INTELLIGENT DEFENSE: THE STRATEGIC ROLE OF AI IN TELECOM CYBERSECURITY

Flagship Report

September 2025

GLOBAL CYBERSECURITY FORUM

stc

The Global Cybersecurity Forum (GCF) is a global, non-profit organization that seeks to strengthen global cyber resilience by advancing purposeful dialogue, enhancing international multi-stakeholder collaboration, and supporting high impact initiatives.

GCF is as a platform where the world's cybersecurity stakeholders can exchange knowledge and collaborate to tackle the critical issues around Cyberspace. GCF aims to catalyze socioeconomic change, expand the boundaries of knowledge on critical cybersecurity topics, and build the foundations for global co operation on the 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 transformation of the cyber world. 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 hub to enable the cyber 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 cyber-empowered future for all.

Foreword

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

Today, telecommunications are driving global digital transformation. They are enabling 5G-powered edge computing, the internet of things (IoT), and soon 6G networks with terahertz speeds and ultra-low latency.

In the Gulf Cooperation Council (GCC) and Middle East and North Africa (MENA) regions, the social and economic impact of telecoms has been profound. This has, however, also attracted cyber adversaries across networks and business systems.

To counter these threats, telecom operators are adopting AI for proactive threat detection, realtime defense, automated response, and strong governance. This flagship report presents a four pillar framework to guide AI-driven telecom security, aligning with GCF's mission to strengthen the safety and resilience of Cyberspace for all through collaborative priorities, purpose-driven dialogue, and impactful initiatives.

I would like to thank the Microsoft team for their valuable and expert insights, as well as all the other contributors to this work. It is through the inclusion of diverse experiences that we can ensure our connected world is built on trust and openness.

Authors

- **Al-Batoul Kutbi,** Microsoft
- **Anas Hadidi,** Microsoft
- **Badr Al Karni,** Microsoft
- **Basmah Alduwayan,** Microsoft
- **Fadi Issa,** Microsoft
- **Mohamed ElNahtawy,** Microsoft
- **Ozair Nadeem,** Microsoft

Contributors

- **Tom Curry,** Google
- **Abdulrazzak Arif Shaikh,** stc
- **Imran Khan,** stc
- **Islam Swelam,** stc
- **Mohammed Y. Uddin,** stc
- **Muhammad Abu Bakar,** stc
- **Nauman Khan,** stc

Knowledge Community: Safeguarding Future Networks and Emerging Technologies

In an increasingly interconnected world, the evolution of next generation ICT technologies, such as 6G, has emerged as a powerful catalyst. The profound implications and transformative power of this next wave demand immediate attention to navigate its complexities, safeguard its deployment, and harness its capabilities for the benefit of society. The 'Safeguarding Future Networks and Emerging Technologies' Knowledge Community is committed to promoting and safeguarding current and future 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

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@GCForum.org.

Useful Acronyms

Acronym	Definition
AI	Artificial Intelligence
AI RMF	AI Risk Management Framework (NIST)
AM	Access Management/Account Management (context-based)
API	Application Programing Interface
APT	Advanced Persistent Threat
BCG	Boston Consulting Group
Capex	Capital Expenditure
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
ECC	Essential Cybersecurity Controls (Saudi Arabia)
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
GCC	Gulf Cooperation Council
GCF	Global Cybersecurity Forum
GDPR	General Data Protection Regulation (European Union)
GPU	Graphics Processing Unit
GSMA	GSM Association
HR	Human Resources
IAM	Identity and Access Management
I-o-C	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
ISMI	International Mobile Subscriber Identity
ITN	Integrated Telecom Network
KPI	Key Performance Indicator
LLM	Large Language Model
Mbps	Megabits per Second
MDR	Managed Detection and Response
MENA	Middle East and North Africa

Acronym	Definition
MFA	Multi-Factor Authentication
ML	Machine Learning
Ms	Millisecond
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond/Recover
NIST	National Institute for Standards and Technology (United States)
NLP	Natural Language Processing
Opex	Operational Expenditure
OTP	One-Time Password
PDPL	Personal Data Protection Law (Saudi Arabia)
PDU	Protocol Data Unit
PGW	Packet Gateway
PR	Public Relations
p/s	Per Second
ROI	Return on Investment
SBA	Service-Based Architecture
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMS	Short Message Service
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
stc	Saudi Telecom Company
TIDS	Threat Intelligence Detection System
TTP	Tactics, Techniques and Procedures
UAE	United Arab Emirates
VOIP	Voice Over Internet Protocol
XAI	Expandable Artificial Intelligence

Executive Summary

Telecoms are increasingly integrated into all aspects of daily life. Enabling a more connected world of knowledge-exchange, 5G networks are empowering edge computing and the IoT, while democratizing access to knowledge. The soon-to-be-launched 6G networks will take mobile telecommunications a step further, into the terahertz space and 1 millisecond (ms) latency.

This positive and evolving influence on society and the economy has not gone unnoticed by the countries of the Gulf Cooperation Council (GCC) and Middle East and North Africa (MENA) regions. Indeed, in both the public and private sectors, this influence plays a pivotal role in these countries' digital transformations.

Yet, the evolution and integration of telecoms into all aspects of daily life and the economy also poses risks. It makes everything from packet data network gateways (PGW) and end-user subscriber identity module (SIM) cards to telecom operators' business systems into lucrative targets for cyber adversaries.

To navigate these evolving threats, telecom operators are increasingly adopting artificial intelligence (AI) as a cornerstone of their cybersecurity strategies. At an unparalleled scale, AI helps them identify emerging threats, detect anomalies in real-time, streamline response efforts, and enforce robust governance.

This flagship report analyzes the experiences and the feedback provided by seasoned industry experts across the GCC and MENA regions. Its intention is to provide the reader with more insight into adopting AI in their cyber toolkit by exploring a four pillar strategic framework that integrates AI across the full life-cycle of telecommunications security practice.

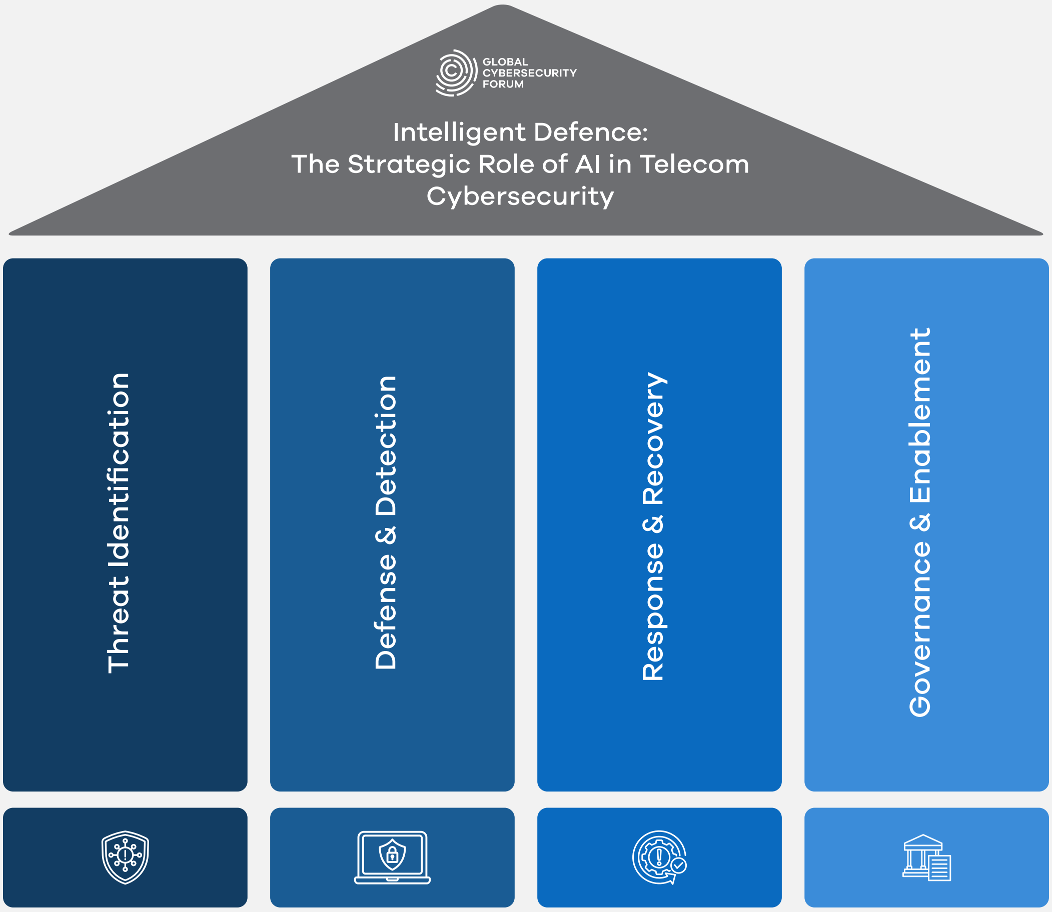
The four pillars are:

Threat identification: Leveraging AI to proactively generate threat intelligence and detect anomalies across telecom networks.

Defense and detection: Deploying AI to automatically monitor, analyze and respond to real-time threats at machine speed.

Response and recovery: Augmenting security operations center (SOC) operations with AI to automate alert triage, guide playbooks and ensure swift recovery.

Governance and enablement: Embedding trust, transparency, compliance, and investment planning within AI's integration into security.



To deliver a forward-looking roadmap, these pillars combine global best practices established by NIST, MITRE FiGHT™, ETSI, and Microsoft with regional insights.

Figure 1: Four pillar strategic framework for AI integration

Introduction

AI is not merely an enabler – it is a strategic imperative in securing telecommunications infrastructure and ensuring service reliability in a complex threat landscape.

Due to its ability to handle massive and diverse data streams to produce actionable threat intelligence, AI has been proving effective in threat identification. Telecom-specific threat frameworks, such as MITRE's FiGHT™ (5G Hierarchy of Threats)[1] can, for example, catalogue adversary techniques, tactics, and procedures (TTPs) when targeting 5G systems. This helps operators understand and prioritize threats. AI systems can help identify rare threats by mining global threat feeds and anomaly patterns in order to predict emerging attacks. Examples of these include new SIM-swap fraud campaigns or zero-day exploits.

