |
| JSON | JavaScript Object Notation |
| JWE | JSON Web Encryption (RFC 7516) |
| LLM | Large Language Model |
| LTE | Long-Term Evolution (wireless broadband communication standard) |
| MAP | Mobile Application Part (SS7 messages) |
| MiTM | Man-in-The- Middle |
| ML | Machine Learning |
| MME | Mobile Management Entity |
| MNO | Mobile Network Operator |
| MSC | Mobile Switching Center |
| MVNO | Mobile Virtual Network Operator |
| NDMO | National Data Management Office |
| NE | Network Element |
| NEF | Network Exposure Function |
| NIST | National Institute of Standards and Technology |
| NF | Network Function |
| NRF | Network Repository Function |
| NSSAAF | Network Slice-Specific Authentication and Authorization Function |
| NGN | Next Generation Network |
| OAM | Operations, Administration and Management |
| OAuth | Open Authorization |
| OWASP | Open Worldwide Application Security Project |
| PAM | Privileged Access Management |
| PDPL | Personal Data Protection Law |
| PII | Personally Identifiable Information |

Useful Acronyms

| Abbreviation | Definition |
|--------------|---|
| P(L)MN | Public (Land) Mobile Network |
| PRINS | Protocol for N32 Interconnect Security |
| P-CSCF | Proxy Call Session Control Function |
| P-GW | Packet Data Network Gateway |
| RAG | Retrieval Augmented Generation |
| RAN | Radio Access Network |
| REST | Representational State Transfer |
| RFC | Request For Comments |
| RTP | Real-Time Transport Protocol |
| SBA | Service-Based Architecture |
| SBC | Session Border Controller |
| S-CSCF | Serving Call Session Control Function(standard) |
| SDLC | Software Development Lifecycle |
| SEPP | Security Edge Protection Proxy |
| SGSN | Serving GPRS Support Node |
| SIP | Session Initiation Protocol |
| SIP-I | SIP with encapsulated ISUP |
| SIGTRAN | Signaling Transport |
| SMF | Session Management Function |
| SMS | Short Message Service |
| SMSF | SMS Function |
| SOC | Security Operations Center |
| SS7 | Signaling System 7 |
| STP | Signal Transfer Point |
| SUCI | Subscription Concealed IdentifierFunction |
| SUPI | Subscription Permanent Identifier |
| TDR | Transaction Data Record |
| TI | Threat Intelligence |
| TLS | Transport Layer Security |
| TTP | Tactics, Techniques and Procedures |
| UEBA | User Entity Behavior Analytics |
| UDM | Unified Data Management |
| UDR | Unified Data Repository |

Useful Acronyms

| Abbreviation | Definition |
|--------------|-------------------------------------|
| UE | User Equipment |
| UPF | User Plane Function |
| VAS | Value Added Services |
| VLR | Visitor Location Register |
| VNF | Virtualized Network Function |
| VoLTE | Voice Over LTE |
| VoIP | Voice over Internet Protocol |
| VPLMN | Visiting Public Land Mobile Network |
| VPMN | Visiting Public Mobile Network |
| VPN | Virtual Private Network |
| XDR | Extended Detection and Response |

Executive Summary

Attackers are now using generative artificial intelligence (Gen AI) to launch faster, more advanced cyberattacks on telecom networks. Nokia's Threat Intelligence Report 2024¹, for example, highlights AI-powered botnets² that rapidly shift distributed denial of service (DDoS) tactics and targets, posing a serious threat to critical telecom infrastructure. Even low-skilled actors can exploit complex telecom protocols using AI-generated code.

This whitepaper focuses on leveraging Gen AI³ to enhance the security of next generation networks (NGN) in the telecom signaling domain. The paper highlights the increasing sophistication of cyberattacks powered by AI and the vulnerabilities of legacy telecom protocols such as SS7, Diameter, and the GPRS Tunneling Protocol (GTP), as well as outlining how Gen AI can address these challenges by enabling proactive threat detection, automating security operations, and reducing reliance on human expertise.

The paper is structured around the following key areas:

1. The threat landscape: The vulnerabilities in signaling protocols and the evolution of AI-powered attacks are explained.

2. Use cases for Gen AI: Gen AI's application in security operations centers (SOCs), threat hunting, and in defending autonomous networks is demonstrated.

3. Technical enablers: The importance of high-quality data pipelines is discussed, along with real-time observability and purpose-built artificial intelligence (AI)/machine learning (ML) models.

4. Safety and governance: The importance of responsible AI practices, regulatory compliance, and mitigating risks – such as bias, data poisoning, and hallucinations – is highlighted.

5. Recommendations: An AI-first approach to telecom security is advocated, integrating Gen AI with threat intelligence and extended detection and response (XDR) systems.

Introduction

Signaling protocols such as Signaling System 7 (SS7), Diameter, GTP and the session initiation protocol (SIP)⁴ form the backbone of global roaming. These were designed, however, for closed and trusted environments – conditions that no longer exist. Yet, despite known vulnerabilities, protocols like SS7 still dominate interconnectivity, posing major security risks in today’s open networks.

Key security challenges in signaling include:

- **Limited human expertise:** Detecting threats in signaling traffic requires deep knowledge of protocol behavior and call flows. Skilled professionals in this domain are scarce.
- **Firewall limitations:** Traditional signaling firewalls offer only perimeter-based controls without deep analytics or behavioral context. They fall short against sophisticated or low-and-slow attacks.
- **Reactive rule-based defense:** Current models rely heavily on static rules, which are typically created after an attack has occurred. A more proactive approach is needed – one that integrates real-time threat intelligence and automation.

- **Poor observability:** High-fidelity visibility into signaling traffic is rare. A complete view requires data from firewalls, core virtualized network functions (VNFs), and/or containerized network functions (CNFs)⁵ and other layers. This data is massive and demands efficient storage, processing, and correlation.
- **A complex ecosystem and false positives:** The roaming chain involves mobile virtual network operators (MVNOs)⁶, aggregators, global title (GT) leasing⁷, and other entities that can trigger false alerts. A context-aware security solution is needed to accurately interpret such scenarios.
- **Lack of signaling threat intelligence:** High-quality threat intelligence is difficult to come by, since signaling security is a very telecom-specific concern.
- **Revenue and experience impact:** Roaming is a significant revenue stream for operators. Mismanaged signaling threats can degrade service or cause outages, negatively impacting both revenue and customer satisfaction. Relying solely on brute-force firewall rules is insufficient.



Methodology

In this whitepaper, we analyze these challenges in terms of the following use-case scenarios:

- **SOC teams:** These are state-of-the-art for many operators, which rely on internal or external/outsourced SOC teams to respond reactively to security threats against the network infrastructure.
- **Threat hunting teams:** These represent more advanced operators who proactively hunt in the wild for new and emerging threats.

- **Autonomous networks:** These represent the evolution of the NGN itself.

The analysis below was conducted by reviewing 35 related publications in order to identify one domain (signaling) and seven key gaps in cybersecurity for telecom networks. The scenarios analyzed included: 1) vulnerabilities in signaling protocols (SS7, Diameter, GTP, and SIP); 2) the impact of Gen AI in enabling complex attacks; and 3) the risks posed to critical infrastructure by state-sponsored attacks and AI-powered botnets.

Key Findings

Operators of mission-critical networks need to pivot towards leveraging Gen AI-powered tools as a foundational element of their security defenses. Given the speed at which Gen AI technology is evolving, continuing to rely solely on human-driven security operations to counter attackers will not scale quickly enough, leaving networks exposed.

A multi-pronged approach based on the following pillars is therefore required:

- **Leverage Gen AI-powered SOC assistants to augment the capabilities and knowledge of the security operations analysts, addressing both skills gaps and scalability.**

- **Leverage Gen AI-powered threat-hunting tools together with threat intelligence as an early warning system for new and emerging threats, containing them before they become too widespread across the network.**
- **Drive network vendors to build Gen AI-powered self-defense into the fabric of the network itself, as part of the journey towards Level 4 autonomy. This lessens dependency on human analysts and security operations teams.**
- **Ensure high-quality data pipelines and observability across the network to feed Gen AI models with relevant, real-time, and trustworthy data.**

1. Signaling Domain

Signaling is the fundamental communication mechanism within telecommunication networks. It enables the exchange of the control information that is necessary to establish connections, manage services, and ensure subscriber mobility. Signaling acts as the network's nervous system, orchestrating functions from call set-up to data session management.

The roaming signaling domain extends this complexity significantly, as it involves the intricate coordination of signaling messages between a subscriber's home network and a visited network. This domain requires robust frameworks, including commercial agreements and technical interconnections.

This ensures seamless service delivery and billing across different operators and geographical boundaries; it also makes interoperability and security critical for global mobile connectivity.

The ability to roam seamlessly across countries and operators has always been a fundamental expectation for mobile subscribers – and an important source of revenue for providers.

Now, with the rapid proliferation of cellular, internet-of-things (IoT) devices, and the global asset tracking requirements of modern supply-chain management systems, ensuring the security of the underlying signaling infrastructure supporting roaming becomes even more critical.

1.1 The signaling threat landscape

The signaling domain is critical for telecommunication network operations. It also faces a diverse and significant threat landscape that can compromise service integrity, subscriber privacy, and financial stability.

Attacks range from spam and spoofing – which exploit unauthenticated identifiers and routing mechanisms to evade billing or send malicious bulk messages – to more sophisticated threats like location tracking, which enables adversaries to pinpoint subscriber locations for further exploitation. In addition, subscriber fraud allows attackers to manipulate profiles or trigger malicious charging, leading to theft of credit or alteration of service plans. Intercept attacks, meanwhile, can eavesdrop on or alter communications, including SMS used for two-factor

authentication. Denial-of-service (DOS) attacks aim to disrupt network availability for individuals or entire regions, while routing attacks and infiltration attacks leverage vulnerabilities in packet-based interconnects and misconfigurations to gain unauthorized access to core network elements. This potentially leads to data theft, unauthorized access to sensitive assets, and widespread service disruption.

Threat modeling frameworks, such as the specialized MITRE FIGHT⁸ for telecommunications signaling and broader models like MITRE ATT&CK, play a crucial role in understanding and defending against cyber threats. As Table 1 shows, they do this by systematically cataloging adversary behavior into tactics, techniques, and procedures (TTPs).

Table 1. Most common categories of signaling attacks (Source: ENISA)

| Type of attack | Description | Potential impact |
|---|---|---|
| Signaling flood (SMS) | This is a type of DDOS attack using the SMS channel. The attacker sends a large number of SMS messages to one or more destinations. The messages may be either valid or invalid. | Saturate network infrastructure (control channel). Overwhelm targeted subscribers or IoT devices. |
| Cross-protocol exploits ^{9,10} | Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control (C2) communications. This can involve, for example, GTP, SIGTRAN ¹¹ , or external domain name server (DNS) protocols. An example of this is the LightBasin GTPDoor attack that used GTP as a backdoor to bypass telecom firewalls. | Data exfiltration. |
| Man-in-the-middle (MiTM) attacks on signaling links ¹² | An adversary may act as a MiTM between two mobile network operators that are connected over an internet protocol (IP) exchange (IPX) network through which the roaming traffic flows. In this scenario, the adversary acquires an MiTM position on the IPX network via the public land mobile network (PLMN) – either via the home PLMN (HPLMN), or the visited PLMN (VPLMN). By providing fraudulent signaling information to the HPLMN the adversary can collect data about roaming subscribers. | Network traffic sniffing/ exfiltration and manipulation of the transmitted data. |
| GT leasing abuse | GTs can be leased out by operators and are generally used by legitimate businesses to offer mobile services. However, they can also be used by attackers to stage signaling related exploits. The United Kingdom's Office of Communications, for example, regards several services performed by leased GTs (such as home location register [HLR] lookups) as higher risk and is moving to ban the GT leasing practice altogether. Many operators worldwide, however, support GT leasing. Effective threat intelligence is an important ingredient in defending against these types of attacks. | Interception of SMS messages and calls. |
| Weakening signaling encryption ¹³ | An adversary with control over roaming nodes or interfaces (security edge protection policy [SEPP] or IPX network) may disable or force usage of a weak encryption algorithm for transport layer security (TLS) or JavaScript object notation (JSON) web encryption (JWE) on the N32 interface. An adversary with control over a visited network user plane function (UPF) may disable IPsec on the N9 interface, or a compromised mobile management entity (MME) or access and mobility management function (AMF) may disable IPsec on the N26 interface. | Eavesdropping on signaling traffic. |

1.2 SS7, Diameter, and GTP vulnerabilities

SS7, Diameter, and GTP currently have the lion's share of inter-operator signaling traffic, accounting for around 90% of the

total between them. Figure 1, below, illustrates the pattern of high-level roaming.

