Ericsson White Paper
GFTL-23:001720 Uen
April 2026

ERICSSON

150 years

Automated threat hunting in telecom networks

Content

Executive summary 3

The Threat Hunting Gap: Why Traditional Defenses Fall Short **5**

Limitations of existing automation approaches 6

Market evolution: increasing complexity and attack surface in telecom networks 7

Threat landscape evolution: sophisticated, stealthy, and telecom-specific attacks 7

Human in the Loop: limitations of traditional and manual hunting approaches 7

From Reactive Detection to Proactive Hunting **8**

Ericsson's advocated approach 9

Advantages and impact 10

Consequences of not investing in threat hunting 10

Conclusion **11**

Key actions encouraged by this WP 12

Strategic implications 12

References **13**

Glossary **14**

Authors **15**

Executive summary

As networks evolve toward 5G and future 6G, they become more dynamic, data rich, and interconnected, making manual and reactive security approaches no longer sufficient. Advanced threat actors, such as those behind long-running campaigns like Liminal Panda and Salt Typhoon, exploit telecom-specific signaling protocols, roaming interfaces, or similar telecom-specificities to stage highly complex attacks. They may further exploit distributed, multi-layered, cloud-native network functions to remain undetected. These threat actors can then lie dormant in the networks for an extended period of time, making the reactive security approaches less efficient. In this case, there is a need for a proactive approach to hunt these threat actors down.

Threat hunting is a proactive security practice for searching across systems, networks, and data to uncover malicious activities that may evade traditional security defenses [1]. Despite its value in early detection and attack prevention, threat hunting is labor-intensive, time-consuming, and highly dependent on skilled analysts who must correlate diverse data sources, interpret subtle indicators of compromise, and continuously adapt to evolving attacker behaviors. This WP presents automated threat hunting in telecom environments, addressing the unique challenges of telecom protocols, distributed architectures, and cross-domain attack propagation.

This paper explores how automation can enable proactive, continuous, and scalable threat hunting across complex telecom infrastructures from a business perspective.

In fact, automation reduces the dependence on scarce expert analysts, shortens detection and investigation time, and lowers operational costs associated with large-scale security monitoring. It also helps telecom operators improve service resilience, protect critical infrastructure, and reduce the financial and reputational impact of security incidents and service disruptions.

This paper explains how automated threat hunting in telecom networks enhances speed, depth, and scale of investigations, reduces analyst workload, and strengthens defenses against stealthy, sophisticated adversaries. It highlights key gaps in current approaches and introduces a general framework for automated hypothesis generation, testing, and validation across telecom-specific data sources such as control-plane signaling, network functions, and cloud-native observability pipelines. It also explains how telecom network providers occupy a unique position by combining deep telecom domain expertise, visibility across network layers, and advanced analytics capabilities, telecom providers are well-positioned to deliver automated threat hunting tailored to telecom operators' operational realities. By adopting the strategies outlined in this paper, telecom providers can significantly strengthen their resilience against advanced persistent threats and secure next-generation mobile infrastructure at scale.

The Threat Hunting Gap: Why Traditional Defenses Fall Short

Effective threat hunting requires a deep understanding of security principles, telecom infrastructure, and the broader operational environment, as well as significant human expertise [2].

In telecom networks (see Figure 1), this challenge is amplified by the scale, heterogeneity, high availability, and criticality of the infrastructure [3]. The 5G networks and future 6G networks with their cloud-native architectures and the upcoming autonomous networks, are making traditional and manual threat hunting approaches increasingly insufficient.

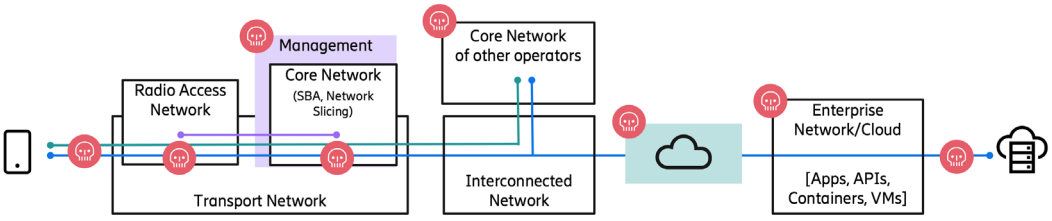


Figure 1. Attack surface in telecom networks.