In defense and detection, AI enables real-time monitoring of network traffic and behavior to detect and prevent intrusions that evade traditional tools.

AI can swiftly flag rogue devices – such as fake base nodes or malicious IoT devices – and adaptively enforce access controls. These capabilities are crucial as 5G's scale and complexity outpaces manual security. Palo Alto Networks, for instance, notes that AI-driven security is now essential to handle the "three S's" of modern threats: massive scale, advanced sophistication, and high speed.[2]

When attacks do occur, AI-augmented response and recovery dramatically improves SOC efficiency. In seconds, AI "agents" can triage thousands of alerts, correlating weak signals across identity, network, and endpoint systems into a meaningful incident narrative. By filtering noise and highlighting truly critical events, this reduces alert fatigue, allowing human analysts to prioritize high-impact threats.

Organizations adopting AI-assisted SOC tools have also reported measurable improvements in operational efficiency. According to a recent survey by Forrester, The Projected Total Economic Impact™ of Microsoft Security Copilot[3], key performance indicators showed an average reduction of 18.6% in mean time to detect (MTTD) and 12.3% in mean time to respond (MTTR), highlighting AI's potential in accelerating threat detection and response workflows.

AI also streamlines incident response with intelligent playbooks. Examples of this include: automatically isolating compromised network segments; suggesting remediation actions; and highlighting potential impacts on critical services, enabling operators to evaluate continuity and cost implications before acting.

Finally, the governance and enablement pillar addresses how to use AI responsibly and effectively. As telecom operators embed AI into security workflows, they must establish trust through model transparency, explainability, and compliance with sector regulations. NIST's AI Risk Management Framework (AI RMF) emphasizes building trustworthy AI – one that ensures reliability, safety, fairness, and accountability – while maintaining rigorous oversight of AI-driven decisions. Leading GCC nations are already aligning with such practices. The National Cybersecurity Strategy (2025) of the United Arab Emirates (UAE) and Saudi Arabia's updated Essential Cybersecurity Controls (ECC), for example, both stress robust governance, data protection laws, and skilled cyber talent to safely harness new technologies.

The AI Act in the European Union (EU) also sets a precedent for global AI regulation by introducing a risk-based approach to AI oversight. The act mandates transparency, human oversight, and strict compliance for high-risk applications, reinforcing a shared international commitment to responsible AI development.

AI has therefore emerged as a strategic ally for telecom security leaders. It can empower threat intelligence to anticipate attackers' moves, fortify defenses to autonomously detect intrusions, empower responders to contain incidents swiftly, and enable a governance framework that ensures these innovations are reliable and compliant.

This report will use the four pillar strategic framework outlined above to take a more detailed look at AI's growing and vital role in cybersecurity.

1. Pillar 1: Threat identification

Effective cybersecurity begins with threat identification and understanding. This is uniquely challenging in the telecoms industry due to a number of factors, including: high-volume networks; diverse signals, such as voice, data, and control signals; diverse devices, such as mobile phones, IoT devices, and infrastructure equipment; and specialized attack vectors, such as signaling exploits and subscriber fraud.

AI is revolutionizing how telecom operators gather, curate, and interpret threat intelligence. In looking at this, Pillar 1 consists of two main components: AI-powered threat intelligence, and anomaly detection.

1.1 AI-powered threat intelligence

Traditional threat intelligence programs struggle to process the enormous amount of data relevant to telecom companies, or telcos. This data range from global attack information repositories and dark web chatter to internal logs and fraud reports.

AI serves as a powerful ally by sifting through these vast datasets to identify patterns and find indicators of emerging threats. Machine learning (ML) models and natural language processing (NLP) techniques, including large language models (LLMs), can mine unstructured data – such as hacker forums, malware samples, and vulnerability disclosures – to provide predictive and pre-emptive insights. Generative AI systems can also summarize threat intelligence reports and support natural language queries within threat intelligence data lakes, improving the productivity and effectiveness of threat intelligence teams.

Figure 2 illustrates some key numbers from recent cyberattacks derived from authoritative industry sources. The SIM swap fraud increase in the United Kingdom detailed below was reported by Cifas in its Fraudscape 2025 report[4]; and both the surge in password attacks and the scale of AI-driven threat mitigation were detailed in the Microsoft Digital Defense Report, 2023.[5]

SIM Swap Fraud Surge (UK, H1 2024)

↑1000%

Year-over-year increase in SIM swap cases

Password Attack Frequency

↑10×

Increase in attempted password attacks (2022–2023)

Daily Threats Blocked by AI Security

30.8 billion

Attacks stopped per day via AI-powered defenses

Figure 2: Key numbers from recent cyberattacks

Source: See above paragraph.

1.1.1 SIM swap fraud

One example of AI's ability to counter these threats is its use in tracking SIM swap fraud campaigns. SIM swapping – where attackers hijack a victim's mobile number by tricking the carrier – has exploded into a global fraud epidemic. In the first half of 2024, the UK saw a 1,000% surge in SIM swap incidents[6], causing GBP 5 million in losses.

Telcos have turned to AI to analyze carrier request patterns, customer profile changes, and social media data to flag suspicious SIM swap attempts in real-time.

By correlating subtle signals – such as multiple SIM replacement requests or compromised user credentials on the dark web – AI-driven systems can detect and block fraudulent number porting before financial damage occurs. This is a prime example of AI-powered threat intelligence, as AI is effectively collating intelligence from various sources (internal telecom databases and external breach data) to identify fraudsters' tactics. Early deployments also claim impressive results – potentially cutting SIM swap fraud rates by up to 80% through rapid detection and intervention.[7]

INDICATOR	MANUAL REVIEW	AI-POWERED REVIEW
Detection time	8–24 hours	< 1 hour
False positives	High	Low
Fraud reduction impact	Around 20%	Up to 80%

Table 1: Comparison of AI-powered review and manual review in SIM swap detection

Source: Microsoft.[5]

1.1.2 DDoS campaigns

AI-driven threat intelligence also extends to detecting DDoS campaigns and espionage by bad actors targeting telecom infrastructure. Modern DDoS attacks often involve large IoT botnets generating huge traffic floods.

AI systems can analyze global traffic patterns and threat actor behaviors to predict which critical telecom services (DNS servers, signaling gateways, etc.) might be targeted next.

They can thus help network teams pre-emptively allocate resources or deploy scrubbing services.

threats from bad actors, telecom operators have leveraged AI to monitor indicators from frameworks such as MITRE FiGHT™, a knowledge base of adversary tactics and techniques for 5G. MITRE FiGHT provides a structured model of how attackers might abuse the 5G ecosystem, such as by exploiting the core network, slicing technology, or attacking the supply chain. By aligning AI analytics with such frameworks, telecommunications operators can intelligently hunt for specific threat techniques in their environment, including by scanning for the tell-tale signatures of an SS7 signaling attack or a malicious network slice configuration. MITRE's FiGHT, much like the well-known MITRE ATT&CK, is intended to enable threat-informed defense – a strategy that helps organizations map their detection coverage against known tactics. An AI system can automate this mapping, continuously processing threat intelligence feeds and updates to alert security teams if a new attack technique, such as a novel 5G protocol exploit, is likely to be relevant to their network.

1.1.3 Regional conditions

From a regional perspective, GCC and MENA telecommunications operators can maximize the benefits of global threat intelligence by tailoring it to local conditions.

Geopolitical tensions in the Middle East have led to targeted attacks on telecommunications operators – both as final targets and as entry points into final targets. Threat actors frequently target telcos in GCC states in order to steal subscriber data or leverage telecommunications networks for broader cyber warfare. AI-powered threat intelligence platforms help regional carriers pool information on such attacks, share indicators of compromise (IoCs), and learn from each incident at speed. By using ML to analyze regional attack patterns – including the preferred tactics of threat groups active in and/or targeting the MENA region – telecommunications providers can ramp-up defensive measures where they're needed most. This might include enforcing SMS one-time-password systems when intelligence shows a spike in SIM swap/social engineering attempts, and tightening firewall rules and limiting traffic rates when threat intelligence shows that hacktivist groups are coordinating DDoS campaigns.

In summary, AI-driven threat intelligence transforms a telecom's ability to identify threats early, shifting security from reactive to proactive. Instead of waiting for an attack to manifest, AI systems continually scan the horizon, warning of new fraud schemes, malware targeting mobile infrastructure, zero-day exploits in network equipment, and other risks. By integrating global data and local insights, AI threat intelligence provides a radar for Chief Information Security Officers (CISOs) in telecommunications to understand the evolving threat landscape and allocate resources optimally. This intelligence feeds directly into the next pillar – informing the real-time defense mechanisms and detection algorithms that guard the network.

1.2 Anomaly detection in network traffic

Telecommunications networks produce an avalanche of traffic and signaling data: billions of calls, text messages, data sessions, and control messages flow through their infrastructure components every day.

Attackers, meanwhile, try to hide their malicious activities within legitimate traffic. This might involve a rogue eNodeB/gNodeB broadcasting quietly, a malware-infected IoT device beaconing out, or a rogue insider quietly extracting subscriber data. AI-based anomaly detection has become an indispensable tool in spotting these unusual and infrequent patterns.

By learning the normal patterns of network behavior, AI can detect subtle deviations that may indicate cyber threats that signature-based systems miss.

To establish baseline "normality" for a variety of telecoms signals streams, modern anomaly detection leverages ML techniques, including unsupervised clustering, neural networks, and one-class models. For example, a model can be trained on typical signaling flows, such as HTTP/2 service-based interface calls in 5G, and then identify anomalies such as suspicious message sequences or unexpected foreign network identifiers that could indicate a signaling attack.

1.2.1 Rogue cell towers

Another significant telecommunications-specific threat that anomaly detection can address is the use of false eNodeBs/gNodeBs (also known as rogue cell towers or International Mobile Subscriber Identity [ISMI] catchers).

These are illicit devices often used for surveillance or fraud that impersonate legitimate cell towers to intercept calls or texts. Ericsson researchers have demonstrated a novel approach in detecting such rogue nodes by using AI to model the expected signal strength patterns of neighboring cell sites and then flag "unexpected values" that occur when a false "base station" is present. In trials, this method successfully caught the anomalies in received signal reports caused by a fake cell transmitter – a task nearly impossible with static threat identification correlation rules. The ability to reliably detect false "base stations" increases the trustworthiness of the mobile network and thwarts eavesdropping attacks.