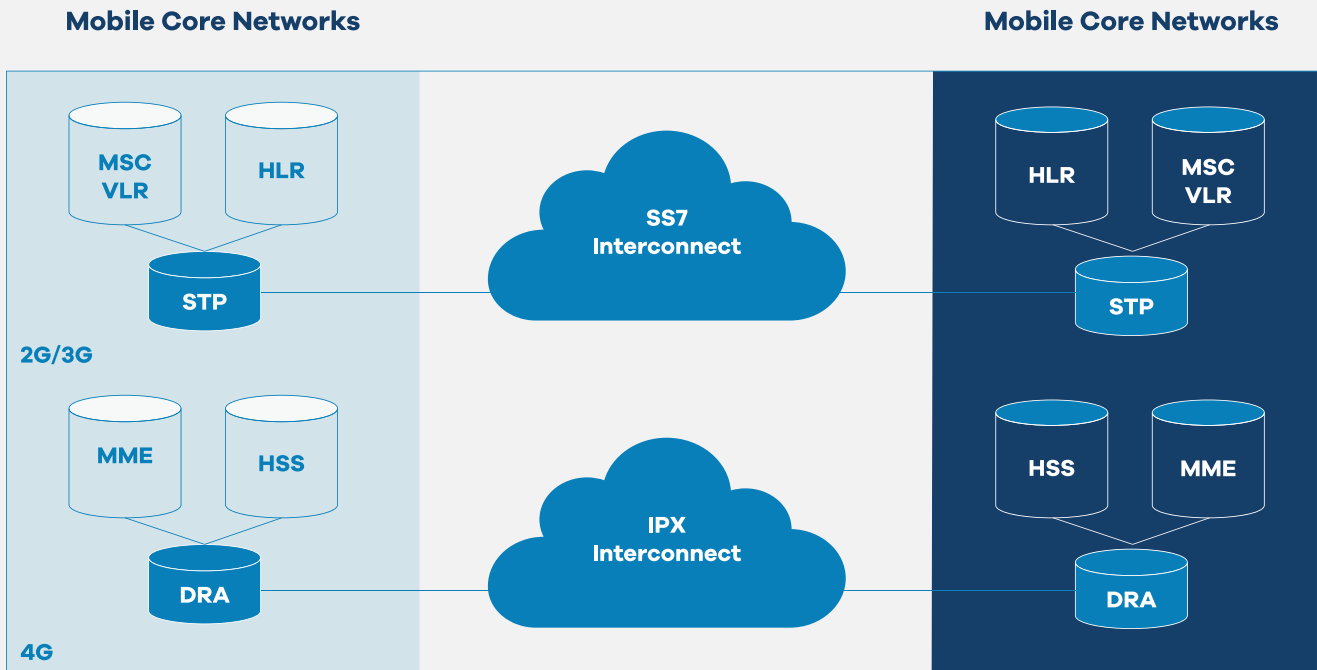


Figure 1: Interconnecting mobile networks with SS7 and Diameter

Note: MSC = mobile switching center; VLR = visitor location register; STP = signal transfer point; HSS = home subscriber server; DRA = diameter routing agent.

Source: ENISA

Unfortunately, these older protocols also have significant security vulnerabilities. A recent example of these vulnerabilities is

shown in Figure 2, which describes the GTPDOOR telecom malware.¹⁴

Targeted MNO

Compromised MNO/Attackers Infrastructure

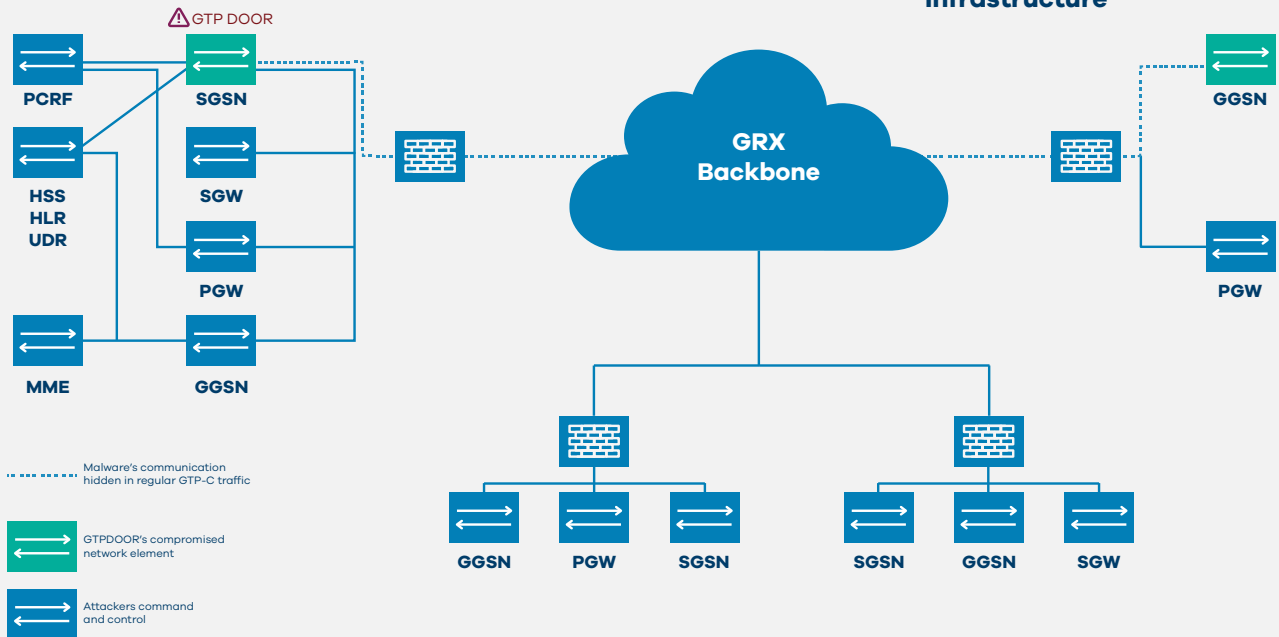


Figure 2: GTPDOOR enabling malicious communication through GTP-C traffic over GRX

Note: GTP-C = GTP control plane; GRX = GPRS roaming exchange; PCRF = policy and charging rules function; UDR = unified data repository; SGSN = serving GPRS support node; SGW = serving gateway; PGW = packet data network gateway; GGSN = gateway GPRS support node.

Sitting adjacent to a GRX network and using compromised malware planted on signaling nodes such as the SGSN, GGSN, and PGW, the malware hides its data transmissions inside normal GTP-C traffic. It can be deployed for intelligence collection operations targeting telecommunications companies, globally.

The Global System for Mobile Communications Association (GSMA) has provided some recommendations on how to address these issues.¹⁵ Their recommendations include:

- **Firewalls and/or static routes to/from STP (SS7) and DEA (Diameter)**
- **STP (SS7) and DEA (Diameter) to hide signaling network topology**
- **A signaling firewall for SS7, Diameter, GTP-C/U for traffic and message filtering**
- **An isolated IPX network and management interfaces, signaling firewalls, routing configurations and other instruments**

- **Detection and blocking of malicious signaling sources**
- **Security analytics for signaling traffic**

The first four items in this list only provide a level of perimeter defense, however. This has limitations, as can be seen in the GTPDOOR example, where the malware was planted on the signaling nodes and hid its traffic inside regular GTP-C traffic to become invisible to the firewall.

To effectively respond to these kinds of sophisticated and dynamically evolving threats – and to be able to contain them without “collateral damage” to subscriber experience and the roaming business mode – a combination of signaling threat intelligence (the fifth item on the above list) and Gen AI powered tools (the sixth item) are essential.

1.3 5G roaming vulnerabilities

Fifth generation (5G) mobile networks introduce many roaming security improvements. These include the use of hypertext transfer protocol version 2 (HTTP/2), TLS, JWE, and native

enforcement points, such as the secure edge protection proxy (SEPP). However, 5G is still not foolproof, as the GSMA has documented.¹⁶

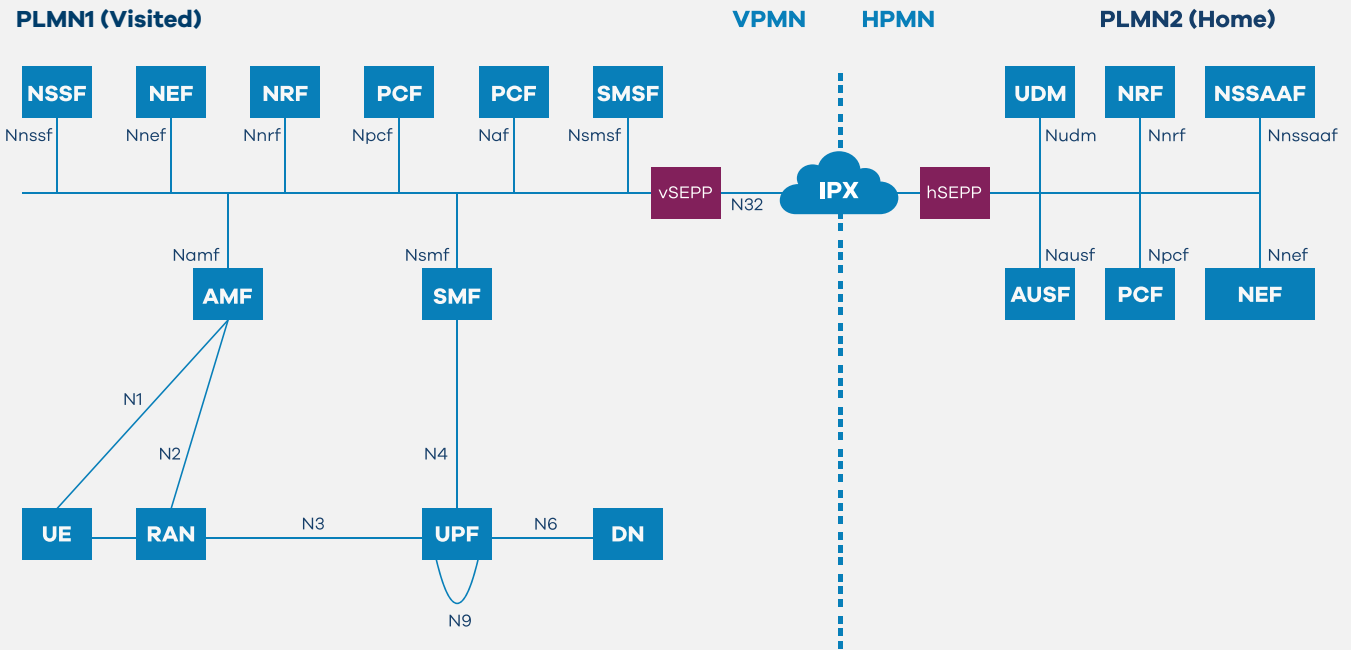


Figure 3: 5G roaming architecture with local breakout using service-based interfaces

Note: VPMN = virtual private mobile network; HPMN = home public mobile network; NSSF = network slice selection function; NEF = network exposure function; NRF = network repository function; PCF = policy control function; AF = authorization function; SMSF = SMS function; UDM = unified data management; NSSAAF = network slice-specific authentication and authorization function; SMF = session management function; AUSF = authentic server function; UE = user equipment; RAN = radio access network; DN = data network.

Source: GSMA

The N32 interface at the boundary of the two networks implements a representational state transfer (REST) interface and is vulnerable to attacks if not properly implemented and monitored. Risks can include: 1) a lack of input parameter validation on the REST application programming interfaces (APIs) that can give attackers access to data or execute actions via request modification; 2) broken access controls – open authorization (OAuth) – that compromise API safeguards; 3) DOS attacks on other network functions that are part of the 5G service based architecture (SBA); and 4) invalid or expired TLS certificates or JWE tokens resulting in sensitive data exposure, among others.

The Nnrf interface for the NRF¹⁷ (which supports service registration and

discovery) is another significant risk, since it is needed during inter-PLMN communication and can be targeted by attackers, if not properly secured by rules at each SEPP, along with monitoring.

A natural question is whether to focus only on legacy SS7/Diameter/GTP, or also include 5G with HTTP/2. The answer is: do both. Even as networks evolve, SS7 and Diameter still exist (for roaming, 2G/3G fallback, etc.), and GTP remains ubiquitous on the 4G/5G user-plane. Indeed, the GSMA guidelines emphasize that signaling monitoring must encompass all generations, as the coexistence of a variety of technologies raises concerns about cross-protocol attacks – concerns that can only be addressed by using a comprehensive approach.

1.4 SIP vulnerabilities

SIP is an application-layer control and signaling protocol used with VoIP¹⁸, rich communications services (RCS), SMS-over-IP, and other popular services. In mobile networks, these services are typically delivered on the Third Generation Partnership Project (3GPP) internet multimedia services (IMS) platform¹⁹ using

a SIP-based architecture. As documented by GSMA FS.38,²⁰ along with growing demand for these services, attackers are finding opportunities to exploit weaknesses in SIP. Signaling for both SIP access and the SIP interconnect between roaming service providers are vulnerable to attacks.

