PRACTICAL THREAT DETECTIONS FOR TELECOMMUNICATIONS

Whitepaper

January 2026

GLOBAL CYBERSECURITY FORUM

stc

GLOBAL CYBERSECURITY FORUM

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

GCF aims to catalyze socioeconomic change, push the boundaries of knowledge on critical cybersecurity topics and build the foundations for global co-operation on key challenges and opportunities in Cyberspace.

By uniting decision makers and thought leaders from around the world, GCF aligns with international efforts to build a safe and resilient Cyberspace that is an enabler of prosperity for all nations and communities.

stc

stc, as the leader in ICT services in the Middle East, has grown beyond telecommunications to connect the world, enrich lives, and drive digital transformation. Through world-class infrastructure, emerging technologies, and a strong commitment to sustainability, stc empowers communities, businesses, and industries in Saudi Arabia, the region, and beyond. stc's investments are pivotal in establishing Saudi Arabia as a major digital hub, enabling the digital ambitions that are redefining industries and enhancing lives in society.

Guided by its values of drive, devotion, and dynamism, stc addresses environmental and social challenges while upholding strong governance, ensuring a secure, sustainable, equitable, and digitally empowered future for all.

Foreword

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

As telecommunications networks become ever more complex and data-driven, it is essential that our approach to threat detection keeps pace.

This work highlights a path forward in which we harness the data we already collect, aligning it with regulatory expectations, and applying advanced analytics to achieve scalable, high-fidelity detection. By embedding telemetry as a cornerstone of security operations, we can close visibility gaps, strengthen identity-centric controls, and better understand emerging threats.

I would like to thank all our contributors for their expertise and insight in shaping this whitepaper. By bringing together diverse perspectives, we can build detection strategies that are effective and sustainable – ensuring that the networks underpinning our societies remain resilient, trustworthy, and open.

Authors

- **Tim Wadhwa-Brown,** Cisco
- **Amr Said,** Cisco
- **Tiju Johnson,** Cisco
- **Osama Hasan,** Cisco

Contributors

- **Nauman Khan,** stc
- **Abdulmajeed Aleid,** stc
- **Mohammed Imran Khan,** stc
- **Mohammed Yousuf Uddin,** stc
- **Islam Swelem,** stc
- **Saad Abuhlayel,** Orange

Knowledge Community: Safeguarding Future Networks & Emerging Technologies

In an increasingly interconnected world, the evolution of next-generation ICT technologies such as 6G wireless technology has emerged as a powerful catalyst. The profound implications and transformative power of this next wave of ICT technologies demand immediate attention – both to navigate its complexities and to harness its capabilities for the benefit of society. The Knowledge Community 'Safeguarding Future Networks & Emerging Technologies' is committed to promoting and safeguarding today's ICT networks, bringing together a diverse array of expertise from multiple stakeholder groups. The community welcomes ICT providers, telecom companies, telecom industry players, cybersecurity research organizations, infrastructure operators, reputable think tanks, academia, and all stakeholders with a vested interest in the security of ICT networks.

Contents

Foreword

Useful Acronyms & Glossary 5

Executive Summary 11

Introduction 12

Key Findings 13

Analysis Methodology 15

1. Detection Requirements Identification 26

2. Priority Telemetry Sources 35

3. Conclusions and Recommendations 41

Bibliography 43

Appendix A: Descriptions of Telemetry Sources 44

Appendix B: Telemetry Source Matrix 47

Appendix C: Summary of Telemetry Evaluation 51

Useful Acronyms & Glossary

Term	Definition
3GPP	3rd Generation Partnership Project – global standards organization developing specifications for mobile telecommunications (3G, 4G, 5G).
5GC	5G Core – cloud-native core network architecture supporting 5G services.
5G SA	5G Standalone – 5G deployment using a native 5G core without LTE dependency.
AAA	Authentication, authorization and accounting – framework for managing subscriber and operator access in telecom networks.
ACL	Access Control Lists – rule sets that define which users, devices, or network traffic are permitted or denied access to systems or network resources.
AI	Artificial intelligence – technologies that enable systems to perform tasks that normally require human intelligence.
API	Application programming interface – a set of routines and protocols that enable communication between applications or systems.
AuC	Authentication Centre – telecom component that authenticates subscriber SIM/eSIM credentials.
BGP	Border Gateway Protocol – routing protocol used to exchange routing information between autonomous systems.
BSS	Business support systems – telecom systems supporting customer-facing processes such as billing, CRM and product management.
C2	Command and control – infrastructure and communication mechanisms used by attackers to manage and coordinate compromised systems.
CAPEX	Capital expenditure – upfront costs associated with infrastructure procurement and deployment.
CDR	Call Detail Record – data record produced by telecom equipment documenting details of voice or data sessions.
CMDB	Configuration management database – centralized repository that stores information about IT assets and their relationships.
CNF	Containerized network function – telecom network function deployed in containers rather than on dedicated hardware.
CPE	Customer-premises equipment – telecommunications or networking equipment installed at the customer's location.
CRM	Customer relationship management – system managing customer data, interactions and support.
CVE	Common Vulnerabilities and Exposures – publicly available catalog of known cybersecurity vulnerabilities.
DDoS	Distributed denial-of-service – attack that disrupts services by overwhelming systems or networks with excessive traffic.
DNS	Domain Name System – protocol and infrastructure that translates domain names into IP addresses; also used for service discovery in telecom networks.
DoH	DNS over HTTPS – protocol that encrypts DNS queries using HTTPS.