Table 2 shows how anomaly detection can enable near-instant flagging of telecom-specific attack vectors. The threat indicators represented have been sourced from Ericsson's Telecom Intrusion Detection System (TIDS). This monitors signaling anomalies across SS7, GTP, SMS, and IoT protocols in order to detect spoofing, botnet activity, and device hijacking.

TRAFFIC TYPE	EXPECTED PATTERN	DEVIATION DETECTED	FLAGGED THREAT TYPE
GTP-C Signaling (Node X)	Stable night load	Spike after 2 a.m.	SS7 spoofing attempt
SMS Origin (SIM 893...)	Average 10/ day	500 in 10 mins	Botnet malware spread
IoT Beacon (Device 1123)	Hourly updates	0 for 6 hours	Device hijack or shutdown

Table 2: Signal deviation analysis chart

Source: See above paragraph.

1.2.2 Traffic anomaly detection

Another key use case is core network traffic anomaly detection. Telecommunications core networks handle sensitive subscriber data and routing information. A breach or misconfiguration in the core – such as a compromised node or a misrouted signaling message – can have cascading security impacts.

AI systems such as anomaly detection forests or deep learning models can comb through core network logs in real time, looking for deviations. Such anomalies could include: a sudden spike in location update messages, which might indicate an attacker querying subscriber locations; unusual call forwarding patterns, which might indicate possible fraud or malware controlling phones; or an atypical surge in data from a particular cell at odd hours, which could signify potential cell site compromise or local denial-of-service. In one approach, a tree-based anomaly detection method was used to monitor network traffic. This produced solid results, even outperforming some deep learning techniques for certain data types. This highlights that a range of AI/ML methods – and not just the most complex neural nets – can be effective in telecom contexts, where interpretability and speed are important.

1.2.3 Subscriber usage anomalies

Subscriber usage anomalies are another domain. By analyzing customer usage data using AI, operators can catch account-level threats.

For instance, if a prepaid subscriber's phone starts deviating from its normal behavior by suddenly making large numbers of international calls at midnight, this might indicate that the SIM has been cloned or the account had been hijacked. AI models detect these outliers and can trigger automated actions, such as blocking suspicious usage and alerting the customer. Similarly, in IoT networks, AI can instantly flag devices such as smart meters for quarantine when normal traffic patterns are breached, preventing an IoT botnet from recruiting them.

1.2.4 AI vs traditional alerts

Crucially, AI-based anomaly detection works in real time or near-real-time. This contrasts with traditional threshold-based alerts – such as CPU usage exceeding 90%, or traffic going above X megabits per second (Mbps) – which are more static and often either too sensitive or not comprehensive enough, resulting in false positives or false negatives.

AI learns a multidimensional profile of metrics that includes not only volume, but also timing, source, destination, protocol mix, error rates, and other factors. It can therefore determine if an observation is truly unusual, reducing false positives while catching genuine anomalies.

For example, a telecommunications operator's AI-powered analytics tool might reveal that a cell tower normally sees 50 SMS messages per second at most. An AI model, however, would learn the tower's more nuanced pattern, including variations between off-peak, daytime, and special event hours to more accurately detect anomalies that might signal SMS spam bot activity or equipment malfunctions aiding an attack. This shows how such intelligence can reach far beyond simple static rules.

1.2.5 Future anomaly detection

Looking ahead, anomaly detection in telecommunications can be enhanced by explainable AI (XAI) techniques to address a particular challenge. Research in XAI for novelty detection has been providing ways to highlight which features contributed most to an anomaly trigger. In practice, an AI system might not only say, "Detecting a Diameter message anomaly in region X," but also indicate why – for example, "unusually high message rate to home subscriber server/unified data management outside business hours." This helps security teams quickly assess the severity and respond appropriately. The benefits of AI-driven anomaly detection in telecoms can therefore be substantial.

Academic research also highlights that AI and deep learning models significantly outperform traditional rule-based methods in scalability, adaptability, and detection accuracy. By leveraging real-time monitoring and adaptive baselines, AI systems can detect anomalies earlier and more accurately, thereby strengthening telecom network resilience.[8]

AI-Based Anomaly Detection in Telecom Networks

Massive Data Volume
Telecom networks generate billions of events daily (calls, texts, data sessions), making manual threat detection impractical.

AI Learns "Normal" Behavior
Machine learning models (e.g., clustering, neural networks, one-class model) establish baselines of normal traffic patterns to detect deviations.

Detection of Rogue Devices
AI can identify false base stations (IMSI catchers) by spotting anomalies in signal strength patterns—something static rules struggle with.

Core Network Protection
AI detects anomalies in sensitive core net traffic, such as:

- Spikes in location updates (possible tracking)
- Unusual call forwarding (fraud/malware)
- Odd data surges (potential DoS or compromise)

Real-Time Monitoring
AI systems operate in real-time, scanning for subtle deviations across multiple metrics, improving trust and response accuracy.

Explainability Matters
Emerging Explainable AI (XAI) helps engineers understand why an anomaly was flagged, improving trust and response accuracy.

Figure 3: AI-based anomaly detection in telecom networks

A growing challenge in modern cybersecurity is the use of adversarial AI by threat actors to enhance the effectiveness and stealth of their attacks. Techniques such as AI-generated phishing emails, deep-fake voice fraud, and evasive malware are becoming increasingly sophisticated, making them harder to detect using traditional rule-based systems. In this context, AI-powered anomaly detection offers a critical defense mechanism. By continuously analyzing network traffic patterns and identifying deviations from established baselines, these systems can flag suspicious behavior indicative of AI-driven threats. This enables faster and more accurate detection of complex attack vectors, including those designed to bypass conventional filters, thereby strengthening overall network resilience.

2. Pillar 2: Defense and detection

While threat identification gives operators forewarning and visibility, the next pillar – defense and detection – is about actively stopping attacks in their tracks.

Telecommunications networks must operate 24/7 with high reliability, so real-time threat detection and automated defenses are critical in preventing service disruptions and protecting customer data. AI plays a central role here by enabling adaptive, fast, and high-accuracy detection mechanisms. By enhancing detection, response, and prevention capabilities, AI technologies can assist in countering a wide range of threats, from stealthy zero-day exploits to blatant brute-force intrusions.

Pillar 2 encompasses two aspects: real-time threat detection with AI, and identity and access AI controls.

2.1 Real-time threat detection with AI

In the era of 5G and cloud-native telecommunications networks, threats can propagate at machine speed. A worm, for example, can begin exploiting a vulnerability across network functions in seconds, while a misconfigured interface can be discovered and exploited by bots almost immediately. AI-enhanced detection systems must therefore act as ever-vigilant sentinels, monitoring networks in real time and spotting malicious activities or anomalies as they occur (as discussed in Pillar1).

Industry research highlights that AI and ML are increasingly essential for rapid, real-time threat detection and response.[9] Palo Alto Networks, for example, credits its AI-driven approach ("Precision AI") with blocking a significant number of attacks per day across its customer base, thanks to a combination of ML, deep learning, and even generative AI analysis of threats.[10] This highlights how AI allows detection systems to scale to the massive volume of threats (billions of events daily) with a speed and accuracy that human analysts or legacy tools alone could never achieve.

As critical infrastructure operators, telecommunications providers are increasingly adopting AI-backed defenses to meet strict security requirements. Indeed, regulators in some jurisdictions have mandated that telecom operators have advanced threat detection and response capabilities in place as part of their licensing or security frameworks. In the United Kingdom, for example, the Telecom Security Act code of practice encourages the use of innovative detection techniques to quickly identify threats in networks.

2.1.1 Zero-day attacks

A prime target for AI-based real-time detection is the zero-day attack – a new exploit or malware that signature-based tools, such as packet-filtering firewalls or signature-based antivirus, don't recognize.

Telecommunications infrastructure, from routers to application servers, can have zero-day and un-patched vulnerabilities that attackers can try to exploit.

AI models, particularly those using ML on telemetry data, can identify the behavioral patterns of an exploit, even if the specific exploit is new. For example, a zero-day in a voice-over-internet protocol (VOIP) server might cause subtle changes in network flows or process behavior.

An AI system that has learned normal CPU usage and call traffic patterns could instantly flag that the server was suddenly executing unusual commands, or sending traffic to an unusual destination, likely under attack. Such anomaly-based detection complements traditional methods by catching these novel attacks.

2.1.2 Rogue device detection

AI can also assist with the detection of rogue devices, including unauthorized devices connecting to the telecommunications provider's internal network and fake end-user devices – such as a cloned SIM or a fraudulent eNodeB/gNodeB.

ML for device fingerprinting involves analyzing characteristics such as network behavior, signal patterns, or authentication abnormalities to differentiate legitimate devices from impostors. For example, a cloned SIM used by a fraudster might have legitimate credentials but exhibit abnormal usage, such as showing a different location or unusually timed authentication attempts. AI models that continuously profile devices based on behavioral biometrics can spot these discrepancies in real time. They can then trigger multi-factor challenges or, if permitted to do so, cut off access. Likewise, if a malicious insider or intruder plugs an unauthorized device into a telecommunications data center network, AI-based systems that are monitoring network packets might immediately see a new, non-whitelisted device signature generating suspicious scanning traffic and isolate it.

2.1.3 DDoS defense

Traditional DDoS mitigation uses rules-based traffic filters and rate limiters, but attackers often adapt to evade these. They may, for example, use multi-vector attacks or mimic legitimate traffic.

AI-enhanced DDoS defense offers a more dynamic response to these by learning what normal traffic looks like across many features. This may involve learning packet sizes, connection patterns, geolocations and other characteristics to filter out anomalies during an attack.

An intelligent DDoS mitigation system on the network edge can deploy ML models on routers that classify incoming traffic streams as benign or malicious with high accuracy.

For example, if a botnet sends seemingly valid HTTP requests to a telecom provider's web portal, the AI system may notice subtle anomalies – such as the absence of a typical user think-time between page requests or an abnormal sequence of URLs – and block those connections.