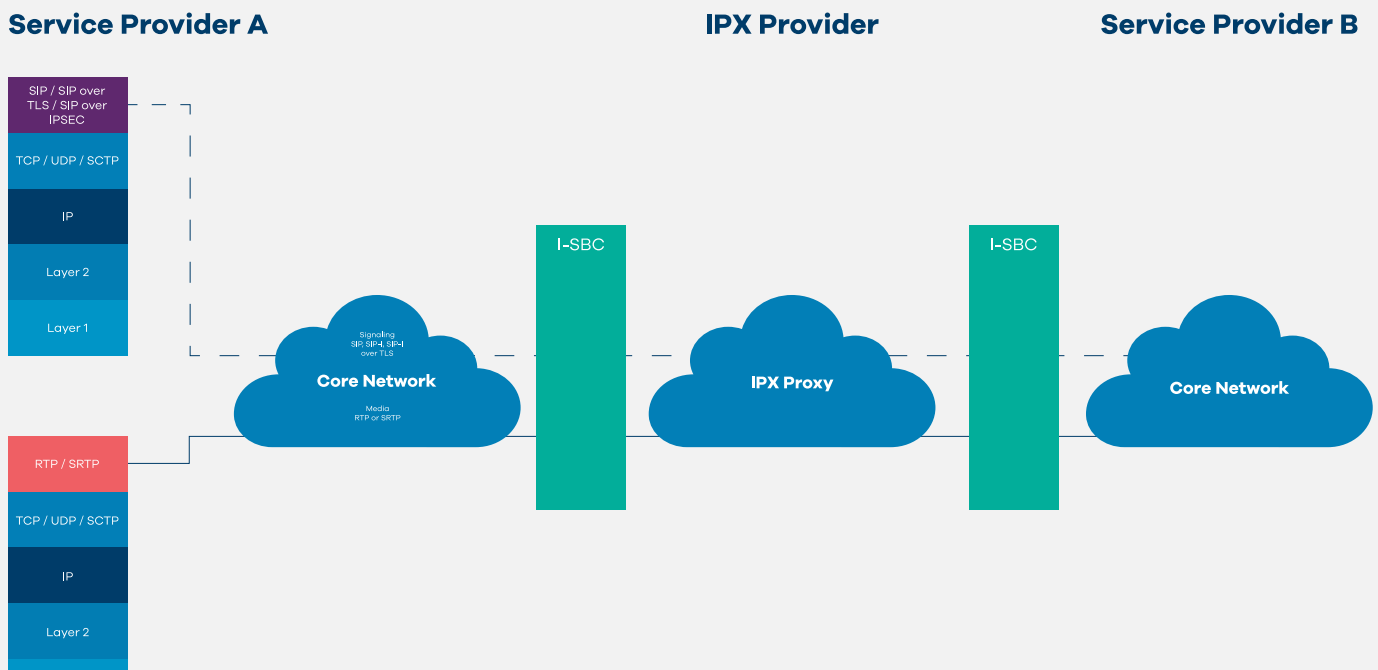


Figure 4: SIP interconnect between two service providers

Note: IPSEC = internet protocol security; UDP = user datagram protocol; SCTP = stream control transmission protocol; RTP = real-time transport protocol; SRTP = secure RTP; I-SBC = interconnect session border controller.

Source: GSMA

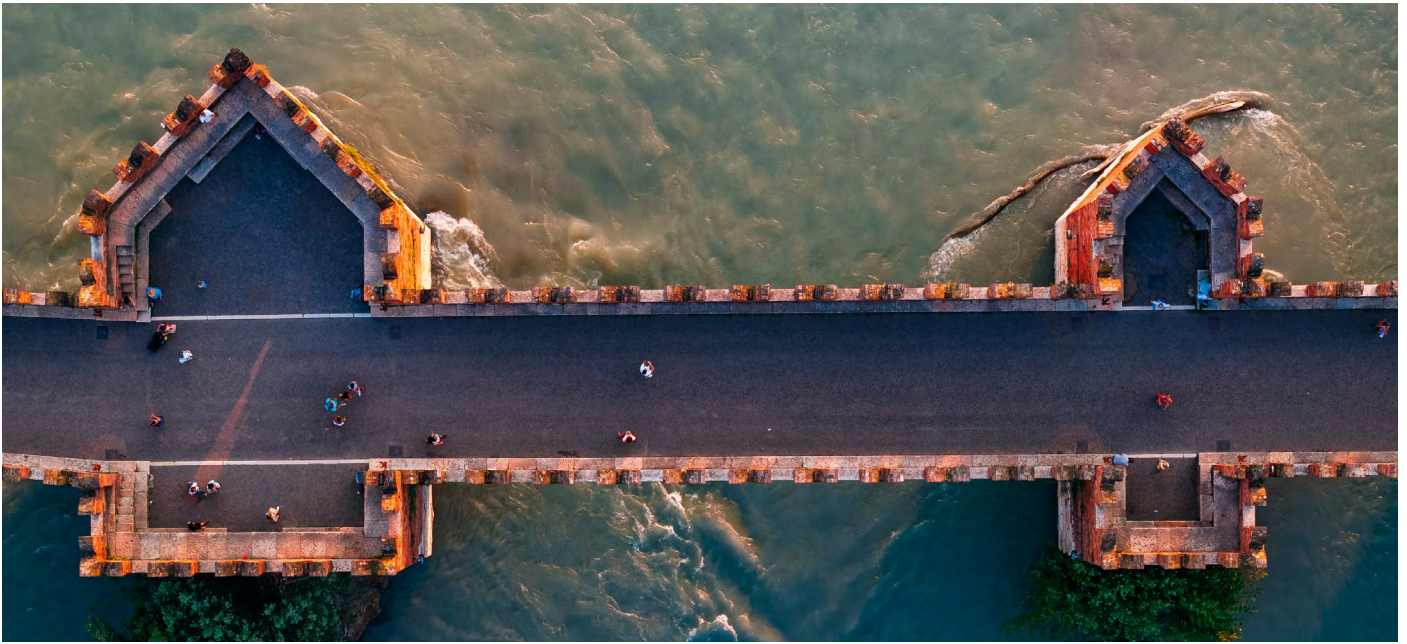
In the above diagram the SIP signaling traffic is shown in the upper part (dashes) and the SIP media traffic in the lower part (solid lines). The I-SBC²¹ is placed at the

connection point between the two networks and – when properly configured and monitored – can help protect both the signaling and media traffic.

Attacks may target either the SIP signaling or SIP media pathways. The varieties of attack include:

- **SIP footprinting:** Information is gathered about a target network, service or device. This may use techniques such as internet and DNS reconnaissance, SIP port scanning, SIP network fingerprinting, and SIP user identification (ID) enumeration
 - **SIP password cracking:** The discovery of the password for an SIP endpoint, which allows the attacker to register and respond to challenges to "Invite" and "Subscribe" messages. The end goal of the attacker can be to make fraudulent calls, or even to sell the information on the darknet
 - **Stealing SIP authentication details:** This is done to discover the SIP user ID, the IP address of the SIP outbound proxy (e.g., the access SBC), the transport type (UDP, TCS, TLS) and port number, certificates, and so on, in addition to the SIP password. This information can be gathered from a compromised database, a customer portal, an insider, a user device or network server, and be used to launch more serious attacks or initiate fraud
 - **Fraud attacks via SIP node or interconnect:** This can involve a compromised interconnect partner or IMS application server, which then initiates fraudulent calls or SMS messages
 - **SIP caller-ID spoofing attacks:** These may be used for telemarketing and robo-calling, but also for more serious illegal activities such as fraud, privacy violations, voicemail hacking or call flooding. Caller ID attacks are seen more often to originate from interconnect networks in which it is harder to perform SIP validation. Notable exploits include the Wangiri fraud,²² in which fake missed call messages are used to convince users to dial international premium rate numbers
 - **SIP DOS attacks:** These can be volumetric attacks that generate high volumes of traffic targeted at services like VoIP in order to cause slowness and disconnects
- Proper border protection controls at both SIP access and interconnect points, together with continuous monitoring and AI-powered threat analytics, are essential to managing SIP security.





2. Using Gen AI for Defense

Potentially, Gen AI technology can significantly enhance signaling security and defense against advanced attacks. It can do this by improving threat detection, automating responses and proactively identifying vulnerabilities through sophisticated data analysis and pattern recognition.

As shown in Figure 5, Gen AI's foundational technology uses machine learning algorithms to create content, including text, audio, video, speech, designs, and software codes.

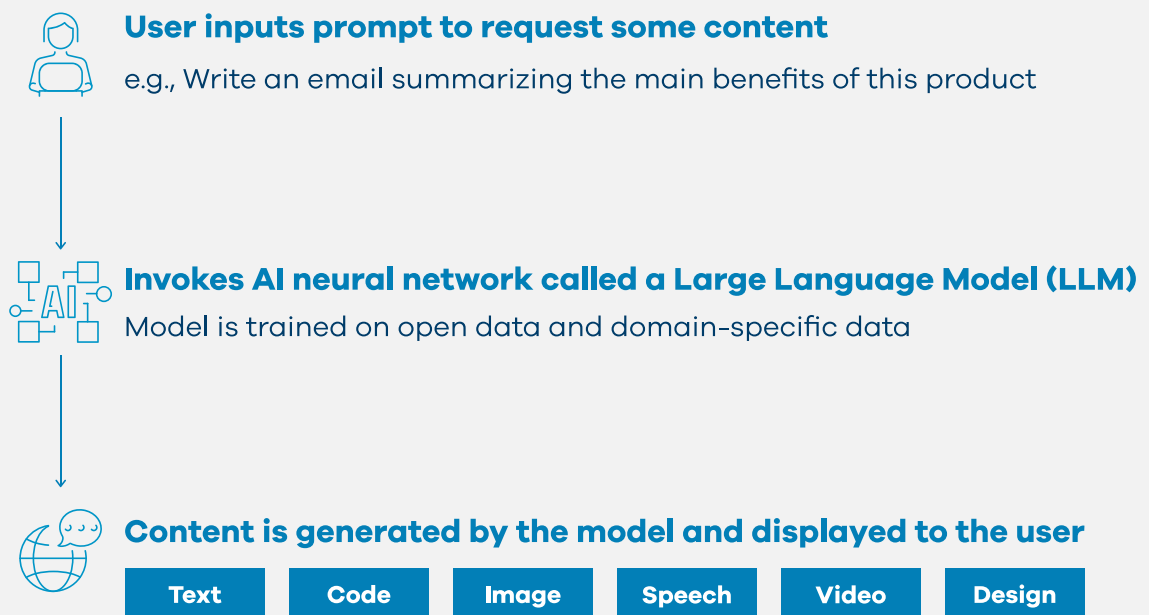


Figure 5: How Gen AI works

Source: Global Data

Large language models (LLMs) are the latest evolution of advanced neural networks. Once trained, LLMs can generate very precise output in response to prompts or questions from humans.

LLMs have a wide range of applications, including natural language processing, chatbots, summarization, language translation and more. Significant productivity gains are foreseen with the adoption of LLMs across organizations.

LLMs are artificial intelligence systems that use deep learning techniques to generate human-like text in natural language.

LLMs use several layers of neural networks and billions and sometimes trillions of parameters. These models are trained on massive amounts of data, such as books, articles and other sources. Reinforcement learning and other techniques are used to optimize model performance.

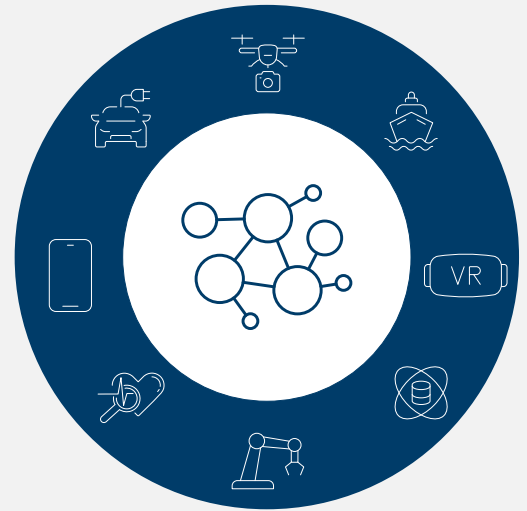


Figure 6: LLMs

In the telecommunications industry, Gen AI for offense is being increasingly leveraged by attackers, as it creates the ability to mount sophisticated attacks faster and at a larger scale. By using Gen AI, complex technology standards that were previously difficult to analyze and exploit are now within easy reach for even low-skilled attackers. Coupled with Gen AI's code-generation capabilities, this will result in a new level of attacks against mission-critical telecommunications infrastructure – one that could previously only be achieved by nation-states.