Limitations of existing automation approaches:

- **Rules/ Security Information and Event Management(SIEM)-led hunting:** This approach is effective for known threats because it relies on predefined indicators of compromise and correlation rules. However, it is inherently static and struggles in telecom environments, where stealthy attacks often abuse legitimate signaling and service interactions rather than exposing clear, known indicators.
- **Security Orchestration, Automation, and Response in telecom (SOAR) /playbook automation:** SOAR reduces analyst workload by automating repetitive investigation and response tasks. Its limitation is that it mainly automates execution steps, not more advanced reasoning needed to generate new hunt hypotheses or connect weak signals across telecom domains.
- **Machine learning anomaly detection:** Anomaly detection can help identify unknown threats, but in telecom networks the notion of normal behavior is constantly shifting due to mobility, roaming, and dynamic service operation. As a result, baseline-driven models often miss stealthy long-dwell attacks or generate too many false positives.
- **Threat-intel frameworks (ATT&CK/FiGHT/MoTIF):** These frameworks are valuable for standardizing adversary behaviors and enriching investigations with known tactics and techniques. However, they do not by themselves automate hunting and still require a telecom-aware model to connect tactics, techniques, procedures (TTPs) to large-scale operators' telemetry and operational context.

Automating threat hunting is therefore essential but requires addressing fundamental technical, operational, and organizational challenges specific to telecom environments. In the following, we outline the key challenges that must be addressed to enable scalable, automated threat hunting in modern telecom networks.

Market evolution: increasing complexity and attack surface in telecom networks

The telecom industry is undergoing a fundamental transformation driven by 5G, virtualization, cloud-native network functions, and the proliferation of internet of things (IoT) devices. This evolution significantly expands the attack surface and introduces new threat vectors. Key technology and architectural shifts include cloud-native 5G core and network function virtualization (NFV), distributed and heterogeneous infrastructure, and massive growth in connected devices (IoT, mobile, critical infrastructure).

Threat landscape evolution: sophisticated, stealthy, and telecom-specific attacks

Modern threat actors use advanced techniques specifically designed to evade detection in telecom environments. Examples of telecom-specific threats include signaling-level attacks and roaming interface, for example, advanced persistent threats.

Human in the Loop: limitations of traditional and manual hunting approaches

Traditional threat hunting relies heavily on human analysts to

- formulate threat hypotheses
- analyze logs and telemetry
- correlate events across multiple systems
- identify suspicious behavior

However, this approach does not scale in telecom environments due to several fundamental limitations:

- massive volume and diversity of telemetry data
- lack of end-to-end visibility across distributed domains
- high reliance on scarce telecom security expertise
- reactive security models are insufficient

From Reactive Detection to Proactive Hunting

As operators move to cloud-native 5G cores and distributed computing, attackers can blend into normal signaling and operations for long periods. A well-known example is Liminal Panda, which targeted telecom infrastructure and remained undetected for years.

Ericsson's advocated approach:

Our approach is based on knowledge-guided, graph-driven hunting automation [4] for threat hunting (see figure 2). Ericsson advocates automating hunting as part of the security management plan using

- knowledge discovery and reasoning for hypothesis generation
- a telecom security knowledge graph to correlate weak signals across domains
- standards-based attribution using MITRE ATT&CK and MITRE FiGHT

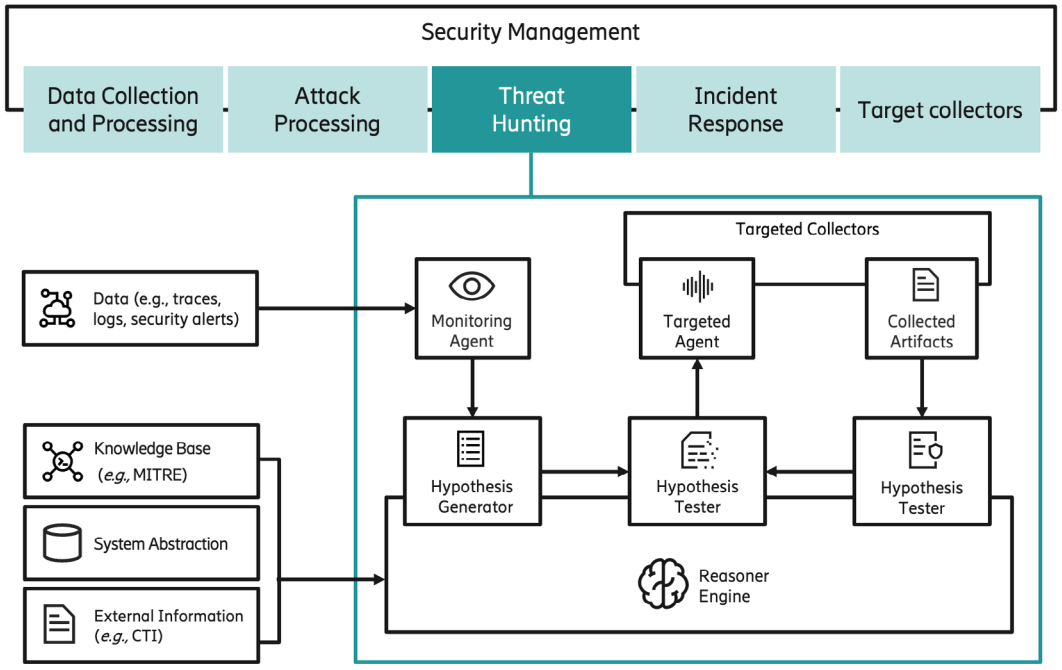


Figure 2. Automated threat hunting loop.