Useful Acronyms & Glossary

Term	Definition
DoT	DNS over TLS – protocol that encrypts DNS queries using TLS.
EDR	Endpoint Detection and Response – security solution that monitors endpoints for malicious activity.
EMS	Element Management System – platform used to configure, monitor, and manage individual network elements.
EPC	Evolved Packet Core – core network architecture for LTE networks.
eSIM	Embedded SIM – digital SIM that can be remotely provisioned without requiring a physical SIM card.
FiGHT™	5G Hierarchy of Threats – MITRE framework mapping adversary tactics and techniques in 5G networks.
GTP	GPRS Tunnelling Protocol – protocol used in mobile networks to carry user data and signaling.
HSS	Home Subscriber Server – central subscriber database in LTE networks.
HTTPS	Hypertext Transfer Protocol Secure – HTTP protected by TLS to provide confidentiality and integrity for web communications.
IAM	Identity and Access Management – framework and systems for managing digital identities and access rights.
IDS	Intrusion Detection System – security tool for monitoring network traffic and detecting malicious activity.
IMEI	International Mobile Equipment Identity – unique identifier assigned to a mobile device, used for device identification and network controls.
IMS	IP Multimedia Subsystem – framework for delivering multimedia services such as VoLTE and VoNR in telecom networks.
IMSI	International Mobile Subscriber Identity – unique identifier for a mobile subscriber stored in the SIM/eSIM, used for authentication and mobility.
IoA	Indicator of Attack – observable behaviors or patterns suggesting an attack is underway (often earlier-stage than an IoC).
IoC	Indicator of Compromise – forensic artifact that indicates potential intrusion or malicious activity.
IoT	Internet of Things – interconnected devices communicating over telecom or internet networks.
IP	Internet Protocol – network-layer protocol that provides addressing and routing so packets can travel across interconnected networks.
IPAM	Tactics, Techniques, and Procedures – adversary behaviors observed during attacks
IPFIX	Unified Data Management – subscriber database function in 5G networks
IPSec	IP Security – suite of protocols that encrypt and authenticate IP traffic (commonly used for VPN tunnels and site-to-site protection).
IT	Information technology – systems, networks, and software used to store, process, and transmit information in an organization.

Useful Acronyms & Glossary

Term	Definition
ITN	Intelligent Trusted Network – architecture concept focused on trusted connectivity, policy enforcement, and security controls across network domains.
KPI	Key Performance Indicator – measurable value indicating the effectiveness of a process or system.
LB	Load balancer – component that distributes client requests across multiple servers/instances to improve availability, scalability, and performance.
LBO	Local Breakout – routing where user traffic exits to the internet or local networks close to the access network, reducing backhaul/core traversal.
LDAP	Lightweight Directory Access Protocol – protocol for querying and managing directory services (users, groups, attributes) for authentication/ authorization.
LTE	Long-Term Evolution – 4G mobile broadband standard providing high-speed packet-based wireless connectivity.
MANO	Management and Orchestration – framework for lifecycle management and automation of VNFs/CNFs (deployment, scaling, healing, updates).
MAP	Mobile Application Part – SS7 signaling protocol used in 2G/3G networks for mobility, authentication, and roaming-related procedures.
MFA	Multi-factor Authentication – authentication method requiring two or more factors (something you know/have/are) to verify identity.
MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge – knowledge base of adversary behaviors across enterprise IT environments.
ML	Machine Learning – AI methods that learn patterns from data to make predictions or decisions without explicit rule-based programming.
MoTIF	Mobile Threat Intelligence Framework – GSMA framework describing mobile-specific adversary TTPs.
MPLS	Multiprotocol Label Switching – high-performance transport protocol used in telecom backbones.
NF	Network Function – logical network capability (e.g., AMF/SMF/UPF in 5G) providing specific control-plane or user-plane services.
NMS	Network management system – platform providing centralized monitoring and control of network devices.
NOC	Network Operations Center – team responsible for monitoring performance, availability and reliability of telecom infrastructure.
OPEX	Operational Expenditure – ongoing costs of maintaining and operating systems.
OS	Operating System – software that manages hardware resources and provides core services for applications.
OSS	Operations Support Systems – telecom systems supporting network operations such as service provisioning and fault management.
OTA	Over-the-Air – remote delivery of updates, profiles, or configuration to devices (e.g., firmware, carrier settings, eSIM profiles).