This approach reduces collateral damage, such as mistakenly blocking real customers, better than fixed rules. Edge computing and AI can also work together here: AI models at the edge (such as in eNodeB/gNodeB or data centers) can filter volumetric attacks closer to the source, maintaining uptime for core services. Continuous learning and reinforcement learning techniques can help tune the models to reduce the potential of over-blocking legitimate usage.

2.1.4 Malware and intrusion detection

Another domain for AI in real-time defense is malware and intrusion detection within the IT systems of a telecommunications provider, such as billing servers and customer data repositories.

Having a large and diverse network of endpoints and servers makes telecommunications providers tempting targets for ransomware and advanced persistent threat (APT) intrusions.

AI-driven endpoint detection and response (EDR) tools employ ML to spot malware by its behavior – such as unusual file encryption activity or process injecting – rather than known attack traffic and signatures.

In a telecommunications provider context, these tools protect the components of critical business infrastructure, such as customer databases or network management systems. If an attacker executes code on such a server, AI-based EDR can detect the anomaly and cut it off within milliseconds. Such deviations could include a process unexpectedly spawning a command shell or connecting to an out-of-profile external host. AI-based EDR can prevent a breach from spreading further into network control systems.

Similarly, AI-driven correlation of signaling logs with other security control sources, including EDR and threat intelligence feeds, can detect cross-domain attack patterns and uncover threats targeting telecommunications providers that could evade traditional, siloed monitoring.

AI can also be used to analyze unknown files and code to determine malicious intent. Through a combination of decryption, de-compilation and code analysis, the latest AI models can detect malware and identify counter measures, even for highly obfuscated and sophisticated code. AI-driven anomaly detection can be leveraged to identify and mitigate malicious signaling traffic. This can include malformed messages, non-standard parameters, and abnormally large protocol data units (PDUs), which are commonly used by threat actors to bypass security controls and exploit protocol vulnerabilities.

2.1.5 5G and beyond

Lastly, real-time AI detection is vital in protecting 5G networks and beyond. 5G introduces technologies such as network slicing, multi-access edge computing, and virtualized network functions – all of which broaden the threat landscape.

AI can monitor each network slice's health and security, detecting if one slice – for example, a slice dedicated to autonomous vehicles – is experiencing abnormal latency or suspicious traffic that could be due to an attack on that slice's resources.

The European Telecommunications Standards Institute (ETSI) envisions that future 6G networks will incorporate an intelligent trusted network (ITN) overlay. Essentially, this uses AI-driven security and trust mechanisms to secure endpoints and interactions across diverse network domains. The concept includes a zero trust model where every interaction is continuously verified by intelligent algorithms, rather than by relying on the implicit trust of network boundaries. Such AI-enabled architectures would allow secure connectivity even when integrating many different networks and devices and proactively prevent 6G-specific cyberattacks through understanding new attack vectors - a key defense factor, according to ETSI.[11]

In summary, AI-powered real-time threat detection fortifies telecommunications networks by shrinking the window of exposure – in other words, by identifying and halting malicious activity at machine speed. Whether the threat is a lightning-fast worm, a stealthy rogue access point, or a massive DDoS wave, AI acts as the nervous system of the network's immune response, sensing and responding to keep services secure and available. In a telecommunications provider environment, traditional security methods alone are hard-pressed in keeping up when the scale runs to billions of events and the complexity to multiple layers of network technology. AI provides the necessary scalability and analytical depth, which is why industry leaders assert that AI is now an indispensable pillar of 5G security strategies.

2.2 AI-powered identity and access controls

In telecommunications security, managing who and what can access systems is as important as defending the perimeter. Identity and access management (IAM) ensures that only authorized subscribers, employees, and devices are allowed appropriate access. However, static IAM policies often fail to catch misuse. Attackers can exploit weak authentication – such as stolen passwords, shared credentials, or social engineering call center processes – to breach accounts or network resources.

AI can enhance identity and access controls by making them adaptive, context-aware, and risk-based. This section covers how AI improves authentication for subscribers, guards against identity fraud and monitors insider access for abuse.

2.2.1 Adaptive authentication

One of the most visible implementations is adaptive authentication for the customers and services of telecommunications providers. This means that the level of user verification is adjusted in real time based on assessed risk.

For instance, a mobile subscriber logging into their account or a partner accessing an application programing interface (API) will encounter differing challenges depending on the context. AI models analyze factors such as device fingerprints, location, usage time, past behavior, and even biometric patterns to generate a risk score for each login or transaction. In a low-risk scenario in which the same device as always is used at its usual location for a typical usage time, the AI might permit frictionless login – perhaps using only the device's presence as authentication. For higher risk scenarios – such as a SIM card just being swapped or a login from an unfamiliar location – the system can enforce step-up authentication. This might require a one-time password (OTP), a biometric check, or some security questions. This dynamic approach balances security and user convenience, preventing unauthorized access by catching anomalies in real-time, while legitimate users enjoy seamless service most of the time. One major telecommunications provider implementing adaptive authentication found it significantly reduced unauthorized account access and improved user experience and satisfaction by minimizing unnecessary password prompts.

Due to the use of behavioral data, such as location and habits, adopters of adaptive authentication need to strike a balance between convenience and privacy of users. It is critical for telcos to be transparent and compliant with data protection regulations when deploying such AI-driven profiling.

2.2.2 Identity fraud

Telecommunications providers are often the linchpin in multi-factor authentication, such as SMS verification codes, which makes telco user accounts prime targets for identity fraud and account takeovers – as seen with SIM swaps.

AI systems, however, can massively enhance detection of these threats by monitoring a variety of channels for unusual activity such as patterns in support tickets, which could indicate social engineering attempts on customer services, changes in user profiles, such as an address change followed by a SIM replacement request, or even voice patterns in support calls - where AI voice analytics flag callers who fail voiceprint checks. By correlating these signals, AI can stop fraudulent actions, such as preventing a scammer from porting a number or accessing a subscriber's online account.

2.2.3 Insider threats

Insider threat monitoring is another crucial application. Telecommunications operators employ large workforces and partner with vendors who may have access to sensitive systems. Resultant risks include an insider abusing privileges, a compromised user account being used to access data, or a compromised device being used as an entry point.

AI tools can analyze logs of administrator actions, database queries, and system access requests to detect when an insider's behavior deviates from the norm – for example, an employee in billing querying large amounts of customer data at 2 AM - indicating an insider threat or the use of compromised data.

ML excels at establishing baselines of normal user behavior and catching the outliers. Some telecom providers have also implemented systems where an AI flags a potential malicious insider and automatically adjusts their access. This might, for example, require them to re-authenticate, or obtain manager approval for certain actions when suspicion is high.

Insider monitoring, however, raises privacy and ethical concerns and false positives can harm morale and productivity. Therefore, AI alerts are often reviewed by human security teams or human resources (HR) before action is taken. Even so, the deterrence factor is valuable: knowing that anomalies in behavior are noticed can discourage malicious intent.

2.2.4 Network access control

In the 5G era, network access control is also being refined through AI. 5G networks will connect not just phones, but factories, cars and critical infrastructure, meaning that the network must dynamically verify and trust a variety of entities, such as applications, slices, and IoT devices.

AI can help implement such granular policy decisions. For example, in the area of network slicing, should a slice for medical devices attempt to communicate with a slice for gaming due to a misconfiguration or an attack, an AI-based policy engine could detect this anomaly and block it, effectively enforcing logical access separation.

Similarly, telecommunications providers are exploring AI-driven authorization. Under this, the system continuously evaluates whether a device or an API call should be allowed based on current context – such as system load or the threat level – instead of relying on a static role-based access control list.

The cumulative effect of AI in identity and access control is a much stronger identity assurance across the telecommunications provider ecosystem. This is especially welcome, as Microsoft's recent security reports emphasize that identity is the new battleground, with password attacks skyrocketing.

In one recent period, the Microsoft Digital Defense Report 2023[5] noted a tenfold increase in password attacks, year-on-year. In response, organizations have been urged to focus on AI-enabled security to handle the scale and complexity of identity threats. For telcos, whose services underpin identity systems ranging from phone-as-identity to SMS 2FA and beyond, failing to secure identities has cascading effects. Therefore, by deploying adaptive and intelligent identity controls, telecom providers not only protect their own systems, but also reinforce the security of digital services, society-wide.

2.2.5 AI and access controls: pros and cons

In practice, entities deploying AI-powered anomaly systems are expected to notice measurable improvements in fraud prevention. Subex highlights how AI-driven anomaly detection enables real-time monitoring of SIM-swap requests, device changes and call anomalies.[12] This allows operators to intervene proactively before damage occurs. These systems also adapt to evolving fraud strategies, improving detection accuracy and reducing false positives, when compared to traditional, rule-based approaches.

AI-driven defense and detection mechanisms also enable telecom networks to become far more resilient and adaptive. Real-time AI detection ensures threats have minimal dwell time, while adaptive identity controls ensure that only the right people and/or devices get the right access at the right time.

While there is an increasing emphasis on the cumulative effect of AI in identity access control – contributing to stronger identity assurance across the telecom ecosystem – operators should also remain mindful of the risks. AI models may misclassify legitimate actions as suspicious, leading to false positives and user frustration. To mitigate this, clear secondary verification paths, continuous model training and human override capabilities are essential governance measures that help maintain trust and operational integrity.

METRIC	MANUAL SYSTEMS	AI-DRIVEN SYSTEMS
Detection speed	Minutes–hours	Seconds
Precision (fewer false alerts)	60%–70%	90%–95%
Scope (devices monitored)	Limited	Full network

Table 3: Impact of AI on threat detection efficiency

Source: See above paragraph.

EVENT TRIGGER	RISK LEVEL	ACTION TAKEN
SIM reissue in under 5-minute window	High	Block + manual review
Login from known device in home area	Low	Auto-approve
Multiple failed logins globally	Medium	MFA prompt + alert

Table 4: Access risk scoring model example

2.2.6 Looking ahead

As telecom networks evolve toward 5G and 6G architectures, new signaling protocols such as Diameter, HTTP/2-based service-based architecture (SBA) and QUIC introduce both enhanced capabilities and novel security challenges. Threat actors may attempt to exploit these protocols for misuse, including session hijacking, signaling storms, or unauthorized access. AI-based anomaly detection plays a vital role in safeguarding these environments. It does this by continuously monitoring signaling behavior and identifying deviations from expected protocol patterns. This enables early detection of malicious activity, even in complex, high-throughput environments. It also ensures that signaling integrity is maintained across next-generation mobile networks.