The same capabilities that empower attackers, however, also offer a powerful

new frontier for defense. Gen AI for defense can provide an essential counter-balance, enabling telecommunications operators to rapidly analyze vast amounts of network data, identify emerging attack patterns, and predict potential vulnerabilities with unprecedented speed and accuracy. This allows defenders to move beyond reactive measures, proactively strengthening critical infrastructure against the advanced, large-scale and rapidly evolving threats orchestrated by Gen AI-powered adversaries. This potentially levels the playing field even against attackers with nation state-level capabilities.

2.1 Industry perspectives

In an age of advanced threats and attackers armed with LLM technology, traditional security measures are no longer sufficient.

AI has the potential to transform cybersecurity by analyzing vast

datasets and identifying critical patterns. Its role in security is therefore essential, with Gen AI offering unique advantages in advanced threat detection, rapid incident response, and comprehensive security management.

Generative AI: Impact on network operations

How do you believe generative AI technologies will have the greatest impact on your network operations?

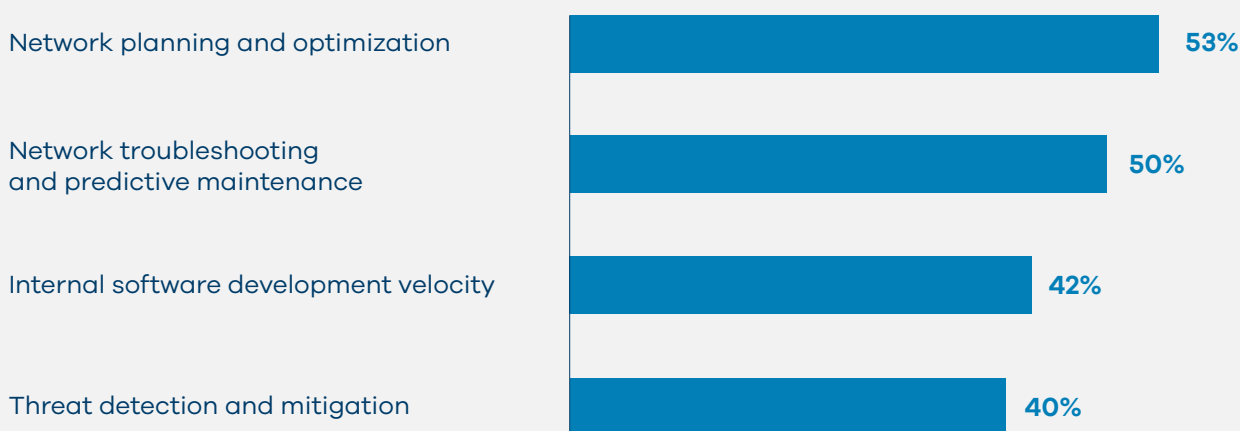


Figure 7: Top five Gen AI use cases for network operations

Source: GSMA

As Figure 7 shows, GSMA's 2024 **Network Transformation survey**²³ revealed that 40% of operators saw Gen AI as transformative because of its threat detection and mitigation capabilities. A further survey conducted that year by OMDIA²⁴ showed 69% of telecoms businesses were also already

incorporating Gen AI into their cybersecurity strategy (see Figure 8).

This highlights the perception of a clear need to efficiently identify and neutralize cyber threats with minimal human error.

Has your organization incorporated GenAI into its cybersecurity strategy?

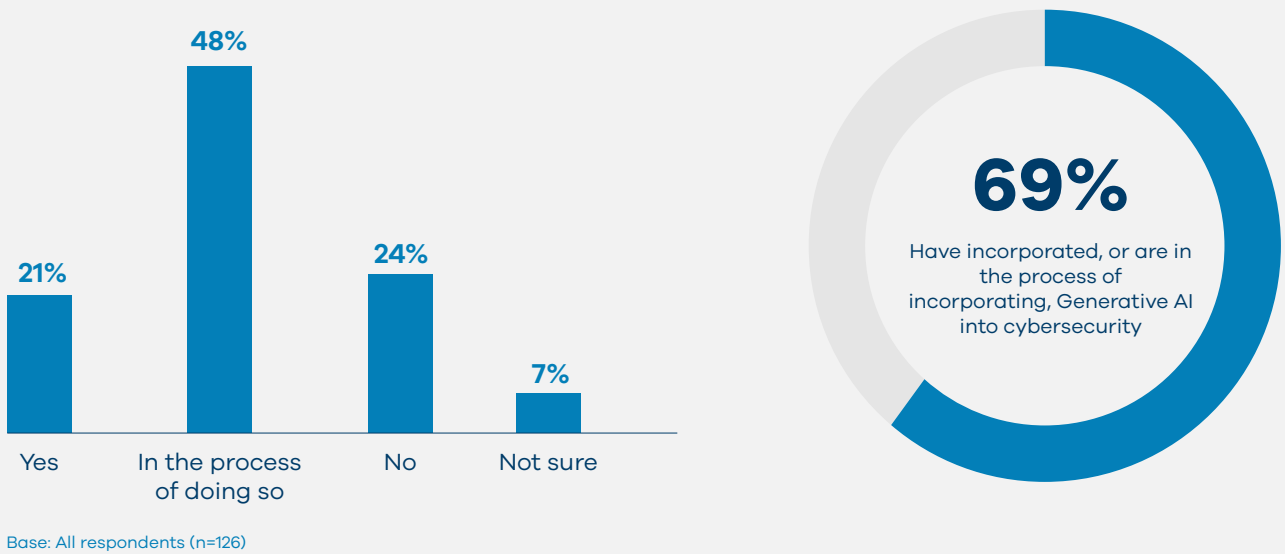


Figure 8: OMDIA survey of telecoms businesses

Source: OMDIA

Given the industry's growing recognition of Gen AI's transformative potential in cybersecurity, particularly for advanced threat detection and rapid incident response, it becomes imperative to examine how these capabilities can be applied to specific operational contexts.

While the general advantages of Gen AI are clear, the unique and complex SOC landscape in telecommunications

presents distinct challenges that traditional IT security approaches often fail to address. Understanding how Gen AI can be tailored to meet the specialized demands of telco SOCs is therefore crucial in accelerating their operations and effectively countering the sophisticated threats facing mission-critical telecoms infrastructure.



2.2 Use case 1: Accelerating SOC operations

As shown in Table 2, telecommunications SOC operations face fundamentally new challenges – ones that cannot be easily addressed by a traditional IT SOC.

Table 2. Differences between IT security and telecom security for SOC operations

| IT security | Telecom network security |
|---|--|
| Security priorities | |
| Avoid data thefts, ransomware, personally identifiable information (PII), etc. | Operational continuity of voice/data networks. |
| Components | |
| Industry agnostic, such as laptops, mobile devices, intranet, IT applications and data centers. | Purpose-built networks, such as Core, RAN, transport, access networks, operational support systems/business support systems. |
| Infrastructure and protocols | |
| Standard protocols, such as transmission control protocol/IP and TLS. | Multi-vendor legacy technologies mixed with latest cloud-based SBA and telco protocols, such as SS7, Diameter, and GTP. |
| Skill sets | |
| Skills in endpoint security (mobile, desktop servers), app security, firewalls and secure gateways. | Expertise in telco network topology, communications protocols, attack scenarios for SBA, network element integrations to collect telemetry data and take action. |
| Tools and technology | |
| Homogenous security tools, such as IT security information and event management, identity and access management, end-point detection and response (EDR), and laptop antiviruses. | Specialized tools, such as telco XDR, mission critical EDR, telco privileged access management (PAM), cloud-native architecture. |
| Regulatory landscape | |
| Governed by standards, such as the Health Insurance Portability and Accountability Act (HIPAA), payment card industry standards, and the General Data Protection Regulation (GDPR). | Abides by 3GPP, GSMA, and country specific regulations, such as the Telecommunications Security Act in the United Kingdom, ²⁵ the Network and Information Security Directive 2 in the European Union (EU), and the Personal Data Protection Law (PDPL)/National Data Management Office (NDMO) regulations in the Kingdom of Saudi Arabia. |

As shown in Figure 9, the differences become even more apparent when consideration is given to the economic consequences of breaches in IT and telecoms security.

Vulnerabilities and implications in IT security

Incidents with generic IT security vendor

- Phishing attempt
- Weak password
- Data theft/exfiltration from customer DB
- Compromised DB
- Adware, crypto-miners and banking trojans

The consequences of a severe attack

- User, PII or credit card exfiltration
- IT service down

Vulnerabilities and implications in telco network security

Critical incidents with a specialized telco security vendor

- Eavesdropping subscriber data/network data
- Signaling storm towards RAN/Core
- Cross technology attacks on roaming interface (SS7/GTP)
- Compromised telco workloads/network functions

The consequences of a severe attack

- Full network outage
- Country-wide communication outage



Figure 9: Consequences of IT and telecoms security breaches

Gen AI assistants enhanced with knowledge of telecom network architectures and telecom-specific threats can amplify the speed and quality of the security operations center response to an emergent threat. This helps address the ever-growing skills gap for telecom security operations

centers, with use cases ranging from forensic analysis to guided response. Gen AI assistants can also help automate the compliance reporting required by an ever-growing array of regulatory requirements, as illustrated in Figure 10.

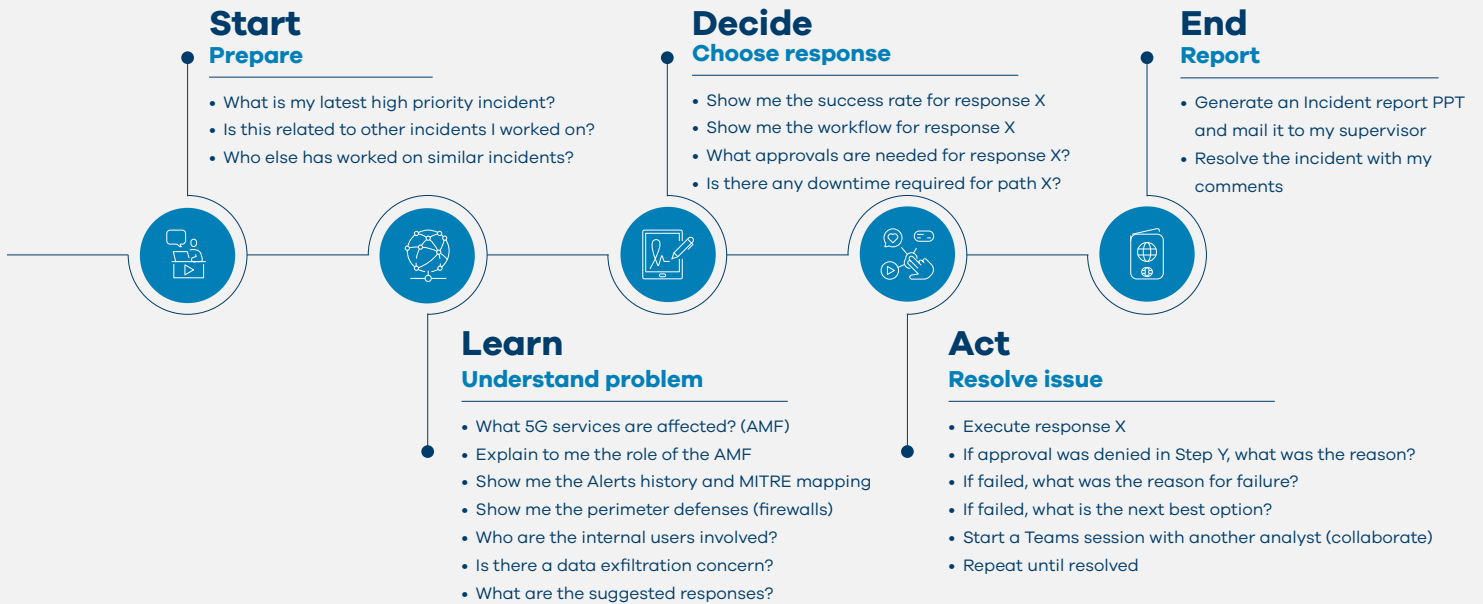


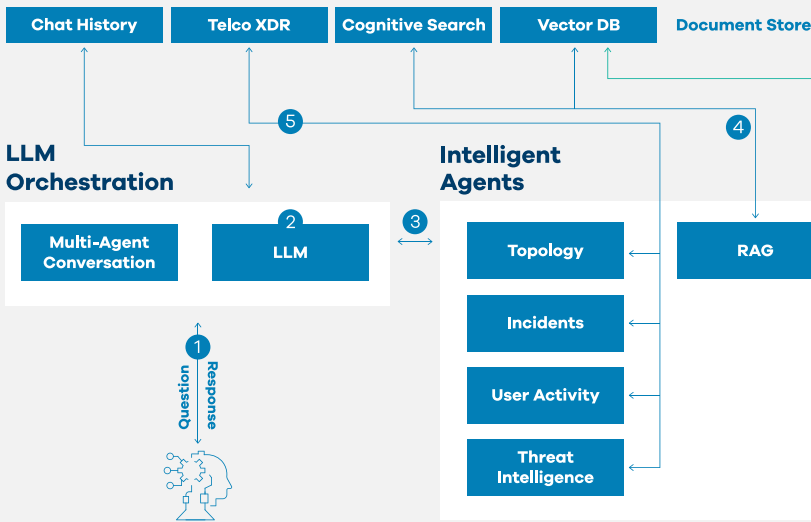
Figure 10: Enhanced SOC analyst journey using a Gen AI chat assistant

In order to be useful, the Gen AI solution must have access to clean, enriched data from a variety of network sources, including both telemetry and topological data about the network. A specialized telco XDR is generally the best answer here, with the added benefit that it

provides the incident management and response functions needed by the SOC analyst. In addition, specialized threat intelligence relevant to the network domain is key in generating useful insights. This is illustrated in Figure 11.