Useful Acronyms & Glossary

Term	Definition
OTP	One-Time Password – short-lived code used for a single authentication event to reduce replay risk.
PAM	Privileged Access Management – solution for controlling and auditing privileged user access.
PAWS	Privileged Access Workstation – hardened, dedicated endpoint used for administrative tasks to reduce exposure and protect privileged credentials.
P-GW	Packet Gateway – LTE/EPC core network function that connects the mobile network to external packet data networks and enforces policy/QoS/ charging for user traffic.
PKI	Public Key Infrastructure – framework for managing digital certificates and encryption.
PoC	Proof of Concept – limited demonstration to validate feasibility or value of a proposed solution before full implementation.
QoS	Quality of Service – mechanisms that prioritize and manage traffic to meet performance targets (latency, jitter, bandwidth, loss).
RAN	Radio Access Network – network connecting user equipment to the core network.
RDP	Remote Desktop Protocol – protocol enabling remote interactive access to a Windows desktop/session over a network.
RPKI	Resource Public Key Infrastructure – security framework for validating BGP route announcements.
SDH/SONET	Synchronous Digital Hierarchy/Synchronous Optical Network – standardized optical transport technologies for high-speed, time-division multiplexed backbone transmission.
SIEM	Security Information and Event Management – solution for centralized log collection, correlation and analysis.
SIM	Subscriber Identity Module – secure module (physical or embedded) storing subscriber credentials and identity information for mobile network access.
SIP	Session Initiation Protocol – signaling protocol used to establish, modify, and terminate real-time sessions such as voice and video (commonly within IMS).
SLA	Service-Level Agreement – contractually agreed performance metrics between service provider and customer.
SMS	Short Message Service – mobile network service for sending/receiving short text messages.
SNMP	Simple Network Management Protocol – protocol for monitoring and managing network devices using polling, traps, and managed objects (MIBs).
SOAR	Security Orchestration, Automation and Response – platforms that automate security workflows (triage, enrichment, containment) and coordinate response actions.
SOC	Security Operations Center – team responsible for monitoring and responding to cybersecurity threats.

Useful Acronyms & Glossary

Term	Definition
SQL	Structured Query Language – language for defining, querying, and managing data in relational databases.
SS7	Signaling System 7 – legacy telecom signaling protocol suite still used for interconnect and roaming.
SSH	Secure Shell – encrypted protocol for secure remote login, command execution, and tunneling.
SSO	Single Sign-On – authentication approach allowing a user to access multiple applications with one set of credentials/session.
STIX	Structured Threat Information Expression – standard format for representing and sharing cyber threat intelligence (actors, TTPs, indicators, relationships).
SUPI	Subscription Permanent Identifier – permanent 5G subscriber identifier (often concealed on the air interface via SUCI) used for subscriber identification.
TAXII	Trusted Automated eXchange of Intelligence Information – protocol for transporting cyber threat intelligence (often STIX) between systems.
TCPI	To-Complete Performance Index – project metric indicating the cost performance needed on remaining work to meet a specified budget target.
TLP	Traffic Light Protocol – information sharing classification (e.g., RED/AMBER/GREEN/CLEAR) that specifies distribution restrictions.
TLS	Transport Layer Security – cryptographic protocol providing confidentiality and integrity for data in transit (e.g., HTTPS, secure APIs).
TTP	Tactics, Techniques and Procedures – adversary behaviors observed during attacks.
UBA	User Behavior Analytics – detection approach that analyzes user activity patterns to identify anomalies and potential threats.
UDM	Unified Data Management – subscriber database function in 5G networks.
UE	User Equipment – end-user devices such as smartphones, IoT devices and customer premises equipment.
URL	Uniform Resource Locator – standard address format used to locate resources on the web (scheme, host, path, etc.).
VM	Virtual Machine – software emulation of physical hardware used for hosting workloads.
VNF	Virtualized Network Function – network function implemented in software running on virtualized infrastructure rather than dedicated hardware.
VoLTE	Voice over Long-Term Evolution – voice calling service delivered over LTE packet networks using IMS.
VoNR	Voice over New Radio – voice calling service delivered over 5G NR networks (typically using IMS with 5G core).
VPN	Virtual Private Network – encrypted tunnel that secures traffic over untrusted networks and can provide remote or site-to-site connectivity.
WAF	Web Application Firewall – security control that monitors and filters HTTP(S) traffic to protect web applications from common attacks.