3. Pillar 3: Response and recovery

Even with robust identification and prevention, no defense is foolproof. Response and recovery - the ability to quickly contain, eradicate, and recover from threats to restore normal operations - is therefore a critical pillar of any cybersecurity strategy.

In a telecommunications provider environment, where uptime and reliability are paramount, efficient incident response can save millions of dollars via loss reduction and keeping revenue generating systems running. It can also preserve customer confidence. AI is transforming SOCs and incident response processes through automation and augmentation. The two focus areas under this pillar are: AI-augmented SOC operations and AI in incident response and recovery.

3.1 AI-augmented SOC operations

The SOC teams of telecommunications providers are inundated with data. There are logs from network nodes, alerts from intrusion detection systems, fraud notifications, device telemetry, and much more. An large organization's SOC may face thousands or even tens of thousands of security alerts every day, many of which are false positive alerts or low priority events. For telecommunications providers, the alert volume can be especially high due to the expansive infrastructure. This leads to "alert fatigue" – analysts are overwhelmed, important alerts get buried and the risk of human error increases. AI-driven SOC solutions aim to dramatically reduce this burden by serving as Tier 1 analysts that can triage and consolidate alerts at machine speed.

3.1.1 Automated triage

One of the most impactful applications is automated alert triage and correlation. Instead of humans clicking through each alert, an AI agent ingests alerts from across the environment (firewalls, endpoint security, network monitors, etc.) and determines which ones represent real incidents and which could be false positives or deprioritized.

For example, an AI agent might notice that three separate alerts – one from an identity system about a suspicious login, one from endpoint antivirus about a blocked file, and one from an email gateway about a phishing link – are all related to the same user in a short timeframe. Individually, each alert might not trigger action, but together they paint a picture of a potential targeted attack on that user. The AI agent "connects the dots," correlating these into a single incident, such as a possible account takeover and malware on a user's device. The AI agent would then escalate the incident with a summary in the same way a skilled analyst would investigate and correlate, but in seconds and consistently for every alert. As a result, the SOC team isn't flooded with thousands of discrete alarms; instead, they receive a manageable list of consolidated, contextualized incidents.

Statistics from organizations using such AI SOC tools are striking. They enhance threat detection and response, with key performance indicator (KPI) improvements including an average reduction in MTTD of 18.6% and an average reduction in MTTR of 12.3%. In one case, a client reduced 15,000 daily raw alerts to just 18 high-fidelity incident tickets that analysts needed to handle, achieving 100% coverage of the important incidents with quicker containment.[13]

Improvements such as these are transformational for the SOCs of telecommunications providers, which often run 24/7 with limited staff.

By filtering out the noise of false positives, or duplicate alerts across systems, while highlighting only actionable issues, AI buys back precious time for analysts.

TASK	AVERAGE TIME SAVINGS (%)
Suspicious script analysis	47%
Building out workloads with natural language prompts	42%
Summarizing alerts and incidents	41%
Troubleshooting minor issues	40%
Preparing reports	39%
Incident prioritization, investigation and response	37%
Leveraging promptbooks	37%
KQL querying	35%
Threat hunting	33%
Processing and resolving help desk calls/tickets	28%
Vulnerability impact assessment	25%
Threat intelligence assessment	23%

Table 4: AI impact on SOC performance

Source: Forrester, 2024.[14]

3.1.2 AI-assisted investigation

Once an incident is identified, an analyst typically has to gather data by checking logs, querying threat intelligence sources and looking at system states. AI-assisted investigation can automate much of this evidence-gathering and reason over the collected results. For example, upon flagging a suspicious server, the AI agent could automatically pull the relevant logs, such as authentication, recent changes, and network connections. The AI agent could then carry out reputation lookups on the internet protocol (IP) addresses found and query the internal configuration management database (CMDB) for what the server is and who owns it. It could then present the analyst with a concise and dossier. This might state that: "Server X was observed communicating with known malicious IP address Y, and a new process, Z, started on it at 3:00 a.m. This server hosts a billing database and is normally not accessed at night. Here are the last 24 hours of login attempts…". By providing this kind of rich context, AI drastically reduces the manual work an analyst must do to investigate, effectively becoming a co-pilot for SOC analysts and allowing them to focus on decision-making and creative problem-solving.

Microsoft's security leaders have referred to AI as a "valuable co-pilot," especially in specialized domains where expertise is scarce, such as IoT/OT security. The same concept applies to telecom SOCs: AI bridges knowledge and resource gaps, improving the team's overall effectiveness.

As an example, suppose a teleco's SOC receives an alert of possible malware on a base station controller. Traditionally, an analyst would scramble to gather technical data and might not even know the normal behavior of that system. An AI that has learned from past incidents and network data could immediately flag how critical that system was – for example, that it controls cell towers in region X. It could then provide likely attack paths and even estimate the likely impact. This not only speeds up triage, but also helps prioritize the incident correctly. Without AI context, the analyst might treat the incident as just another malware alert; with AI context, they might realize it was a critical issue requiring instant action to avoid an outage.

3.1.3 AI-augmented SOC operations: pros and cons

AI-augmented SOC operations lead to faster detection, faster response and more efficient use of human expertise. They effectively multiply the SOC's capacity without proportional headcount.

AI can also dramatically improve SOC staff morale and retention by filtering noise and delegating mundane tasks, such as checking IP address reputation, or gathering log snippets, allowing analysts to engage in more meaningful work, such as developing threat hunting scenarios or handling complex incidents. Indeed, organizations have noted better analyst retention when AI helps eliminate drudgery. This is crucial at a time when cybersecurity talent is in short supply, globally.

However, telecommunications providers adopting this system must do so carefully: the AI models and automation should be well-tested to avoid automating errors, such as incorrectly suppressing a true alert. Many SOCs start with the AI operating in a recommendation capacity in which analysts double-check AI decisions for a specific period. Gradually, trust is gained in full automation for certain well-defined tasks. This aligns with the concept of "human-in-the-loop" (AI does the work but a human supervises) evolving toward "human-out-of-the-loop" for routine scenarios once confidence is high.

3.2 AI in incident response and recovery

During an active incident, AI can enable dynamic playbooks that adjust in real time based on evolving conditions.

For instance, AI can automatically isolate compromised nodes and predict potentially impacted customer segments. It can also suggest remediation steps based on attack behavior. This agility is especially critical in telecommunications, where service disruptions can affect thousands, or even millions, of users.

After an incident, AI can support post-incident analysis, too, by identifying root causes, recommending security control updates and feeding lessons-learned back into detection models.

MANAGED SERVICE	RESPONDENTS REDUCING RELIANCE
Managed detection and response (MDR)	57%
Security information and event management (SIEM)	53%
Managed SOC	49%
Threat intelligence	41%
Incident response	39%

Table 5: AI-enabled security operations: reduction of reliance on managed services (%)

Source: Forrester, 2025.[5]

Once an incident such as a malware outbreak, network intrusion or data breach is confirmed, the focus shifts to containment, eradication and recovery. Time is of the essence, as in a telecommunications provider environment, an incident can quickly impact at scale service availability or customer data. AI can significantly assist in orchestrating and optimizing the incident response process, as well as in forecasting and mitigating the impact of attacks. In turn, this enhances customer satisfaction and experience by ensuring service continuity, minimizing downtime, and reducing potential revenue loss. As an example, if malware is detected in a mobile core node, AI can simulate the effect of shutdowns or rerouting to assist in recovery decisions.

As AI for response is embraced by telecom operators in the GCC and worldwide, operators also need to incorporate it into their business continuity and disaster recovery plans. Cyber incidents are now considered on a par with natural disasters or major outages in terms of business risk. Incorporating AI-driven analysis into drills and exercises will ensure that when a real incident hits, the teams trust and know how to leverage their AI tools effectively.

3.2.1 Impact forecasting

One key contribution of AI is in impact forecasting during an incident. Telecom provider networks are highly complex systems with many interdependencies. If a particular node or service is compromised, it is not always obvious what customer services or network segments will be affected.

AI models leveraging digital twins based on graph networks, graph analytics and historical incident data can simulate the effect of taking certain components offline, or the spread of an attack.

As an example, in attacks on core routers, an AI system can quickly predict how rerouting traffic would affect latency or congestion in other parts of the network. Alternatively, if a customer database was breached, AI might estimate how many customer records were at risk based on access logs and patterns of exfiltration observed. This kind of intelligent impact analysis helps incident managers make informed decisions. They can weigh actions, such as shutting down a subsystem (to stop the bleed) against the service outages it might cause, with a clearer understanding of trade-offs. It also supports communication to executives and stakeholders. An example of this might be by providing an early estimate that an incident may potentially affect 5% of a telco's mobile subscribers in region X, if the incident is not contained. Having data-driven impact forecasts improves transparency and ensures the response is proportional to the threat.

3.2.2 Intelligent playbooks and analysis

AI also enables intelligent playbooks in the incident response workflow. Traditionally, incident response follows predefined playbooks – step-by-step guides for common scenarios such as a DDoS attack playbook: identify source, invoke mitigation service, and so on. Real incidents, however, often deviate from the script.

AI can bring adaptability to these playbooks by analyzing the specifics of the incident in real time and suggesting or automating the next best action. For instance, in a malware outbreak, a static playbook might say "disconnect infected systems and start scans." An AI-augmented playbook might dynamically determine which systems to disconnect by analyzing which ones are actively communicating with a malicious host, or even auto-generate a custom malware signature if it has identified the malware strain. AI can then push that to endpoint security tools in order to quarantine files.

In a sense, AI can curate a tailored response sequence: if step A doesn't stop the malicious activity, it can quickly pivot to step B, learning from how the threat is behaving and evolving. This is akin to having an expert incident commander who adjusts strategy on the fly, but encoded in the AI logic. Already, some advanced security orchestration, automation, and response (SOAR) platforms are beginning to incorporate AI to decide among multiple playbook branches, or to handle unexpected conditions.