Knowledge Stores



Retrieval & Generation Process

1. User Question
2. LLM Orchestration chain starts
3. LLM invokes 1 or more Agents to gather information
4. RAG Agent retrieves static document data using Cognitive Search:
5. Dynamic Agents retrieve live data from Telco XDR
6. LLM generates final response

Indexing Process

1. Split input document
2. Store Embeddings and Indexes into Vector DB
3. Store document into Document Storage:

Figure 11: Building blocks for a Gen AI powered telco SOC assistant

Note: DB = database; RAG = retrieval-augmented generation.

Another key capability that the SOC assistant can offer is its ability to incorporate operator-specific or country-specific policies and procedures into the incident handling guidance offered to the SOC analysts, as custom documents added to the Gen AI knowledge base.

Normally, this type of knowledge dissemination requires training (and re-training), which may not be fully adhered to. By incorporating such information into Gen AI responses, the information is readily available in-context for the SOC analyst.

Once deployed into the SOC, the Gen AI-powered assistant can aid the analyst in several ways. It can provide:

- A smart summary of the incident
- Topology analysis in a 5G/NGN network-aware way
- Indicators of compromise (IoC)/ indicators of attack (IoA) analysis based on high quality threat intelligence integration
- Malicious user activity analysis based on user entity behavior analytics (UEBA)

- Malware activity analysis based on EDR data integration
- Guided resolution to select the remediation plan with the best outcomes
- Incident report generation for dissemination within the SOC or across operators

In summary, the key benefits of using Gen AI include:

- **An improvement in incident handling time:** Rich insights are provided – and all at the responder’s fingertips
- **Skills gap improvement:** Less experienced analysts are provided with an inline knowledge base and guidance on how to respond
- **Accuracy improvement:** Even when a critical security situation is unfolding, this solution ensures that all the information is considered when making decisions



2.3 Use case 2: Proactive threat hunting

Threat hunting is the process of proactively discovering signs of malicious activity in the NGN infrastructure that have evaded the existing security defenses and controls. The goal of threat hunting is to capture new and emerging threats, before they

have a chance to become too deeply entrenched in the network and cause serious damage. In other words, threat hunting seeks to reduce the breach detection gap or “dwell time” for a new attack, as shown in Figure 12.

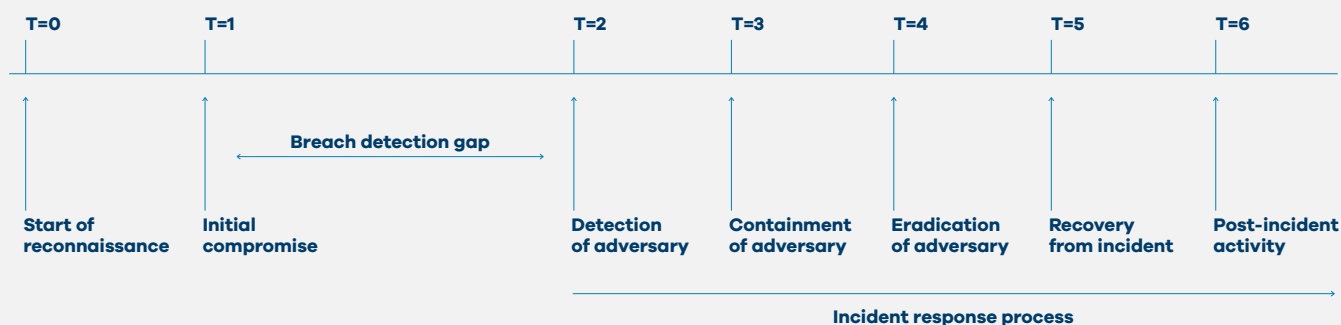


Figure 12: The breach detection gap

Source: TaHiTi Threat Hunting Methodology

Threat hunting is considered an advanced capability in an SOC,²⁶ requiring senior analysts with deep systems knowledge and a data science background to detect complex patterns of attack. It is also a high effort activity,

since it involves interpreting raw telemetry feeds across multiple monitoring points over time, with data volumes in the terabytes. Figure 13 shows one way of characterizing an organization’s threat hunting capability.

Hunt Maturity Model (HMM) is a way to characterize an organization's hunting ability. Gen AI powered tools can help improve this by providing AI-assisted automation for Telco threat hunting.

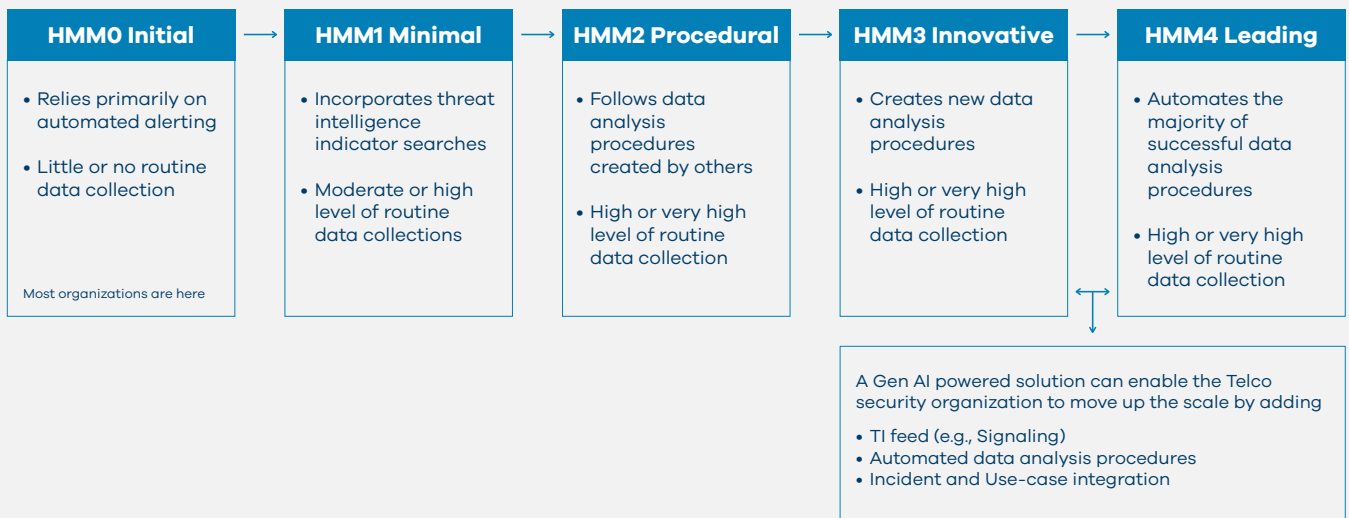


Figure 13: Threat hunting: The Hunt Maturity Model (HMM)

This is where a Gen AI powered system can be a tremendous advantage, both in terms of the advanced reasoning capabilities it brings, as well as its scalability and sophistication in terms of ML-based data analysis. A properly trained Gen AI system with access to a telecom XDR layer for NGN topology and telemetry can reduce what took many months of labor to a few minutes.

Threat intelligence needs to be an integral part of the Gen AI powered system. For example, in the SS7 signaling domain, information about a malicious GT serves as an “early warning” defense against known malicious actors reported by the global IPX community. By avoiding the “needle-in-a-haystack” problem, this results in a more focused and therefore faster hunt.

We now look at the various activities within a threat hunting session and examine how Gen AI can be leveraged to optimize them:

- Data integration:** High quality data received in a timely fashion is critical for effective threat hunting. This is ensured by having a telco XDR as a foundational element of the Gen AI-powered threat hunting solution. The Gen AI components can then

leverage both telemetry from the network functions and network topology during the inference process. For example, AI agents that are aware of the signaling firewall transaction data can record (TDR) data schema, as well as relationships with other data from other network functions involved in the SS7 calls flows. Many operators already collect large quantities of security telemetry in data lakes; this is something the Gen AI solution should be able to process.

- Threat intelligence integration:** Information about known malicious actors provides a valuable trigger for threat hunting. By using these early-warning signals from the community, the operator can anticipate and block these malicious actors before they cause significant damage. For example, in the signaling domain, the threat intelligence can be a list of known malicious GTs, based on profiling their behavior in the global IPX networks. When these malicious GTs are encountered in the operator’s firewall logs, the Gen AI system can automatically start analyzing their behavior and trigger containment actions.

- **Telco knowledge base:** The Gen AI-powered hunting solution needs to be specifically trained on a high-quality knowledge base from which it can derive the necessary insights. For example, using the information in GSMA FS.11²⁷ for SS7 attack scenarios, the Gen AI system should understand mobile application part (MAP)/customized applications for mobile networks enhanced logic (CAMEL) Category 1-3 message classifications and their implications for the signaling threat model.
- **Hypothesis generation:** In a traditional hunt, this is a human-centric activity. However, with the help of Gen AI, this process can now be automated and becomes much faster and more complete. The key metrics are the quality of the hypotheses generated (these may be multiple, depending on the particular threat actor) and the threat model coverage.
- **Evidence gathering:** Once hypothesis generation is complete, the next stage is the collection of evidence. This requires painstaking and thorough analysis of the logs. Here again, the analytic query generation capabilities of a properly trained and telco-aware Gen AI solution are needed. A variety of data sources and tables may need to be checked by the Gen AI solution to find this information
- **Attack chain reconstruction:** Many threats today are complex multi-stage attacks. The attacker may execute a sequence of moves, lying low for long periods of time to conceal their tracks. The Gen AI solution needs to understand the TTPs used by the attackers, then reconstruct the attack chain, using an industry-standard methodology such as the MITRE Attack Framework for telco networks.²⁸
- **Impact assessment:** The motive or end-goal for the attacker may be economic or adversarial. This is where a Gen AI-powered solution can incorporate threat intelligence about known threat actors and their motives into its analysis. For example, from the signaling world, some of the motives could be location tracking of mobile subscribers (a privacy attack), or disconnecting IoT devices used in industrial operations (with economic impact), spam/phishing (ransomware attack), or a billing system bypass (fraud).
- **Presentation and user feedback:** Having automated most of the hunting process, the Gen AI-powered system should still offer an option for “human-in-the-loop” in order to present the hypothesis and supporting evidence.
- **Response generation:** Once confirmed, the Gen AI-powered system can then proceed with containment and eradication. Here again, the telco-aware Gen AI solution, together with its knowledge of the network architecture, can be leveraged to generate efficient and accurate responses. In the signaling domain example, there are business consequences if the response action does not account for commercial contracts between roaming partners. Therefore, a Gen AI solution that can also factor in business impacts while choosing an appropriate solution will add value.

Figure 14 is a schematic representation of the application of Gen AI for hunting in the SS7 signaling domain.