This can be achieved by implementing a system that ingests telecom and cloud telemetry from multiple layers, including signaling and control-plane activity, network function logs, service-based architecture and API interactions, as well as Kubernetes and broader cloud events, then normalizing and labeling these data streams into a knowledge graph aligned with MITRE ATT&CK and FiGHT.

Within this graph, key entities such as network functions, subscribers, sessions, clusters, and identities are represented as nodes, while operational relationships such as service calls, authentication events, configuration changes, and roaming activities are captured as edges. On top of this representation, the system generates and prioritizes investigation hypotheses by combining graph-based pattern analysis with statistical change detection to identify suspicious behaviors, such as previously unseen or rare network function (NF)-to-NF communication paths or abnormal access patterns associated with roaming activity. It then automates investigation by traversing the most likely attack paths and bundling the relevant evidence, ultimately producing attribution and reporting outputs mapped to ATT&CK techniques and FiGHT 5G security use cases to support consistent reporting, coverage assessment, and security operations tracking.

Advantages and impact:

The main advantage of this approach is that it enables earlier detection of stealthy advanced persistent threats [5] that unfold gradually across multiple systems and over extended periods, which is a common failure mode where isolated alerts often miss the broader attack progression. It also reduces the analysts' workload by minimizing the need for ad hoc querying and replacing it with repeatable, explainable hunting outputs built around explicit threat hypotheses and supporting evidence. Beyond the operational efficiency, the approach produces operator-ready assurance artifacts through ATT&CK- and FiGHT-aligned reporting, which strengthens governance, supports audits, and enables continuous improvement of detection coverage and security posture over time.

Consequences of not investing in threat hunting:

Not investing in threat hunting increases the likelihood that adversaries and advanced threats will remain undetected for long periods, giving them more opportunities to establish persistence and move laterally across roaming, core, and edge domains before defenders recognize the full scope of the intrusion. In telecom environments, where attackers often unfold across distributed and interdependent systems, this extended dwell time significantly raises the risk of silent compromise and broader operational exposure. It also leads to higher financial and operational costs, since delayed detection and containment typically allow incidents to escalate, making response more complex, disruptive, and resource-intensive while increasing the potential impact on service continuity, customer trust, and regulatory posture.

Conclusion

As telecom networks become society-critical infrastructure, operators face increasingly sophisticated and stealthy cyber threats that cannot be reliably detected using traditional, reactive security tools alone. Threat hunting, while essential for identifying these advanced threats, remains heavily dependent on scarce expertise and manual effort, making it difficult to scale across complex, distributed, and cloud-native telecom environments. At the same time, regulatory and industry trends are moving toward mandatory, proactive threat hunting, reinforcing the need for automation and standardized, intelligence-driven approaches.

This WP highlighted automated threat hunting as a strategic capability that enables telecom operators to continuously monitor, early detect, and investigate advanced threats at scale. By leveraging telecom-aware knowledge models, machine learning, artificial intelligence, and standards-based attribution (e.g., MITRE ATT&CK and FiGHT), automation makes threat hunting faster, more consistent, and operationally sustainable. This shift transforms threat hunting from an expert-driven, reactive activity into a proactive, scalable, and intelligence-driven security capability.

Key actions encouraged by this WP:

Telecom operators, security leaders, and technology decision-makers should:

- recognize automated threat hunting as a strategic security capability, not just an operational enhancement, particularly as networks evolve toward cloud-native and distributed architectures
- assess current threat hunting maturity, including visibility gaps, manual dependencies, and the ability to correlate events across core, edge, and cloud environments
- invest in automation platforms that integrate telecom-specific knowledge, automation, and threat intelligence, enabling scalable hypothesis generation, investigation, and attribution
- align threat hunting practices with industry standards and frameworks such as MITRE ATT&CK, MITRE FiGHT, and security guidance to improve detection coverage, reporting, and interoperability
- incorporate automated threat hunting into long-term security and infrastructure planning, especially for 5G, edge computing, distributed computing architectures, and future network evolutions

Strategic implications:

Organizations that adopt automated threat hunting will strengthen their ability to detect and respond to advanced threats earlier, reduce operational burden on security teams, and improve resilience across critical telecom infrastructure. Conversely, organizations that delay this transition risk longer attacker dwell times, reduced visibility into advanced threats, and increased difficulty securing complex, cloud-native telecom environments.