Another application is the use of AI for post-incident analysis and automated learning. After recovery, AI can analyze the incident data to identify root causes and trends, which then feed back into improving the security posture.

For example, AI might find that the breach occurred because of a certain misconfigured firewall rule – an insight that can be used to fix similar configurations network-wide. AI can also evaluate the response, asking whether the containment time was fast enough, or could be improved, or which steps had caused bottlenecks. AI can propose and implement new detections and new playbooks to improve the response.

Over time, this leads to continual improvement of incident response, guided by AI analytics.

3.2.3 Prioritizing service restoration

During recovery, telecommunications operators also need to prioritize service restoration. If an attack has partially disrupted services – some cell sites might be down, for example, due to a ransomware affecting their controllers – AI models can help prioritize which areas to restore first.

For example, by analyzing customer impact, AI might discover that one affected region has more critical communications needs or critical customers and network redundancy. This type of analysis ensures an efficient recovery that aligns with business priorities and service level agreements. AI might even suggest temporary mitigations, like offloading traffic to other network elements to reduce customer impact while the affected part is being fixed. This overlaps with network self-healing concepts in which AI helps networks reconfigure around failures.

As an illustrative scenario, imagine a successful intrusion into a telecom provider's internal network discovered that certain customer data had been accessed. Via log analysis, AI could assist by quickly scoping which systems and data had been accessed, thus defining the breach radius. AI could then forecast the potential regulatory impact – for example, if X thousand customers' data was involved, it would be necessary to notify and offer remedies and other services. By automating much of this analysis, the company can respond transparently and swiftly to regulators and customers, reducing the fallout.

3.2.4 AI in response and recovery: pros and cons

AI's role in incident response and recovery is about speed, precision and foresight. Speed, by automating repetitive containment actions and analysis tasks; precision, by pinpointing what is affected and what the best responses are; and foresight, by predicting consequences of actions or inactions.

It is also worth noting how AI can help manage public communications and misinformation in incident response. Cyber incidents at telecommunications providers can draw media attention and speculation, especially in cases of outages which might be perceived as cyberattacks. AI-driven tools can aid social intelligence by monitoring social media and news for emerging narratives or customer concerns during an incident, aiding the company's crisis management team to address the incident proactively. AI can therefore form part of a holistic incident response – one that ensures accurate information is conveyed, and trust is maintained.

By augmenting human responders, AI helps ensure that a security incident – which in a telecommunications provider environment could potentially disrupt critical communications or lead to leaking sensitive personal data – is handled in the optimal way with minimal damage.

This aligns with industry observations that AI can significantly enhance an organization's security posture and resilience by bridging expertise gaps and enabling effective threat response. The benefits of AI usage in this environment are clear: reduced meantime to respond, less fallout and better compliance through quick containment and thorough forensic investigation. A potential concern to manage is how to avoid over-reliance on automation, so that if the AI fails or encounters a novel scenario, the team is not caught flat-footed. That's why AI in incident response is generally used to augment rather than fully replace human decision makers. The AI might execute 95% of a playbook automatically, but crucial decisions, such as shutting down a major service or declaring an incident publicly, typically remain with humans, informed by AI's recommendations.

In summary, AI can transform response and recovery by accelerating investigations, prioritizing containment actions and reducing the cognitive load on analysts. It turns the SOC into a proactive, learning-driven command center.

4. Pillar 4: Governance and enablement

Underpinning the first three pillars is the necessity of governance – policies, oversight, compliance, and strategic planning that ensure AI is used effectively and responsibly in telecom cybersecurity. In contrast, Pillar 4 covers the organizational and structural elements needed to support long run AI-driven security.

This includes establishing trust in AI systems, ensuring regulatory compliance and ethical use as well as building the right capabilities and investing wisely. This section therefore breaks down into two sub-sections: AI trust, governance and compliance; and AI maturity and investment models.

4.1 AI trust, governance, and compliance

As telecommunications operators deploy AI across a variety of security functions, they must maintain trust – both in the technology and with stakeholders such as customers, regulators and partners.

AI decisions need to be transparent, explainable, and fair as they can significantly impact security outcomes, such as blocking a service or flagging a user's behavior as fraudulent. Moreover, telecommunications is a regulated industry in most countries, meaning any use of AI must align with telecoms regulations, cybersecurity laws and data protection requirements.

4.1.1 AI audits and governance frameworks

A key concept here is AI auditability and explainability. Regulators and internal governance teams will ask how AI makes decisions and how it can be verified that it is working correctly.

For example, if an AI system blocks a customer's activity after suspecting fraud, the telecoms provider should be able to explain that action. Frameworks such as NIST's AI RMF emphasize that AI systems should provide explanations of their operations and outputs to those who operate or oversee them. Together, explainability and interpretability help users and auditors gain confidence in AI's decisions. In practice, telecommunications providers might implement dashboards where for each major AI-driven decision, some rationale is logged. An example of this might be something such as, "Anomaly score of 0.98 on feature X triggered this alert." This doesn't mean exposing proprietary model details, but giving enough information to satisfy that the AI is behaving as intended and not in an arbitrary or discriminatory manner.

Governance frameworks should also be established to oversee the AI lifecycle. From data management, model training, validation and deployment to ongoing monitoring, issues such as data bias must be carefully managed.

If, for example, the training data for an AI system involved in anomaly detection mostly come from certain network segments, there is a question over whether the AI should generalize across all network segments. A telecommunications provider's datasets might have imbalances – for example, more data from urban networks than rural, or more data on home network users compared to roaming users. Because of this, governance should enforce practices that retrain or tune models for diverse conditions, ensuring no part of the network is left with blind spots. Additionally, cybersecurity AIs themselves need security. There should be policies to protect AI models and data from tampering – for instance, in adversarial attacks where hackers try to poison the training data or trick the model with specially crafted inputs.

4.1.2 Compliance and risk

Telecoms providers in the GCC and globally are subject to various regulations, such as national cybersecurity frameworks and data privacy laws. Examples include the General Data Protection Regulation (GDPR) in Europe, or the Personal Data Protection Law (PDPL) in Saudi Arabia.

There may also be security requirements that are specific to telecommunications providers, such as lawful interception readiness. Any AI solution that touches customer data must comply with existing privacy mandates. If, for example, customer behavior for adaptive authentication is being used, providers must ensure that this is allowed under privacy policies and that data is handled lawfully.

In addition, telecommunications sector security regulations often call for robust risk management and auditing. The European Union Agency for Cybersecurity (ENISA) has guidelines and threat landscapes for 5G, for example.

While not directly regulating AI, ENISA does expect operators to manage risks in new technology, such as AI. In the United Kingdom, the Telecom Security Act and its Code of Practice require telecoms to secure networks at all layers. Using AI can help meet that requirement, but operators must also ensure that the AI controls themselves are auditable and don't inadvertently violate obligations, such as emergency call availability – an AI system should not block emergency communications erroneously. Compliance extends to demonstrating to regulators how AI is used. We may therefore see regulators asking for evidence of AI oversight, a process akin to how banks must validate their AI models to financial regulators.

4.1.3 Ethics and trust

Ethical use of AI is also crucial for maintaining trust. This includes avoiding practices that might unfairly target or impact certain user groups. For instance, an AI fraud system should not unwittingly have biases that flag prepaid users more often than postpaid simply because of data biases.

Telecommunications providers should also align with broader AI ethics principles such as fairness, accountability, and transparency. Indeed, many frameworks, such as AI RMF and the EU's AI Act, highlight this requirement. Some providers might set up an internal AI ethics board or committee to review new AI uses, especially those affecting customer-facing decisions.

On the internal side, trust in AI among staff needs fostering. If SOC analysts or network engineers are skeptical of the AI's recommendations, they might ignore or override them, negating the benefits. Thus, training and change management are part of governance. Teams should be shown how the AI works, involving them in tuning and gradually building confidence. A phased approach in which AI suggestions are initially reviewed by humans can also help, creating a feedback loop that improves the model and the team's trust simultaneously.

Another concrete step is the implementation of algorithmic accountability mechanisms. Essentially, these ensure that there are mechanisms for auditing, explaining and rectifying AI-driven decisions. If an AI makes a mistake – say, a false positive that cut off a service – there should be a process to analyze this and correct it by, for example, updating the model or adjusting its thresholds. This is very similar to how a safety incident would also be reviewed.

4.1.4 Enabling regulation

From the perspective of enablement, regulators in the GCC are supportive of innovation, but watchful. Saudi Arabia and the UAE, for example, have been quickly embracing digitalization with new strategies and regulations to ensure security is not left behind.

The UAE's 2025 National Cybersecurity Strategy explicitly aims to enable safe adoption of new technology. This implies that telecommunications providers using AI must do so under a coherent governance framework. Saudi Arabia's updated ECC would apply to telecommunications providers that are designated as critical infrastructure, requiring strong control over any systems, including AI. Telecommunications providers should thus anticipate that in the near future audits or requirements related to the reliability and explainability of AI systems will become part of compliance. Indeed, alignment with international standards, such as NIST's broader trustworthy AI work, which stresses validity, reliability, security, and the resilience of AI, can help operators demonstrate due diligence.

PRIORITY	GCC TELCOS (%)	GLOBAL TELCOS (%)
Explainability of AI models	82%	74%
Regulatory compliance	78%	80%
Bias and fairness auditing	64%	59%
Internal oversight mechanisms	70%	68%

Table 6: Key AI governance priorities for telecoms (survey data)

Source: Global Cybersecurity Forum (GCF), stc & Microsoft

In summary, establishing trust, governance, and compliance for AI means institutionalizing AI risk management within the telecom sector. This is not only a technical issue, but a legal and ethical one as well. Approached correctly, it can unlock AI's potential by ensuring there are guardrails and accountability. Customers can trust that their carrier's AI will protect them from fraud and other issues without violating their privacy or rights. Regulators can trust that AI helps improve security and continuity, rather than introducing uncontrolled risks. Internally, leadership can trust AI deployments are contributing to strategic goals and are not just "black boxes".

5.Maturity and investment models

For many telecoms providers, adopting AI in cybersecurity is a journey that unfolds in stages. Having a clear view of the maturity model and aligning investments to the development of capability is crucial.

This section discusses how telecommunications providers can assess their current status, plan for scaling AI capabilities and ensure they invest wisely to get the best returns on AI initiatives.