Useful Acronyms & Glossary

Term	Definition
WAN	Wide Area Network – network spanning large geographic areas connecting multiple sites and networks.
WDM	Wavelength Division Multiplexing – optical transport technique that carries multiple signals over a single fiber using different light wavelengths.
XDR	Extended Detection and Response – security approach/platform that correlates telemetry across multiple domains (endpoint, network, cloud, email) for detection and response.

Executive Summary

Existing literature and industry research largely emphasizes theoretical threat models in the telecommunications space, often referencing frameworks like MITRE ATT&CK and GSMA Mobile Threat Intelligence Framework (MoTIF), as well as European Telecommunications Standards Institute (ETSI) and vendor-specific guidance. However, these frameworks fall short when it comes to evaluating how those threats manifest in real-world telecommunications environments and how detection can be operationalized at scale.

To build practical threat detection strategies, this whitepaper sets out to analyze and validate the theoretical landscape– reviewing cited data sources, tactics, techniques, and procedures (TTPs)– and mapping them against the specific needs, telemetry capabilities, and architectures of mobile and other telecommunications service providers.

In particular, this paper seeks to:

- Align threat detections with the organization's strategic objectives to achieve maximum value while minimizing implementation and operational overheads
- Provide a technical definition of protective and detective measures for telecommunications that considers the likely Indicator of Attack (IoA) and Indicator of Compromise (IoC) and the practical capabilities that are available to security operations center (SOC) and network operations center (NOC) teams managing these infrastructures.
- Integrate cybersecurity into broader enterprise risk management
- Emphasize the importance of outcome-driven measurement

This paper offers a prioritized set of telecommunications telemetry capabilities that are practical, cost-effective, and that offer real value in the current landscape.

Introduction

Given the functionality present in telecoms equipment, particularly those components that are most closely associated with modern mobile networks, it is pertinent to ask which aspects of their usage, or misuse, can be effectively monitored, and how. Practical monitoring should be based on existing vendor capabilities and/or naturally occurring artefacts rather than high-level concepts of threats, which may be infeasible to monitor in practice.

For example, detections built on flow logs from the signaling plane and Border Gateway Protocol (BGP) authentication errors are highly feasible. The former is easy to implement because NetFlow does not require a specific configuration on the compute equipment, while the latter is often already generated for operational purposes. By comparison, detections based on an Endpoint Detection and Response (EDR) may not be supported for deployment, and detections that ask for knowledge of low-level particulars of a protocol to be analyzed and reported on, may not be feasible without specialized application gateways being introduced, for example, Signaling System 7 (SS7) firewall. Details of documents relevant to this discussion and analysis can be found in Table 1.

The purpose of this whitepaper is to inform an audience of senior decision-makers on the suggested prioritization of telemetry sources for practical threat detection within a telecommunications environment.

While the overall audience is likely to be decision-makers, it is expected that the evaluation itself and the prioritized telemetry sources should also inform architects, operations teams, and engineers – whether telecommunications or cybersecurity focused.

The scope of this document is as follows:

- Discuss and align on the proposed source telemetry methodology for the detection of threats
- Discuss and align on proposed source telemetry for scoring and prioritization of threats

Key Findings

The analysis of detection requirements and telemetry sources revealed that practical security monitoring in telecommunications must balance feasibility, cost, and operational value. Unlike traditional information technology (IT) environments, telecommunications networks rely on highly specialized components and protocols, many of which lack native integration with enterprise monitoring frameworks. Effective detection strategies must therefore prioritize telemetry sources that are both naturally occurring and operationally relevant, while avoiding dependence on theoretical controls that cannot be realistically implemented.

The key findings are grouped across three domains: detection requirements, telemetry sources considerations, and a consolidated matrix, which maps sources against visibility domains.

Detection requirement considerations

Detection requirements within telecommunications are heavily influenced by the unique architecture of mobile and fixed-line networks.
Key considerations include:

- **Domain specificity –** Threats manifest differently across domains such as the Radio Access Network (RAN), packet core, Operation support systems/Business support systems (OSS/BSS), Domain Name System (DNS), and transport networks. A one-size-fits-all detection approach fails to provide meaningful coverage.
- **Integration with operations –** Telemetry that is already used by NOC teams (e.g., register health events, radio alarms, NetFlow) often holds dual value for security. Leveraging these streams reduces operational friction and eliminates the need for new data collection mechanisms.
- **Threat relevance –** Detection priorities should be aligned with adversary tradecraft observed in practice (e.g., signaling abuse, BGP manipulation, credential theft) rather than abstract or purely theoretical threat models).
- **Cost-benefit alignment –** Some high-value telemetry requires substantial capital expenditure (CAPEX)/operational expenditure (OPEX) investment (e.g., deep packet inspection for signaling protocols). These must be justified against the detection benefit delivered, especially in large-scale environments.
- **Scalability of analysis –** Data sources such as NetFlow and authentication, authorization and accounting (AAA) logs generate high throughput. Automated analysis techniques, including anomaly detection and clustering, are critical to ensure scalability.
- **Regulatory and compliance drivers** National and international standards increasingly mandate specific visibility domains (e.g., signaling monitoring, lawful interception auditability), which shape detection requirements.