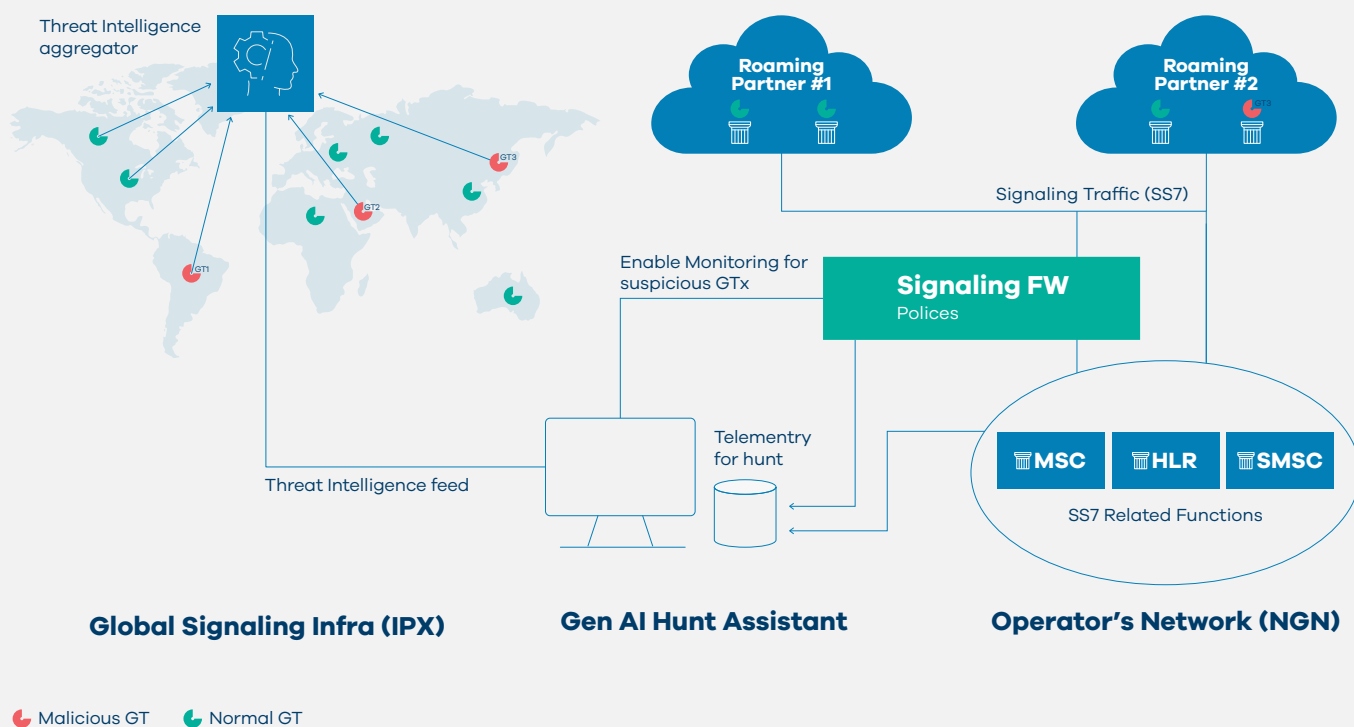


Figure 14: Gen AI hunt assistant for SS7 signaling threats

The diagram shows an operator who has roaming arrangements set up over SS7 with two partner networks. The operator's network contains a signaling firewall that can be configured with policies on what types of traffic to allow, as well as the ability to extract telemetry about the signaling messages for enabling threat hunting. There are also several SS7 related nodes in the network for handling the roaming traffic (HLR, MSC, short message service centers).

GTs are the addresses of the SS7 signaling nodes. While originally intended to be secure entities in a closed, communications service provider (CSP)-only ecosystem, modern business practices such as GT leasing have resulted in additional risks due to the introduction of non-CSP players.²⁹ In the diagram, GTs that have been identified with bad behavior (marked in red), or exhibit otherwise anomalous behaviors, are reported via a worldwide, up-to-date threat intelligence feed.

The Gen AI-powered hunt assistant receives this threat intelligence feed and combines it with continuously flowing telemetry data received from the signaling firewall as well as the signaling nodes. The hunt assistant is trained to understand low-level details about the signaling flow – for example, it can identify suspicious patterns of MAP and CAMEL messages from the raw telemetry.

Based on this information, the hunt assistant can generate one or more hypotheses about the intent of the malicious GT. It also generates analytic queries to collect evidence from the telemetry data. By applying advanced reasoning techniques, it is then able to reconstruct the attack chain and eventually the intent of the attacker and its impact. This is summarized in Figure 15.

Hypothesis

Attackers have compromised SS7 signaling equipment inside a roaming partner's network, and are using it for subscriber **location data exfiltration** from Globecom (i.e., the NCYD customer).

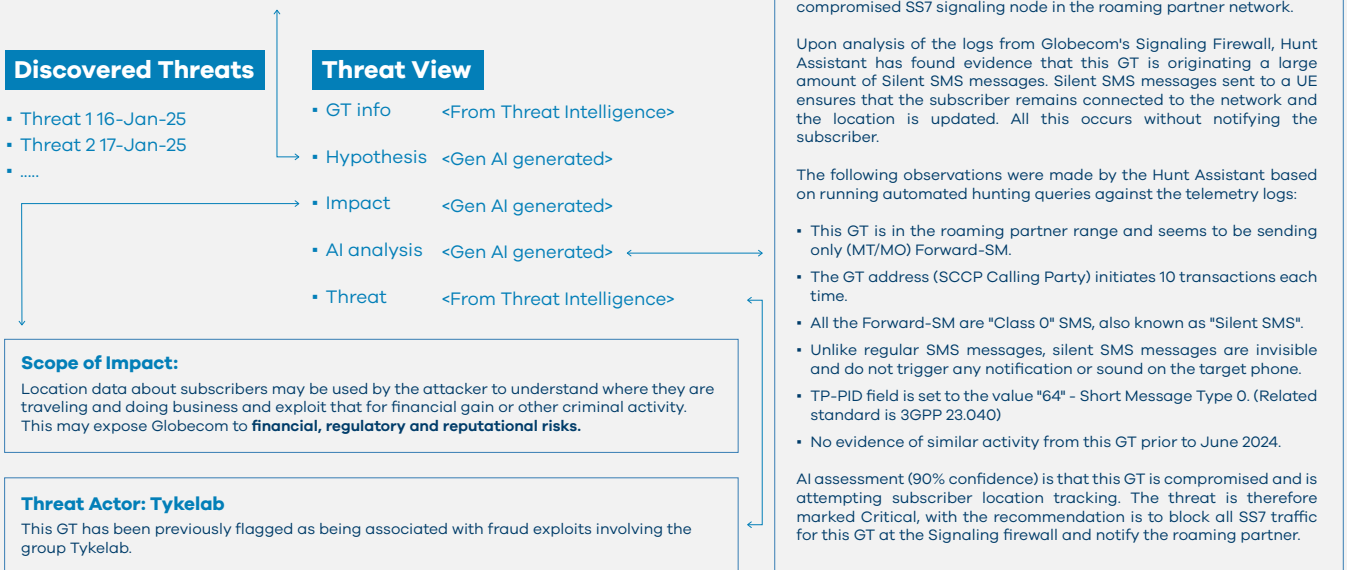


Figure 15: Using Gen AI for a signaling threat hunt

In conclusion, using Gen AI powered threat hunting to proactively mitigate inter-roaming attacks complements the reactive capabilities of the SOC, providing the widely-advocated balanced approach.³⁰

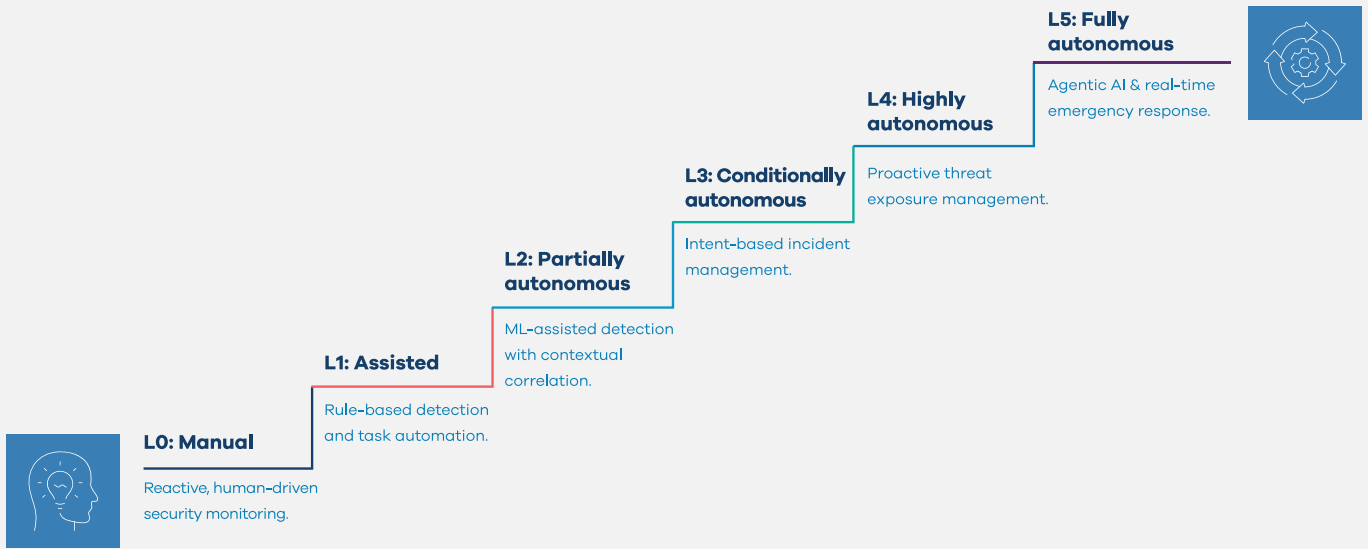
2.4 Use case 3: Self-defending autonomous networks

According to Moody's Ratings³¹, telecom networks are at the highest level of cybersecurity risk due to their integral role in global and national infrastructure. A breach here is more than a corporate setback – it is a threat to public safety, national security and the global economy.

Imagine the chaos if emergency communication lines were taken offline, or hospital networks were hacked, or oilfield operations were sabotaged. CSPs are already managing complex systems that combine existing infrastructure with advanced technologies, such as industrial robotics enabled by 5G/NGN networks. This complexity makes staying on top of both innovation and security a constant challenge.

To meet these demands, telecom security should operate at the highest levels of efficiency, managing large data volumes while preventing and responding to threats in real-time. Traditional SOCs based on a small number of human analysts will be too slow and not scalable enough to respond to the volume and velocity of threats. Instead, what is required is that the network itself becomes capable of autonomously detecting and responding to threats as a self-defense mechanism. There can still be a manual override, but in this case the model will become "human-as-the-observer," instead of "human-as-the-doer," as it is today.

The journey **toward autonomous security assurance** is evolutionary rather than revolutionary. Building on the foundation of TM Forum’s automation maturity model,³² a cybersecurity-focused, five-level framework to help CSPs build networks with advancing levels of security automation is outlined in Figure 16, with details of the levels given below.



Inspired by TM forum

Figure 16: Five steps to autonomous security assurance

Level 0: Manual

All security operations are manual and reactive. Threat detection relies on isolated data sources with no automation or threat hunting. SOC analysts are solely responsible for investigating incidents and mitigating threats.

- **Example:** Analysts manually investigate firewall alerts and security event logs to trace and mitigate anomalies

Level 1: Assisted

Basic automation supports analysts in repetitive tasks, such as log correlation and rule-based detections, but humans remain fully in control.

- **Example:** The system automatically detects unusual traffic spikes suggesting a potential DDoS attack. Analysts validate the alert and reroute traffic through a scrubbing center for mitigation

Level 2: Partially autonomous

ML-assisted detection with contextual correlation; dynamically, the system begins to adjust thresholds and isolate anomalies with continuous human validation.

- **Example:** The system analyzes top malware infections weekly, identifies active C2 server IPs and updates firewall access control lists after human validation to minimize false positives.

Level 3: Conditionally autonomous

Intent-based management of security incidents with cross-domain correlations and contextual analysis. The system uses AI models to detect anomalies, provide insights into potential IoCs and recommend actions for assessment.

- **Example:** AI analyzes logs from telecom network functions, management systems and privileged access records. It correlates unusual logins, or lateral movement patterns and suggests remediation actions to the analyst to resolve the incident's root cause.

Level 4: Highly autonomous

AI predicts security incidents and creates detection rules autonomously. Proactive threat-hunting techniques allow the system to auto-generate detection models and perform what-if scenarios to anticipate security risks.

- **Example:** Intent specifications enable the system to resolve a malware infection, using AI and automation to take closed-loop actions across different domains, such as isolating affected ports, disabling compromised user accounts, and executing preventative measures. The system automatically triggers service level agreement/regulatory compliance reports and adjusts resource allocation based on the severity of the incident, while the analysts review and oversee these actions.

Level 5: Fully autonomous

The network's security assurance function operates with autonomous AI agents that collaborate to find the best resolution to complex incidents in real time, including emergency response. These agents autonomously handle proactive measures, crisis management and real-time adaptation with minimal human intervention.

- **Example:** During a ransomware attack, multiple large action model agents work together, isolating compromised nodes, blocking malware spread, restoring systems, and implementing countermeasures, such as closing ports and validating backups. Analysts provide high-level oversight, guiding strategic decisions and ensuring policy adherence.

Adversaries no longer rely on AI just to create more convincing spear-phishing messages; they're crafting malicious code, automating complex attacks, and manipulating live video and audio streams. In response, defense systems should evolve to match this new level of sophistication and speed.

The benefits of advanced automation in NGN security assurance are clear: faster response times, reduced errors, and the ability to address increasingly sophisticated threats. Still, most operators are just beginning to adopt AI and automation. These are critical environments in which "five-nines" availability³³ allows only 5.26 minutes of downtime per year. Earning trust in AI requires thoughtful planning, careful oversight, and commitment to ethical AI practices.

Much like automating the entire cycle of network and service operations, operators should invest in continuous automation advancement in security assurance in order to protect networks as they grow smarter, faster, and more autonomous.