Maturity models provide a structured way to gauge how advanced an organization is in leveraging AI for security. At a basic level, a telecoms provider might start with automation of simple tasks, such as scripts and basic anomaly rules. This would be a low maturity stage, where AI/ML usage is minimal. Then, they might progress to using point solutions with ML, such as a specific, AI-based fraud detection tool or an AI-enhanced SIEM for correlation. Next, a more mature stage involves integrating AI across multiple SOC processes and establishing an orchestrated approach. The highest maturity might be an autonomous security environment with continuous learning, organization-wide AI governance, and perhaps even a predictive/prescriptive security strategy guided by AI analytics.

Assessing maturity involves looking at four dimensions in particular: strategy and culture, technology and data, process integration and skills.

With the first, an assessment would ask if the leadership was prioritizing AI and teams understood its value. The second would examine if the necessary data pipelines and tools were in place; the third would involve looking at whether AI outputs are properly embedded in workflows. Finally, the skills dimension means determining whether staff have an understanding of data science or AI, or if they instead rely solely on vendors.

Given the current shortage of telecom cybersecurity professionals, it is imperative to provide comprehensive training in both telecommunications cybersecurity and AI in order to develop a highly skilled workforce equipped to tackle evolving threats.

5.1 Investment

The recent Boston Consulting Group (BCG) IT benchmarking study of telecom providers TeBIT 2024,[15] found that while providers saw AI as a key solution and their AI maturity was on par with other industries, they still might not be investing enough.

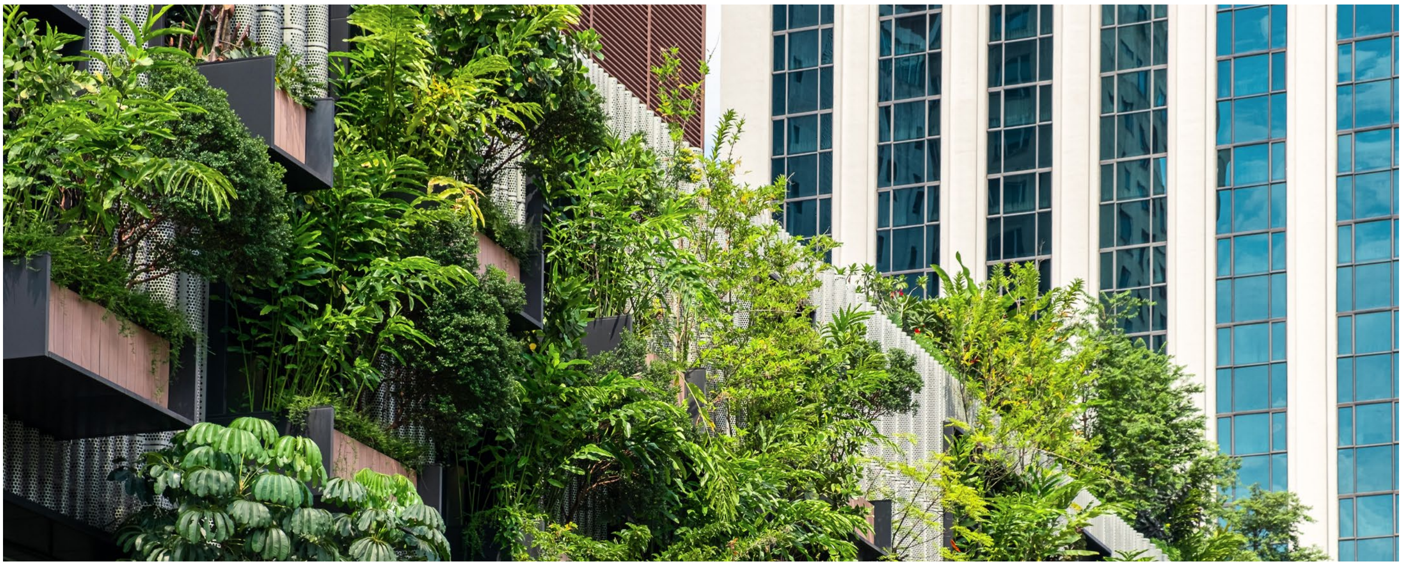
On average, telecommunications providers' AI spending was only 0.16% of revenues in 2023, a figure lower than the global cross-sector average of 0.42% . This suggests that to reach higher maturity, many telecoms providers will need to boost investments and treat AI as a core part of their business transformation, rather than as an add-on. The BCG study implies that providers should plan AI investment volume and priorities more strategically, rather than undertake piecemeal efforts.

In this context, 'investment models' mean having a roadmap and business case for AI's use in security. When allocating budgets, the executives and boards of telecommunications providers need to be convinced of the benefits of bringing AI onboard in terms of return on investment (ROI) and risk reduction. To do this, it can be helpful to map AI use-cases to business outcomes. As an example, the case might be made that AI-driven SIM swap detection could save X amount in fraud losses annually and protect customer trust, or that AI SOC automation could allow the provider to handle five times the number of alerts with the same amount of staff – avoiding Y amount in additional headcount cost, while also improving incident response by Z%. Quantifying these benefits helps justify investments.

Many telecommunications providers initially pilot an AI use case in a contained area – deploying an AI anomaly detector in the core network only, for example. They then measure the results. If positive, the provider might scale the AI more broadly. This phased investment approach aligns with proving value, learning and then expanding.

Another aspect is building versus buying AI capabilities. Mature organizations often invest in building internal data science teams and customizing AI models to their unique data. This is especially the case with big operators with resources. Others might rely on vendor solutions or cloud AI services for faster time-to-value.

Both require investment – either capital expenditure (Capex) in hiring and developing, or operational expenditure (Opex) in procuring services. As highlighted in the previous section, governance also requires investment. This might be, for instance, in implementing a data lake for security logs, labeling data for model training, or tools for model monitoring. These expenditures are often overlooked in budgets, but are essential for long-term success.



5.2 Readiness and training

Before jumping into advanced AI, telecommunications providers must ensure the foundational elements are in place. These include comprehensive data collection, because if logs are incomplete or siloed, AI cannot provide a magical solution: if bias exists in training datasets, bias will be present in outcomes.

Other key foundational elements include the availability of the computing infrastructure for AI workloads, along with a cybersecurity architecture that can integrate AI outputs. This might consist of a SOAR platform that can take automated actions.

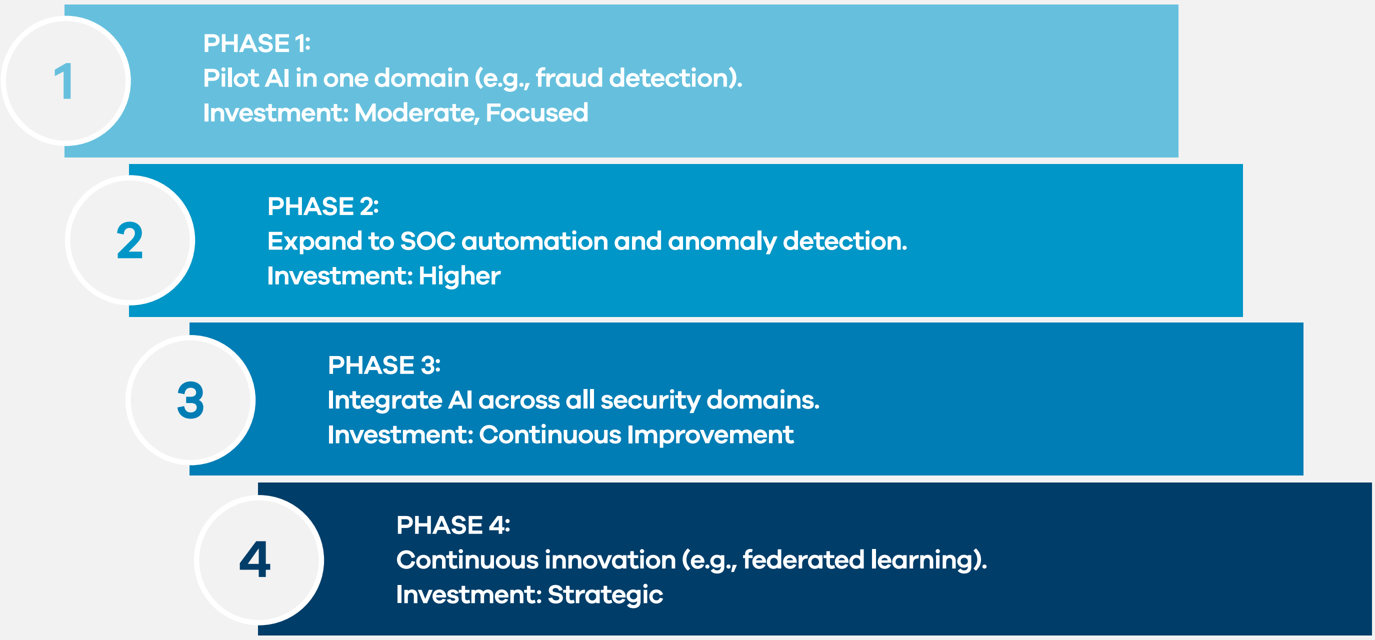
Some organizations use a readiness assessment checklist that covers the above bases. Only when the basics are solid does it make sense to implement a cutting-edge deep learning solution, for example.

In addition, for AI adoption, training the workforce is as crucial as the technology. A telecommunications provider might invest in upskilling security analysts with basic AI and ML concepts and applications, and/or train them on effective prompt engineering.

At the same time, to be effective, in-house data scientists need training on telecommunications domain specifics, such as network protocols and types of telecom fraud.

The intersection of telecommunications engineering and AI is also a niche that needs cultivation. Some leading providers partner with universities or run innovation labs focusing on AI in networks and security.

When scaling AI capabilities, an iterative, capability-building model is beneficial. Figure 4 provides an illustrative example.



1 PHASE 1:
Pilot AI in one domain (e.g., fraud detection).
Investment: Moderate, Focused

2 PHASE 2:
Expand to SOC automation and anomaly detection.
Investment: Higher

3 PHASE 3:
Integrate AI across all security domains.
Investment: Continuous Improvement

4 PHASE 4:
Continuous innovation (e.g., federated learning).
Investment: Strategic

Figure 4: The four-phases AI adoption

- **Phase 1:** Pilot AI in one domain – for example, fraud detection. Learn from it, establish governance frameworks. Level of investment: moderate, focused.