Telemetry source considerations

Evaluating telemetry sources revealed that not all data streams are equally valuable for detection.
Key considerations include:

- **Practicality of collection –** Sources such as DNS logs and NetFlow are widely supported and operationally integrated, making them highly practical. In contrast, telemetry requiring custom agents or vendor-specific Application Programming Interfaces (APIs) may not be feasible at scale.
- **Value of enrichment –** Standalone telemetry streams may lack sufficient context. Cross-correlation (e.g., combining AAA logs with identity and access management/ privileged access management (IAM/PAM) enhances detection fidelity and reduces false positives.

- **Operational overlap –** Telemetry already generated for service assurance (e.g., Simple Network Management Protocol (SNMP), radio health events) can be repurposed for threat detection, reducing incremental cost.
- **Artificial intelligence (AI)/Machine learning (ML) suitability –** High-volume, patterned data such as signaling flow records and application logs lend themselves to anomaly detection and predictive analysis, providing a pathway to advanced analytics.
- **Security blind spots –** Some domains (e.g., transport routers, RAN devices) provide minimal native security telemetry, leaving blind spots that must be mitigated with complementary data sources or external probes.
- **Ecosystem alignment –** Industry frameworks such as MITRE FiGHT™, GSMA MoTIF, and European Union Agency for Cybersecurity (ENISA) guidelines consistently highlight AAA, IAM, signaling, and DNS telemetry as cornerstone sources for detection.

Telemetry source matrix

A detailed Telemetry Source Matrix, mapping each source to its associated visibility domain and identifying its detection relevance, can be found in Appendix C: Telemetry Source Matrix. Key insights include:

- **Cross-domain coverage –** AAA, IAM, and PAM logs provide detection value across almost all visibility domains, supporting credential theft detection, privilege escalation monitoring, and persistence tracking.
- **Network-centric telemetry –** NetFlow, intrusion detection system (IDS), and firewall logs remain the backbone of transport and interconnect visibility, providing early indicators of signaling abuse, lateral movement, and exfiltration.
- **Domain-specific value –** Register health events, radio logs, and DNS telemetry are highly specialized to telecommunications and offer unique visibility not achievable through traditional enterprise data sources.
- **Operational reuse –** Telemetry traditionally used for fault management (e.g., SNMP, system logs, configuration change events) can be leveraged for both performance monitoring and security detection.
- **Balanced prioritization –** While the matrix highlights over 25 potential telemetry sources, only a subset offer both high practicality and high detection value. These should be prioritized for implementation to achieve maximum risk reduction with minimal operational burden.

In summary, the telemetry source matrix validates that a layered and cross-domain approach is necessary. No single source delivers comprehensive coverage, but when correlated across domains, the combined telemetry set provides actionable visibility into adversary tactics and techniques.

Analysis methodology

The recommendations presented in this whitepaper are derived from a structured analysis methodology designed to ensure they are practical, effective, and aligned with the strategic objectives of a telecommunications organization. To bridge the gap between theoretical cybersecurity principles and the operational realities of managing a modern network, our approach is organized into two distinct, sequential phases.

The first phase, the identification of detection requirements, establishes the foundational context by defining what needs to be monitored. The second phase, Evaluation of Telemetry Sources, assesses how to best achieve this monitoring in a way that is both cost-effective and operationally viable.

This two-phase process ensures our conclusions prioritize actionable and outcome-driven threat detection strategies that deliver maximum value while minimizing implementation overhead. Each phase is detailed in the subsections that follow.