2.5 Gen AI safety and governance

Safety and governance controls are important for the Gen AI applications used in a telecom environment. This is the case for several reasons:

- From the user perspective, it is important to ensure quality of responses and therefore the trustworthiness of the assistant or autonomous agent
- From the organizational perspective, it is crucial to ensure that usage is consistent with corporate policy
- From the regulatory perspective, it is obligatory to ensure compliance with all applicable laws

2.5.1 Responsible and ethical AI

Organizations such as the National Institute of Standards and Technology (NIST)³⁵, the GSMA³⁶ and Microsoft³⁷ provide guidance on how to develop and deploy AI applications in a way that builds trust.

Key aspects that must be considered throughout the SDLC of a Gen AI solution for telecom environments include:

Security vulnerabilities

LLM and Agentic AI are themselves vulnerable to a variety of attacks, as described by the Open Worldwide Application Security Project (OWASP)^{38,39}. The Gen AI solution should therefore include mitigations and safeguards against such attacks – notable examples of which include:

- **Prompt injection:** In this scenario, carefully crafted inputs are used to manipulate outputs. This attack can be mitigated by implementing guardrails to filter and constrain model responses to the domain context.

The essential pillars of safety and governance to keep in mind are:

1. Responsible and ethical AI:³⁴ This set of principles and practices should be followed throughout the software development lifecycle (SDLC) and deployment of the Gen AI solution.

2. Regulatory compliance: Compliance with legal and regulatory requirements should be ensured. The details of this are further discussed in the following sections.

- **Jailbreaking:** In this scenario, the attacker forces the LLM to bypass safety protocols. Mitigations include using guardrails implementing filtering and better controls during model fine-tuning to improve safety and alignment.
- **Data poisoning:** The attacker introduces backdoors, biases, or other vulnerabilities in the data during pre-training, fine-tuning or embedding to alter the LLM responses. Monitoring data quality in the data pipelines and providing a feedback loop to users to flag incorrect AI responses, so that retraining is applied, can be used to mitigate this.
- **Information leakage:** When using shared LLM instances, data may be potentially disclosed to other users or leveraged by the cloud-based LLM provider to improve their model. Using a trusted/private cloud environment with clear data ownership rules can help mitigate this.



Data privacy and copyright infringement

Gen AI models can bring significant data privacy and copyright infringement challenges. A significant risk is posed by unintended outputs, in which personal information about subscribers or network-sensitive information, such as device credentials and topology, are revealed. In the telecom environment, it is especially important to ensure that any sensitive data used in the AI training or embedding is anonymized, strict data classification and access controls are applied, and the AI is only trained with information that adheres to copyright laws.

Access control and privileged use

Gen AI systems can autonomously trigger external actions, such as a change in network or firewall configurations as part of a remediation response. This can potentially be abused by a compromised or malicious account or user. To mitigate this, strong role-based access controls and just-in-time (JIT) permissions should be leveraged, with a human-in-the-loop model supported for high-risk actions.

Model explainability and accountability

Many Gen AI models tend to operate as a “black box”, sometimes generating outputs that are not easily understood by humans. This can trigger regulatory and accountability concerns. When applied to Gen AI models, explainable AI techniques can help clarify AI decisions in a way that humans can understand and help build trust in the AI system. Stanford University has developed its Foundation Model Transparency Index⁴⁰ to help in the selection of foundation models for a Gen AI application, based on these criteria.

Hallucination management

Gen AI models can hallucinate – fabricate false information and include

it in their output. This is a significant barrier in developing trust. Careful prompt engineering and guardrail-based techniques can be used to ensure that this is not an issue in the Gen AI solutions used for telecom environments.

Managing harmful bias

Gen AI models can exhibit bias due to the nature of their training data. That data may have been skewed towards a certain population, for example, leading to Gen AI responses that may be more advantageous to users from that population. Harmful biases also have the potential to reduce the productivity benefit seen for certain individuals, or, by not considering local or regional aspects, biases may result in an incomplete or even inaccurate response, causing a loss of trust. For Gen AI-based telecom solutions, appropriate techniques, such as prompt engineering or fine-tuning additional data, can be used to resolve this.

Human oversight

While Gen AI solutions bring the potential for extreme automation, in order to minimize risks, it is still necessary to allow for human oversight. This is especially important in mission-critical telecom environments and is often required for regulatory compliance. Over time, however, as technology progresses and trust is built, a greater amount of autonomy can be ceded.

Abuse monitoring

Users may try to inappropriately use Gen AI (especially chat interfaces) for harmful or abusive actions, including obscene content. This is generally in violation of country laws and organizational policies. The Gen AI solution should therefore include mechanisms to detect, prevent, and report such activity, using techniques such as content filtering⁴¹ and chat session recording.

Supply chain integrity

Gen AI applications are vulnerable to supply chain attacks against both the foundational models and the libraries or frameworks they consume. It is therefore essential to ensure that the Gen AI solution is built and delivered using secure development, security, and operations processes with artificial signing to ensure supply-chain integrity. This protects both the LLM and the content used in its knowledge base (e.g. prompts, docs, etc.) to mitigate data poisoning concerns.

Robustness

Gen AI applications need to continue functioning correctly even in the face of missing or incorrect data, agent communication failures, hacks, and other obstacles. A thorough testing strategy is key to ensure the resiliency of the Gen AI system.

Data sovereignty and cross-border aspects

The residency of the data, as well as the foundational models used by the Gen AI applications, should be considered in order to ensure compliance with regulatory requirements. The ability to deploy within regional data centers or even local on-premises can help mitigate this. Roaming introduces additional considerations, due to the potential involvement of foreign entities and associated lawful interception, cross-border data flow, or surveillance obligations. Appropriate tagging or handling/segmentation of data related to international signaling traffic can help address this.

2.5.2 Regulatory compliance

The regulatory landscape for Gen AI applications is evolving, with governments trying to find the right balance – one that allows innovation while also protecting consumers.

Table 3 looks at some key jurisdictions and their relevant regulations.

Table 3. Notable regulations for AI and data privacy

| Country/region | Description |
|----------------|--|
| EU | <ul style="list-style-type: none">• AI Act: Categorizes AI systems into four risk categories, each with specific regulatory requirements. Gen AI is covered under General Purpose AI (GPAI) rules, and providers are expected to disclose training data summaries, ensure copyright compliance, and manage systemic risks.• GDPR: Covers data privacy aspects |
| United States | <ul style="list-style-type: none">• State-level data privacy and AI regulations include California AB 2013 and the CCPA/CPRA, the Colorado AI Act, New York SB 8755 and Montana SB 212 |

| | |
|-------------------------|--|
| Kingdom of Saudi Arabia | <ul style="list-style-type: none"> • PDPL: Regulates the processing of personal data and the rights of individuals thereof • NDMO: Provides a set of standards to safeguard public and government data as part of the Vision 2030 development plan • National Cybersecurity Authority (NCA): Provides the framework for cybersecurity regulations • Communications, Space and Technology Commission (CST): Oversees the telecoms, space and IT sectors |
| United Kingdom | <ul style="list-style-type: none"> • UK AI Regulation Bill (proposed): Addresses ethics, safety and copyright issues • UK GDPR and Data Protection Act 2018: Addresses data privacy |
| Canada | <ul style="list-style-type: none"> • Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems • Artificial Intelligence and Data Act, Bill C-27 (AIDA): This bill failed to pass |
| India | <ul style="list-style-type: none"> • Draft AI regulation framework in progress • Digital Personal Data Protection Act 2023 (DPDPA): Addresses data privacy |
| China | <ul style="list-style-type: none"> • Interim Measures for the Management of Generative Artificial Intelligence Services 2023. • Personal Information Protection Law (PIPL): Addresses data privacy |

In the telecom environment, Gen AI solutions must factor in compliance monitoring/reporting as part of their design and deployment processes.

2.6 Enablers for AI-driven telecom security

2.6.1 High-quality data pipelines

Ensuring that Gen AI models receive relevant, real-time, and trustworthy network data begins with robust data pipelines and full network observability. In telecoms, this means continuously collecting live signaling and user-plane data from all parts of the network – both legacy and modern. It also means verifying data quality before feeding it into AI/ML systems.

For telcos, high-quality pipelines must ingest massive volumes of network activity data, scrub and normalize it in real time, and monitor for anomalies.

This means deploying streaming platforms and monitoring tools that can handle the velocity of network events, immediately flagging any data collection issues. By continuously monitoring data health, telcos can detect drift or gaps before AI models consume flawed inputs.

In short, built-in observability ensures “garbage in, garbage out” is avoided – AI models must learn only from clean, complete data.

2.6.2 Real-time network observability

A 360° observability approach, spanning RAN, core, transport and interconnect – is needed. Operators are increasingly unifying data from diverse sources into a common framework. Nokia’s Cybersecurity Dome XDR and Autonomous Networks portfolio, for example, uses Agentic AI to give operators holistic, real-time network observability across any vendor or architecture. Practically, this means collecting telemetry and logs from base stations, core elements (MME/AMF, HSS/UDM/UDR, etc.), interconnect points, signaling gateways, an EDR and PAM systems, often with collection points that are geographically distributed.

For signaling threats, any blind spot is dangerous. Observability pipelines must therefore include SS7/Diameter probe feeds and GTP capture as well. This ensures AI models see the full picture. Key sources of data include: SS7 probe outputs or firewall logs; Diameter routing agent logs; GTP-C/U records; and – for 5G – control-plane API logs.

These feeds are routed into the data pipeline in real time. Because signaling traffic is structured (in, for example, CDR-like records), it can be parsed into features for ML. But it is also sensitive, so pipelines must secure and normalize it. XDR systems must store SS7/Diameter logs with tight integrity and timestamping, so incidents are forensically traceable.

Modern architectures leverage streaming to transport this data to analytics and storage layers. Network observability platforms ingest streaming data (packet probes, log feeds, and performance counters) and expose it for AI models.

These platforms also log their own health: if a data source stops reporting or lags, this triggers alerts downstream so that issues can be fixed immediately. In sum, real-time observability in telecoms means end-to-end visibility into all signaling and traffic flows, along with automated monitoring of the data pipelines themselves.

2.6.3 Purpose-built AI/ML models

Traditional rule-based filtering, such as static firewalls or regex scrubbing, often fails in the face of novel or sophisticated signaling attacks. Research shows that rule-based detection mechanisms are ineffective when it comes to roaming-based signaling exploits, with hope lying instead in deep learning (DL)-based solutions. In practice, operators and vendors need to use AI/ML to detect anomalies in signaling flows and cross-protocol signaling firewalls in order to spot fraud and spoofing across SS7, Diameter, GTP, and even HTTP/2, in real time. By correlating patterns across protocols, attacks that span SS7 and Diameter can be flagged.

Studies indicate that semi-supervised deep learning models, such as autoencoder-based networks, can outperform traditional ML and rules in detecting SS7 attacks.⁴² It was found that a semi-supervised model (PReNet) had the highest recall and F1 for SS7 intrusion detection. Other proposals use hybrid ML pipelines, such as entropy-based features on GTP flows plus random forests, or convolutional neural network models on

signaling message sequences. The key point is that AI can adapt to new threat patterns. In practice, telco operators need to integrate these AI detectors either in-network (on security groups or firewalls) or in the XDR, with these detectors streaming raw signaling logs into an AI engine that scores each session in real time. Alerts are then fed back into the observability layer.

Gen AI is currently being used for threat hunting, as demonstrated by Nokia with their Cybersecurity Dome Hunt Assistant.⁴³ By training on large corpora of logs and attack signatures, LLM-powered agents can summarize suspicious events or suggest forensic hypotheses. Recent advances with DL and LLMs are accelerating AI use in telecom security. Agentic AI frameworks promise autonomous detection.

In summary, new Gen AI-based research and products are rapidly pushing the ability to learn and predict signaling threats from streaming data far beyond the ability of static filters.



3. Conclusion

As the preceding sections have shown, the evolving threat landscape – characterized by attackers leveraging Gen AI to launch faster and more complex cyberattacks – necessitates a fundamental shift in how NGNs are protected.

In addition, while this study focuses on the signaling domain, the benefits of using Gen AI-powered security clearly also apply to many other domains. Traditional, human-driven security operations and static firewall rules are no longer sufficient to defend against these advanced, AI-powered adversaries.