- **Phase 2:** Expand to SOC automation and network anomaly detection. Level of investment: higher, building on the success of Phase 1 to perhaps purchase enterprise AI-SOC platform.

- **Phase 3:** Integrate AI across all security domains and fine-tune collaboration between them – for example, threat intelligence AI informs SOC AI. Level of investment: in continuous improvement, specialized talent and potentially, AI research partnerships.

- **Phase 4:** Continuous innovation and evaluation of new AI technologies. These could include federated learning to share threat models without sharing raw data, or, in the future, quantum-resistant AI security, if relevant.

The maturity model also ties in to measuring success. Telecommunications providers should track metrics such as the reduction in incidents, faster response times and fewer customer complaints related to security.

They should also track compliance audit results and ultimately how AI is contributing to the bottom line by preventing losses or improving operational efficiency. These KPIs will inform decisions over whether further investment is warranted or needs redirection.

Importantly, the enablement part of this pillar is about empowering the organization to adopt AI. That might involve creating cross-functional teams involving network engineers, security, and data scientists all working together on AI projects. It might also mean fostering a culture that is data-driven and encouraging innovation while managing risks.

Executives and security leaders working for telecoms providers should champion an AI-enabled vision – one in which instead of viewing security as a cost center, it is seen as a competitive differentiator. An example of this would be in being able to market to customers that the provider uses advanced AI to keep their communications secure. This could be a significant trust and brand value point.

5.3 Regional funding

GCC telecommunications providers often have strong national support backing and even mandates to be at the forefront of technology. This is certainly the case with the national AI strategies of the UAE and Saudi Arabia.

The region's leaderships recognize AI as transformative, which can be an advantage in securing funding for ambitious AI initiatives. Organizations in the Middle East have been quick to adopt generative AI, for example, though many are still exploring how to get optimal benefit from this. This suggests a willingness to invest, but also underscores the point that investment must be tied to outcomes. Indeed, a recent McKinsey report, The state of gen AI in the Middle East's GCC countries: A 2024 report card[16], indicates the likely need to translate adoption into tangible results.

For telecommunications providers' security, GCC players can set a benchmark by showcasing how strategic investments in AI yield safer networks.

As the critical nature of secure telecoms at global events hosted in the region indicates, this can be an important message in attracting businesses and events.

In conclusion, maturity and investment models guide telecoms to methodically build AI capabilities, rather than invest in one-off deployments. By understanding where they stand and plotting a course to the next maturity level, operators ensure that each dollar (or riyal/dirham) spent on AI contributes to a stronger, smarter defense posture. By aligning those investments with governance (Pillar 4) and tactical needs (Pillars 1–3), they can create a sustainable, resilient security program.

9. Conclusion

Telecommunications providers sit at the heart of digital society, enabling everything from personal communications to national infrastructure. This central role makes them high-value targets for cyber adversaries – whether those be financially motivated fraudsters, hacktivists seeking disruption, or state-sponsored groups engaging in cyber warfare.

The evolving threat landscape for telecom providers is therefore characterized by higher stakes, greater complexity, and greater volume than ever before. To meet this challenge, the industry is undergoing a paradigm shift in cybersecurity – with AI at its core.

Although AI is not a complete solution, it can provide powerful capabilities across the security spectrum. These range from threat anticipation to defense fortification and from supercharging responses to ensuring robust oversight. In threat identification, AI-driven intelligence and anomaly detection can unveil hidden risks, such as stealth network intrusions and insider plots, much earlier and more accurately than traditional means. In defense and detection, AI can act as a real-time guardian, filtering out attack traffic, flagging zero-day exploits by behavior and continuously validating identities and accesses. This moves telecommunications security towards a true, zero-trust model in which every anomaly is scrutinized. During response and recovery, AI can become the tireless assistant of human teams, eliminating alert overload, piecing together incidents in seconds, and even executing parts of the response playbook automatically, thereby minimizing damage and downtime. Underpinning all of this is governance and enablement – ensuring that AI is used wisely, ethically and effectively, with clear accountability, regulatory compliance and strategic alignment guiding its deployment.

For executives and security leaders in telecoms, a few strategic insights emerge:

- **Integrate AI with a purpose:** Rather than sporadic AI experiments, develop a clear strategy aligning AI use cases with your most pressing threat scenarios and business needs. For example, if subscriber fraud is causing reputational damage, prioritize AI solutions in fraud detection and identity verification. If nation-state threats are a concern, invest in AI-enhanced network monitoring and threat intelligence sharing, leveraging frameworks such as MITRE FiGHT to inform defenses. Providers should ensure each AI initiative also has defined success metrics, such as a reduction in incident response time or losses to fraud.

- **Focus on data and infrastructure readiness:** AI's effectiveness is directly tied to data quality and availability. Break down silos between network operations, IT and security data. Consider building a unified data lake for security events and investing in tools that facilitate real-time data processing. Modern telecommunications networks (5G and beyond) are software-defined and produce telemetry at scale. This should be harnessed with AI before network attackers do. Also, upgrade your infrastructure to handle AI workloads, whether these are on-premises graphics processing unit (GPU) clusters or cloud-based AI services, securing those platforms.

- **Augment, don't replace – keep humans in the loop:** Use AI to handle the volume and do the heavy lifting, but maintain human oversight – especially for high-impact decisions. Cultivate an AI-savvy workforce by training analysts to understand AI outputs and to feed their domain knowledge back into AI tuning. The goal is a human-AI symbiosis; AI offers unprecedented speed and pattern recognition, while humans provide context, intuition and ethical judgment. Together, they form an intelligent defense that is greater than the sum of its parts.

- **Strengthen governance and build trust:** Establish an AI governance framework as part of your corporate governance. Treat AI models similarly to how you treat financial models or critical IT systems. This means validation, periodic audits and continuous monitoring. Document the decisions taken and ensure explainability, especially for any AI that has customer impact. Pro-actively engage with regulators, demonstrating how your AI-driven security measures enhance resilience and protect user data. This could be done, for instance, by showing how AI cut SIM swap incidents by X%, thereby protecting consumers – a narrative regulators will appreciate. Leading with transparency can turn compliance into a competitive advantage, assuring customers that security is rigorous and accountable.

- **Collaborate and share knowledge:** Cybersecurity is a team sport, and this extends to AI in security. Consider partnerships with academia, startups and industry consortia to stay at the cutting edge of AI techniques. Participate in telecom information-sharing groups, potentially sharing anonymized threat data to improve AI models and building collective defense. The GCC and MENA regions, in particular can, benefit from a collaborative approach, given shared threats and the presence of major events, which can often attract attacks. By pooling AI insights on attacks, regional operators can create a united front, aligning with the knowledge-sharing ethos behind initiatives in global threat intelligence and frameworks such as Mitre FiGHT and GSMA MoTIF.

- **Plan for continuous evolution:** The threat landscape will not stand still and neither will AI technology. Today's ML models may give way to more advanced forms, including: federated learning, in which carriers could jointly train models without sharing raw data; and the deployment of more explainable AI, as the field matures – making regulators and operators even more comfortable with AI decisions. Also prepare to update your AI tools and models regularly. Security AI is not a one-and-done product, but a constant learning process. In addition, keep an eye on adversaries using AI for social engineering and/or automated attacks; defensive AI must innovate to counter offensive AI.

The GCC region's drive to be a global technology and digital hub comes with the responsibility of robust cybersecurity. As highlighted, GCC nations are heavily investing in cybersecurity resilience, upskilling their workforces and embracing advanced technologies. By strategically leveraging AI for telecom cybersecurity, the region's operators can not only protect their critical communications infrastructure, but also set global benchmarks for how AI can be deployed at scale to secure the next generation of networks.

This will enable the trusted digital ecosystems required for initiatives such as smart cities, digital economies and IoT deployments that feature prominently in national visions.

Intelligent defense is the way forward – an adaptive, AI-empowered cybersecurity posture that learns and improves continuously to outsmart threats.

Telecoms that adopt this approach will be better positioned to safeguard their customers, ensure service reliability and maintain trust in an era where connectivity is as fundamental as electricity. The strategic role of AI in telecom cybersecurity is no longer optional; it is becoming central to defending the networks that connect our world. By embracing the four pillars outlined above – from foresight in threat identification to rigorous governance – telecom leaders can transform their security from a reactive shield into a proactive, intelligent defense system ready for the challenges of 2025 and beyond.

Endnotes

1. MITRE (September 2025). 5G Hierarchy of Threats

2. Palo Alto Networks (November 2024). Unit 42 Predicts the Year of Disruption and Other Top Threats in 2025

3. Forrester (September 2025). New Technology: The Projected Total Economic Impact of Microsoft Copilot + PCs

4. CIFAS (September 2025). This Is Fraudscape 2025

5. Microsoft (September 2025). Digital Defense Report 2023

6. CIFAS (September 2025). 1055% Surge in Unauthorised SIM Swaps as Mobile and Telecoms Sector Hit Hard by Rising Fraud

7. Thomson Reuters Institute (September 2025). A Deep Dive into the Growing Threat of SIM Swap Fraud

8. Artificial Intelligence Review (September 2025). AI-Driven Advances in Anomaly Detection for Telecom Networks

9. The Business Research Company (September 2025). AI in Cybersecurity Market Report 2025

10. SiliconANGLE (September 2025). How Palo Alto Networks Is Forging a Collaborative Future for 5G Security

11. ETSI (September 2025). A Vision for Communications Security

12. Subex (October 2024). How AI Enhances Anomaly Detection to Prevent Telecom Frauds

13. Culminate Security (July 2025). From 10,000 to 10: How AI Identifies Which Alerts Actually Matter

14. Forrester (November 2024). New Technology: The Projected Total Economic Impact of Microsoft Security Copilot

15. BCG (September 2025). 2024 Executive Report: Smart AI Usage for Telcos

16. Quantum Black AI by McKinsey (September 2025). The State of GenAI in the Middle East's GCC Countries: A 2024 Report

GLOBAL
CYBERSECURITY
FORUM

stc