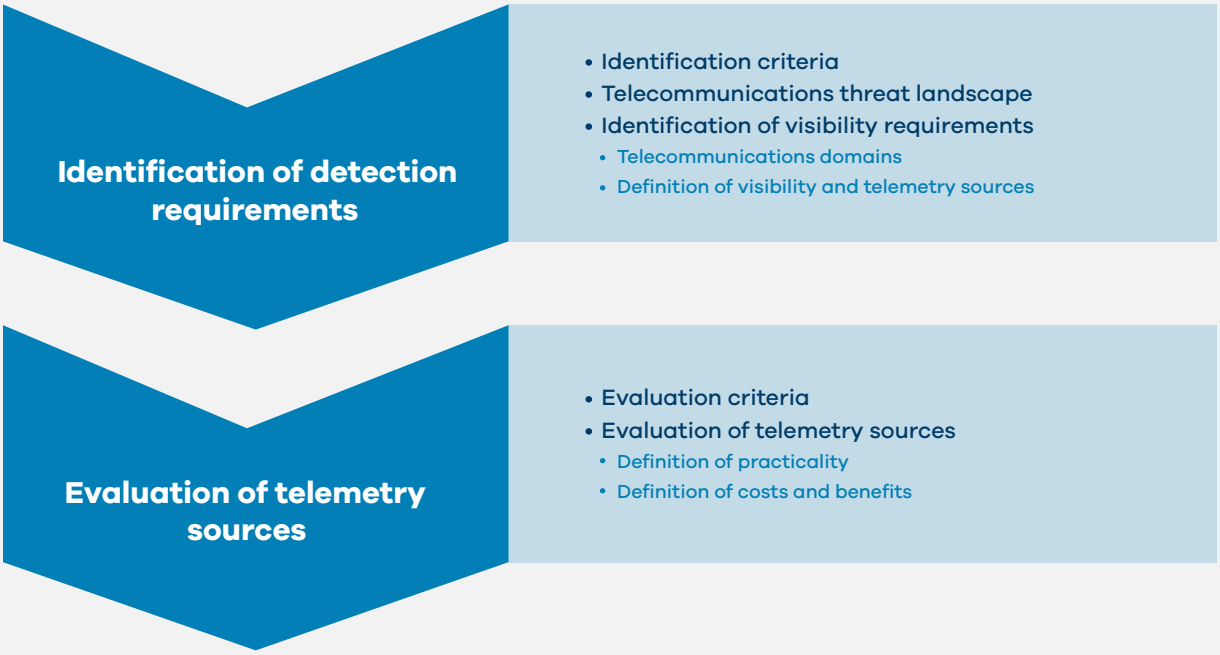

Figure 1: Analysis methodology

Identification of detection requirements

Identification criteria

The authors of this whitepaper believe that no research project can be delivered without a basic understanding of previous research on a given subject.

This may include, but is not limited to:

- Research on existing attacks on the same technology
- Research of adjacent technologies

In particular, this gives the researcher the opportunity to:

- Gain further familiarity with the target
- Identify effective methodologies for the detection of threats that they might not otherwise have considered
- Prove or disprove previous researcher-derived security claims

It also ensures a more robust research design, which will be able to withstand challenges raised during the peer review process.

In this case, the review of existing research included a number of documents, which can be found in the Bibliography, as well as recent updates to telecommunications regulations, introduced in the UK, and publicly available threat intelligence from a variety of government, commercial, and non-profit organizations.

The primary purpose of this evaluation was to assess how the detection requirements captured in these documents could best be addressed by the available telemetry.

Telecommunications threat landscape

As the previous section indicates, the telecommunications threat landscape is unique due to the industry's position as critical national infrastructure, its vast and complex attack surface, and the ongoing convergence of traditional telecom protocols with standard IT and cloud-native technologies.

Unlike typical enterprise environments, telecommunication networks must defend against both conventional cyber threats (e.g., ransomware, data breaches) and highly specialized attacks targeting the signaling, data, and management planes of mobile networks.

The transition from closed, proprietary systems to open, IP-based, and virtualized architectures, particularly with 5G, has expanded this attack surface significantly. This evolution introduces new vulnerabilities while retaining legacy risks.

To ensure our analysis is practical and relevant for operational teams, this section provides a structured overview of the key threat actors and attack vectors. While public reporting of in-the-wild threats is limited, publicly documented threats that have been considered in the publication of this paper include:

- Reporting around LIMINAL PANDA threat actor, targeting aspects of mobile network infrastructure for collection and leveraging signaling protocols for command and control and exfiltration
- Reporting around Salt Typhoon threat actor, targeting fixed network infrastructure including firewalls, routing, and switching fabric for persistence, command and control and exfiltration
- Reporting around GTPdoor malware family, which hides C2 traffic within the GPRS Tunneling Protocol (GTP)
- Reporting around misuse of user equipment for voice and text-based phishing and related activities
- Examples of outages caused by compromise and infection of virtualized OSS and BSS infrastructure
- Examples of IP theft and route hijacking resulting from poor IP management
- Examples of outages and other routing related incidents resulting from weaknesses in routing configurations
- Known malware affecting common Android and iOS devices
- Historic vulnerability disclosures relating to various classes of telecommunications equipment, ranging from femtocell type devices to high-end network equipment, including routing and switching fabric such as Multiprotocol Label Switching (MPLS) enabled routers

Beyond specific examples such as these, we have also considered other practical and theoretical lines of attacks, as posited in frameworks such as ATT&CK, MoTIF, and FiGHT, within the context of each major telecommunication domain, which have shaped our definition of detection requirements:

Core Network Threats (EPC & 5G Core):

- Signaling Plane Attacks: Exploitation of protocols like Diameter (4G) and Hypertext Transfer Protocol Secure (HTTP) (5G) to perform:
  - Location Tracking: Illegally obtaining a subscriber's real-time location