This whitepaper advocates for an AI-first approach to telecom security, integrating Gen AI as a foundational element across security operations. As detailed in Section 5 above, the successful implementation of this strategy hinges on several critical technical enablers:

- **High-quality data pipelines and real-time network observability:** Gen AI models demand clean, relevant, and trustworthy data, ingested in real-time from across the entire network stack (core, RAN, transport and roaming interconnect). Telco-native XDR systems are crucial for collecting massive amounts of telemetry and providing the deep, end-to-end visibility required to feed these models effectively.
- **Purpose-built AI/ML models:** Beyond static rules, advanced DL and semi-supervised models are essential in detecting anomalies and correlating patterns across diverse signaling protocols (SS7, Diameter, GTP, SIP and HTTP/2) in real-time, identifying sophisticated, multi-stage attacks.
- **Gen AI-powered SOC assistants and threat hunting tools:** These tools augment human capabilities, addressing skills gaps and scalability challenges. They enable faster incident response through smart summaries, topology analysis, IoC/IoA analysis, and

guided resolutions. At the same time, proactive threat hunting leverages Gen AI with threat intelligence to identify new and emerging threats before they cause widespread damage.

As highlighted in Section 2, however, the transformative potential of Gen AI should be balanced by a robust safety and governance framework. Operators should proactively address the inherent vulnerabilities of Gen AI systems, including prompt injection, data poisoning, and information leakage. Ensuring data privacy, managing harmful biases, and mitigating hallucinations are paramount for building trust and ensuring reliable outputs. Furthermore, the deployment of Gen AI solutions should incorporate strong access controls, maintain human oversight for critical actions, and rigorously adhere to the rapidly evolving global regulatory landscape for AI and data privacy.

In conclusion, enhancing the protection of NGNs with Gen AI is not merely an option, but a strategic imperative. By embracing a multi-pronged approach that leverages Gen AI for defense, drives network vendors to build self-defense into the network fabric, and ensures high-quality data and observability, telecommunications operators can move beyond reactive measures.

This enables them to proactively strengthen critical infrastructure, reduce the breach detection gap, and maintain operational continuity, all in an era where cyber warfare against mission-critical telecom assets is increasingly sophisticated and AI-driven.

The journey towards autonomous security assurance is evolutionary, requiring thoughtful planning, continuous investment and an unwavering commitment to responsible AI practices. Only in this way can the digital services of the future be secured.

4. Recommendations

The insights presented throughout this document underscore that telecommunication operators now find themselves at a critical juncture: they should fundamentally transform their cybersecurity strategies in response to an increasingly sophisticated and AI-driven threat landscape. To secure NGNs and maintain operational integrity, a proactive, AI-first approach is no longer optional, but essential.

Based on this whitepaper's analysis of current vulnerabilities, the capabilities of Gen AI and the challenges faced by telecom security operations, telecom operators are given the following recommendations:

1. Adopt an AI-first security paradigm:

Operators should shift from traditional perimeter-based, reactive security to an "AI-first" mindset. This involves integrating AI-driven security analytics as a core defense component. Advanced AI models and reasoning should be leveraged to understand and mitigate the complex behavior of adversaries across the entire network. Actively deploying Gen AI for defense enables rapid analysis of vast datasets, identification of emerging attack patterns and prediction of vulnerabilities with unprecedented speed and accuracy. This can effectively level the playing field when facing sophisticated threats.

2. Empower SOC teams with Gen AI

assistants: Implement Gen AI-powered SOC assistants to augment human capabilities, bridging the cyber skills gap and improving scalability. These tools should accelerate incident response through smart summarization, 5G/NGN network-aware topology analysis, IoC/IoA analysis with integrated threat intelligence, and UEBA and malware activity analysis (with EDR data integration). Gen AI can also provide guided resolution paths and automate compliance reporting, significantly enhancing incident handling time and accuracy.

3. Establish proactive threat hunting capabilities with Gen AI:

Integrate Gen AI-powered threat hunting tools with specialized threat intelligence for telecom networks. This serves as an early warning

system for new and emerging threats, enabling containment before widespread damage.

4. Ensure high-quality data pipelines and real-time network observability:

High-quality, real-time data is foundational for any AI-powered system. Operators should invest in robust data pipelines capable of ingesting massive volumes of relevant and trustworthy data from all network parts (RAN, core, transport, and interconnect). Deploying Telco-native XDR systems is essential for deep observability across the NGN stack, including SS7/Diameter probe feeds, GTP capture, and 5G control-plane API logs. This ensures data integrity and continuous monitoring to prevent flawed AI inputs.

5. Implement robust Gen AI safety and

governance frameworks: Deploying Gen AI solutions requires comprehensive safety and governance. Operators should adhere to responsible and ethical AI principles throughout the development lifecycle, addressing model explainability and accountability, and managing harmful biases. Safeguards against Gen AI-specific vulnerabilities (e.g., prompt injection, data poisoning) should be proactively implemented, while strict data privacy and copyright compliance (e.g., PII anonymization) should be ensured. Human oversight should be maintained via strong RBAC and JIT permissions. Additionally, active monitoring and compliance with evolving AI and data privacy regulations (e.g., the EU AI Act, GDPR) is critical, while also considering data residency and cross-border data flows.

Operators adopting these recommendations will be far better equipped to survive in an era in which cyber warfare against mission-critical telecom assets is becoming increasingly sophisticated.

Endnotes

1. Nokia (October 2024). Threat Intelligence Report: What's Next for Telecom? Emerging Trends and Technologies. (Accessed 20 November 2025).
2. A botnet is a network of compromised systems that is under the control of an attacker. MITRE (2025). "Acquire Infrastructure: Botnet." MITRE ATT&CK. (Accessed 13 November 2025). With a botnet at their disposal, adversaries can launch large-scale attacks, such as DDOS or phishing campaigns. Cloudflare (2025). "Defending the Internet: How Cloudflare Blocked a Monumental 7.3 Tbps DDoS Attack." (Accessed 20 November 2025).
3. Gen AI (generative AI) is a new, disruptive AI technology. It can be leveraged by attackers to create sophisticated malware and phishing content. Conversely, it can also empower network defenders and security operations teams to scale up their detection and response.
4. SS7 is a protocol originally developed for second generation (2G) and third generation (3G) mobile technologies to exchange roaming information between networks for voice calls and short message service (SMS) texts. Diameter is a newer replacement that was developed for fourth generation (4G) and long-term evolution (LTE) mobile technologies. GTP is used for roaming data connections. SIP is an application-level protocol for services such as voice-over-internet protocol (VoIP).
5. A VNF is a software implementation of a network function that can run on virtualized hardware such as VMware. A CNF is a containerized implementation of a network function that can run in Kubernetes.
6. An MVNO provides services to its customers using the network owned by another mobile network operator (MNO) with whom it contracts to obtain bulk access to network services.
7. A GT is an address used for routing signaling messages on telecommunications networks. National authorities allocate numbering resources to communications providers, which reserve part of those numbers to use as GTs. The practice of leasing GTs (by a 'GT lessor' to a 'GT lessee') has enabled additional entities to gain access to the global SS7 network and exchange signaling messages.
8. MITRE (2025). 5G Hierarchy of Threats v3.0.0. (Accessed 18 November 2025).
9. MITRE (2025). "FGT1041." FiGHT Techniques. (Accessed 18 November 2025).
10. MITRE (2025). "FGT1071.502." FiGHT Techniques. (Accessed 18 November 2025).
11. SIGTRAN is a protocol used, for example, to carry SS7 signaling data over IP networks.
12. MITRE (2025). "FGT1557.502." FiGHT Techniques. (Accessed 18 November 2025).
13. MITRE (2025). "FGT1600.502." FiGHT Techniques. (Accessed 18 November 2025).
14. Nair, P. (March 2024). "Stealthy GTPDOOR Linux malware targets mobile operator networks." OT:today. (Accessed 18 November 2025).
15. GSMA (July 2020). Diameter Interconnect Security FS.19, v8.1. (Accessed 20 November 2025).

GSMA (November 2019). GPRS Tunneling Protocol (GTP) Security FS.20, v4.0. (Accessed 20 November 2025).

GSMA (August 2020). Interconnect Signaling Security Recommendations FS.21, v8.0. (Accessed 20 November 2025).

16. [GSMA \(May 2022\). 5G Interconnect Security FS.36. \(Accessed 20 November 2025\).](#)
17. [The NRF supports registration, lifecycle management and discovery of 5G network function instances. In a roaming scenario, the visited NRF and home NRF communicate over the N27 reference point to provide management, discovery, and OAuth 2.0 authorization token support. Bianco, D. \(October 2015\). "Hunting Maturity Model." SANS Institute. \(Accessed 19 November 2025\).](#)
18. [VoIP includes voice over LTE \(VoLTE\) and voice over 5G \(Vo5G\).](#)
19. [3GPP \(2025\). IMS Stage 2, TS 23.228. \(Accessed 20 November 2025\).](#)
20. [GSMA \(April 2021\). SIP Network Security FS.38. \(Accessed 20 November 2025\).](#)
21. [Among other things, the I-SBC can provide inspection and rules for SIP signaling messages, volumetric DDoS protection, topology hiding, lawful interception, recording, and other functions. In the 3GPP architecture, the SIP SBC function may be implemented by the IMS proxy call session control function \(P-CSCF\) or in a SIP signaling firewall.](#)
22. [ITU-T \(February 2025\). Methodologies to Mitigate Wangiri Fraud. \(Accessed 18 November 2025\).](#)
23. [GSMA Intelligence \(December 2024\). Operators in Focus: Network Transformation Survey Dashboard 2025. \(Accessed 18 November 2025\).](#)
24. [Omdia \(April 2024\). Generative AI: A Force for Change in the Cybersecurity Ecosystem. \(Accessed 18 November 2025\).](#)
25. [UK Department for Media, Digital, Culture and Sport \(December 2022\). Telecommunications Security Code of Practice. \(Accessed 20 November 2025\).](#)
26. [Bianco, D. \(October 2015\). "Hunting Maturity Model." SANS Institute. \(Accessed 19 November 2025\).](#)
27. [GSMA \(May 2019\). SS7 Interconnect Security Monitoring and Firewall Guidelines FS.11, v6.0. \(Accessed 19 November 2025\).](#)
28. [MITRE \(2025\). 5G Hierarchy of Threats v3.0.0. \(Accessed 18 November 2025\).](#)
29. [GSMA \(March 2023\). Global Title Leasing Code of Conduct FS.52. \(Accessed 19 November 2025\).](#)
30. [Rempe, R., Salač A., & Birnbreier O. \(March 2025\). "Interconnectivity Threats and Proactive Threat Discovery." IoTNow, Analysys Mason, Nokia Perspectives. \(Accessed 19 November 2025\)](#)
31. [Wieland, K. \(18 November 2024\). "Telecom Moves Into Highest Level of Cyber Risk." TelecomTV. \(Accessed 19 November 2025\).](#)
32. [Nokia Bell Labs \(September 2024\). "Autonomous Networks – what is the current state and how to move forward?" \(Accessed 19 November 2025\).](#)
33. ["Five nines" availability means the system is available 99.999% of the time.](#)
34. [Responsible AI \(or ethical AI\) is a term used to describe those principles of AI systems development that have a beneficial effect on humans and society.](#)
35. [NIST \(March 2023\). "Trustworthy and Responsible AI." \(Accessed 19 November 2025\).](#)
36. [GSMA \(2024\). "Why Is Responsible AI Important?" \(Accessed 19 November 2025\).](#)

37. Microsoft (September 2025). "What Is Responsible AI?" (Accessed 19 November 2025).
38. OWASP (November 2024). "OWASP Top 10 for LLM applications." (Accessed 19 November 2025).
39. OWASP (February 2025). "Agentic AI – threats and mitigations." (Accessed 19 November 2025).
40. Stanford CRFM (May 2024). Foundation Model Transparency Index. (Accessed 19 November 2025).
41. Microsoft (August 2025). "Content Filtering Overview." (Accessed 19 November 2025).
42. Guo, Y., Ermis, O., Tang, Q., Trang, H., & De Oliveira, A. (September 2023). "An Empirical Study of Deep Learning-Based SS7 Attack Detection." *Information*, 14(9), 509. (Accessed 19 November 2025).
43. Nokia (February 2025). "Nokia adds new Agentic-AI capabilities across its autonomous networks portfolio #MWC25." (Accessed 19 November 2025).

Bibliography

1. Brookson, C., et al. (May 2024). "A Vision for Communications Security." European Telecommunications Standards Institute (ETSI) White Paper No. 62. (Accessed 13 November 2025).
2. Cybersecurity and Infrastructure Security Agency (CISA). (December 2024). "Enhanced Visibility and Hardening Guidance for Communications Infrastructure." Arlington. (Accessed 19 November 2025).
3. European Network and Information Security Agency (ENISA). (March 2018). "Signaling Security in Telecom SS7/Diameter/5G." Athens. (Accessed 19 November 2025).
4. Szili, D. (June 2019). "Building and Maturing Your Threat Hunting Program." SANS Institute. (Accessed 20 November 2025).
5. Daszczyszak, R., et al. (March 2019). "TTP-based Hunting: MITRE Technical Report MTR 180158." MITRE. (Accessed 20 November 2025).
6. Van Os, R., et al. (2018). "TaHiTi: Threat Hunting Methodology." Dutch Payments Association Whitepaper. (Accessed 20 November 2025).