References

1. A Survey on Threat Hunting in Enterprise Networks
https://ieeexplore.ieee.org/document/10216378
2. An Interview Study on Third-Party Cyber Threat Hunting Processes in the U.S. Department of Homeland Security
https://www.usenix.org/system/files/usenixsecurity24-maxam.pdf
3. Unveiling the Hunter-Gatherers: Exploring Threat Hunting Practices and Challenges in Cyber Defense
https://www.usenix.org/system/files/usenixsecurity24-badva.pdf
4. Automa: Automated Generation of Attack Hypotheses and Their Variants for Threat Hunting using Knowledge Discovery
https://ieeexplore.ieee.org/document/10477575
5. Securing networks against sophisticated threats:
https://www.ericsson.com/en/blog/north-america/2025/securing-networks-against-future-threats

Glossary

ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
FiGHT	Five-G Hierarchy of Threats
IoT	Internet of Things
MoTIF	Mobile Threat Intelligence Framework
NF	Network Function
NFV	Network Function Virtualization
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
TTP	Tactics, Techniques, Procedures

Authors

Boubakr Nour: Boubakr's research is focused on proactive security and automated threat hunting. He has published over 60 papers in peer-reviewed journals and international conferences. Alongside his role at Ericsson Research in Canada, which he joined in 2022, he serves as an Affiliate Assistant Professor at the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University in Montréal, Canada. He holds a Ph.D. in Computer Science and Technology from the Beijing Institute of Technology in China.

Dr. Makan Pourzandi is a research leader at the research department, Ericsson, Canada. He received his Ph.D. degree in Computer Science from University of Lyon I Claude Bernard, France and M.Sc. in parallel computing from École Normale Supérieure de Lyon, France. He has more than 20 years of experience in the fields of cyber security, Telecom and distributed systems. He co-authored two books on cyber security published by Springer on auditing in cloud environments and software security. He is the co-inventor of 25 granted US patents. He has published more than 80 research papers in peer-reviewed scientific journals and conferences. His current research interests include cyber security, cloud computing, software security engineering.

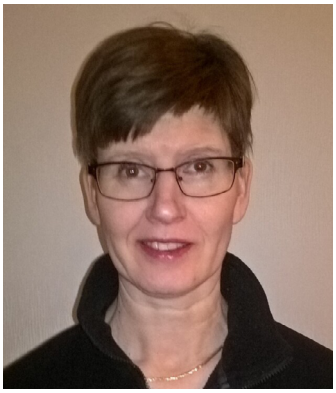
Eric Sisi: Eric is an industry veteran with strong international experience in defence, enterprise computing and security business. Eric served in the Canadian Military, then went on to manage businesses and services at a senior levels in Europe, The Middle East and Asia. Eric has strong information security experience, having spent more than 15 years in the information security industry. Eric has a Bachelor of Computer Engineering from The Royal Military College of Canada and a Masters of International Business Law from the University of Liverpool.

Eric is the Portfolio Director - Security at Managed Services. With the responsibility of developing the managed security services that benefit our telecommunications customers, Eric also maintains strong dialog with customers and regulators on the many challenges with security in the telecommunications sector.

Eva Fogelström is director of the Security Research department within Ericsson Research. She holds a Ph.D. in Telecommunications and an M.Sc. in Electrical Engineering, both from KTH Royal Institute of Technology in Stockholm, Sweden. Eva has been with Ericsson since 1997, working in the fields of security, mobility and standardization.

Jan Willekens: I am a get-things-done security executive with a drive to constantly be one step ahead of adversaries. I've followed the classical path from developer and infrastructure engineer, to IT solutions and security architect, progressing via enterprise architect to leadership roles. Throughout my career I've built and improved, from data centers in the early days, security in financial products and services later on, to SOC, CSIRT or threat intel teams more recently. My current focus is on maturing security teams, ensuring they are ready when the next big one hits and preparing them for TTPs which we currently have not been able to imagine yet.

Jesus Alatorre: Jesus Alatorre serves as an AI Incident Responder at Ericsson, where he established a dedicated AI unit within the Cyber Defense Center (CDC). He specializes in custom machine learning architectures, AI security research, and enhancing enterprise cyber defense capabilities. With an academic foundation in Mathematics and a deep history of leading security investigations as a Threat Hunter, Jesus translates state-of-the-art research into practical defense mechanisms, recently achieving a proprietary technology patent. Additionally, he acts as an internal algorithmic advisor and collaborates on creative red teaming initiatives to fortify AI-driven security infrastructures.



Leena Mattila: Leena works in the Ericsson Product Security Incident Response Team (PSIRT) as a threat intelligence specialist. She is one of Ericsson's representatives in the GSMA Fraud and Security Working Groups. She has a solid background in telecom networks and telecom-related protocols and her current work is focused on security threats in these networks and protocols.

Leena holds an M. Sc. in Computer Science from University of Turku, Finland. She joined Ericsson in 1991 and has worked with product development, network design and product security.