Denial of Service: Overloading core functions , namely Mobility Management Entity (MME), Access and Mobility Management Function (AMF), Session Management Function (SMF), with signaling messages, causing service outages for subscribers

- Subscriber Data Modification: Illegally altering subscriber profiles in the Home Subscriber Server (HSS)/ Unified Data Management (UDM)
- Data Plane Attacks:
  - Distributed Denial-of-service (DDoS): Saturating User Plane Functions Serving Gateway (S-GW), Packet Gateway (P-GW), User Plane Function (UPF), to degrade or block user data traffic
  - Data Interception: Capturing user traffic if encryption is weak or improperly implemented

Cloud-Native Vulnerabilities (5G Focus):

- API Abuse: Exploiting insecure APIs between Network Functions (NFs) in the Service-Based Architecture
- Container & Orchestration Risks: Compromise of container images, misconfigurations in Kubernetes, or gaining control of the management and orchestration (MANO) platform

RAN Threats:

- Denial of Service: radio frequency jamming or launching signaling storms to overwhelm base stations (eNBs/gNBs), creating coverage blackouts
- IMSI Catchers ("Stingrays"): Man-in-the-middle attacks that impersonate legitimate cell towers to intercept calls, messages, and data, or to track device locations
- Base Station Compromise: Gaining remote or physical access to a base station to use it as a launch point for attacks against the core network or to manipulate user traffic.

Interconnect & Roaming Interfaces GPRS Roaming Exchange (GRX)/IP Packet Exchange (IPX):

- Signaling Fraud: Rogue roaming partners sending malicious signaling messages
- SMS Fraud (e.g., Smishing): Using interconnects to send fraudulent SMS messages at scale

DNS Threats:

- As a central dependency, DNS is a prime target for DDoS, cache poisoning, and DNS tunneling to exfiltrate data

Billing and Customer Support Systems:

- Traditional IT targets holding valuable subscriber data, making them prime targets for data theft and ransomware

Identification of visibility requirements

Telecommunications domains

For the purposes of this whitepaper, we specifically looked at sources of publicly available Threat Intelligence (TLP: Clear and TLP: Green) where misuse of telecommunications equipment is a defining factor in the reporting.

The Evolved Packet Core (EPC) in LTE networks shown in Figure 2, below, represents a critical telecommunications infrastructure that demands comprehensive security monitoring. Understanding the threats, risks, and appropriate monitoring approaches helps telecommunications providers implement effective security controls and detection mechanisms.

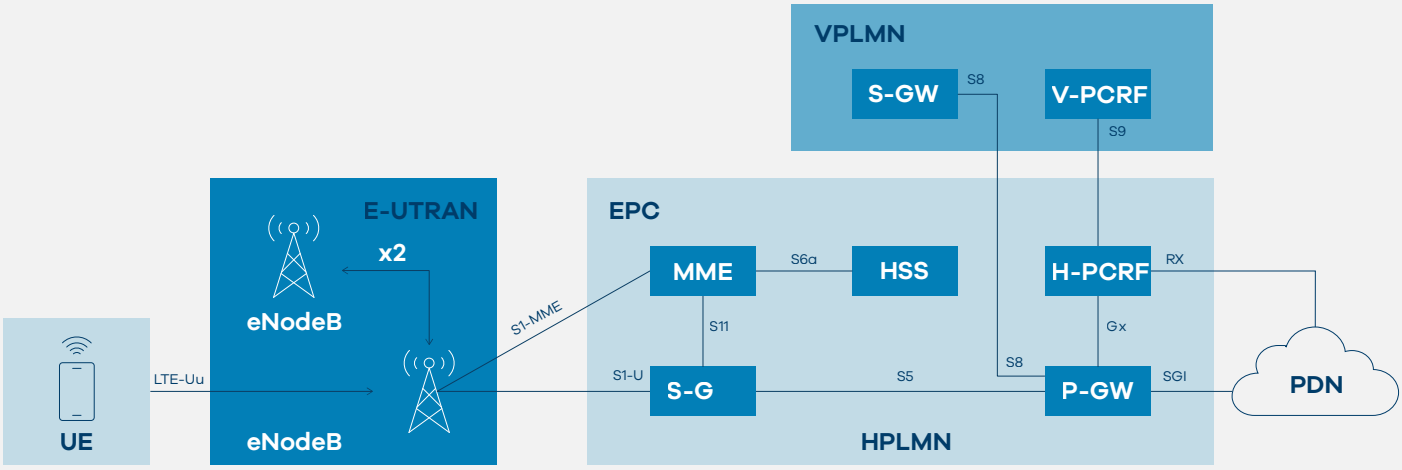

Figure 2: Evolved Packet Core (EPC) in LTE networks

We have focused on aspects of the landscape that are most relevant to mobile networks, considering both the end-user perspective and the operational needs of teams responsible for managing and maintaining network equipment. For Security Operations Centres (SOC), a critical consideration is understanding which source components exist and which visibility domains provide the greatest opportunities for collecting telemetry, such as logs, and conducting effective monitoring.

Examples of telecommunications domains relevant to threat detection and monitoring will be addressed in detail in the following sub-section.

Platform

As with all technology today, there are centrally managed aspects of the telecommunications environment. Examples could include cloud computing tenancies, VMware vSphere, or other overarching interfaces that allow orchestration beyond a single function.

Compute

In the context of this whitepaper, we refer to the generic systems that can run Windows, Linux, etc. that can load function-specific platforms or applications.

While there are many aspects of a modern telecommunications network that still require dedicated hardware and software, just as with other sectors, vendors are keen to embrace and adopt concepts such as virtualization and containers to help manage workloads more efficiently.

OSS/BSS, RAN, Packet Core, Subscriber Databases, Transport

Beyond the generic functions offered by platforms and compute, there are inevitably application stacks with APIs and databases that perform specific telecommunications functions. Whilst these will vary by role and are dependent on the feature sets developed by their vendors, they typically include a web-based interface for administrative access as well as a programmatic interface to expose their intended telecommunications function.

Functions that are typically exposed in this fashion include:

OSS

- Service Provisioning and Activation: This automates the process of setting up new services for a customer, such as activating a new internet plan or a mobile line. It configures the necessary network elements to deliver the service
- Fault Management: This system continuously monitors the network for issues, detects problems like network outages or device failures, and sends alerts to technical teams to ensure quick resolution
- Performance Management: This component tracks network performance metrics such as latency, jitter, and packet loss to ensure that the quality of service (QoS) meets a customer's service level agreement (SLA)
- Centralized Authentication, AAA, IAM, and PAM functions into which the telecommunications network is integrated

BSS

- Customer Relationship Management (CRM): This manages all customer information and interactions, including service history, support tickets, and contact details. It provides a unified view of the customer for all business departments
- Order Management: This system handles the entire lifecycle of a customer order, from the initial request to its completion. It validates the order, tracks its progress, and communicates with the OSS to trigger service activation
- Product Management/Catalogue: This component manages the product and service offerings a telecom provider sells. It handles the creation, pricing, and bundling of various plans and services
- Billing and Revenue Management: This is a crucial component that automates the billing process. It collects usage data, calculates charges, generates accurate and timely bills, processes payments, and manages collections
- Vendor-Specific Interfaces: Supporting Radio Access Network, Packet Core, and Transport
- Network Management System (NMS): NMS has an end-to-end view of the entire network. It aggregates data from multiple Element Management Systems (EMS) and can manage network elements from various vendors. The NMS is responsible for functions like service routing across different devices, correlating alarms from multiple devices to identify a single root cause, and ensuring connectivity across the entire network
- EMS: EMS focuses on managing individual network devices (elements) from a specific vendor, like Cisco routers. It provides detailed, device-specific functions for configuration, fault monitoring, and performance data collection for a single device or a group of similar devices. Think of it as the "manager" for a particular type of network equipment
- Register Functions: Utilized by mobile networks for managing subscribers, registering user equipment to the network, and facilitating voice and data sessions

DNS

In modern telecommunications networks, the DNS is a foundational technology that enables devices and network functions to dynamically locate and connect to services. While commonly associated with web browsing, DNS is deeply integrated into the core operations and service delivery of telecommunications infrastructure. Its usage extends far beyond traditional software stacks, often requiring advanced IP Address Management (IPAM) solutions to address the scale and complexity of telecom environments.

Key DNS functions in telecommunications:

- Internet Access (Standard Use): When a user enters a Uniform Resource Locator (URL) (e.g., www.example.com) on a mobile device, a DNS query is generated to translate the domain name into an IP address. This request is typically processed by a DNS resolver operated by the mobile network provider
- Network Function Discovery in EPC/5GC: DNS facilitates dynamic discovery and routing to core network functions
- In 4G EPC: The PG-W may use DNS to locate external services. DNS assists in routing signaling between network components (e.g., MME, S-GW, P-GW)
- In 5G (Service-Based Architecture): DNS is essential for NF discovery. Functions such as AMF, SMF, and UPF resolve the hostnames of target NFs via DNS – an especially vital process in cloud-native, dynamic environments where IP addresses may frequently change
- Access to Operator Services, namely IMS, Voice over Long-Term Evolution (VoLTE), 5G Standalone (5G SA): DNS resolves service domains (e.g., ims.mncXXX.mccXXX.3gppnetwork.org) to enable access to the IMS core for services like VoLTE or Voice over New Radio (VoNR). This process employs various DNS records (NAPTR, SRV, A/AAAA) to determine the correct server, protocol, and IP address
- Roaming: When users roam into new networks, DNS is used to:
  - Locate home network functions (e.g., HSS, UDM)
  - Locate visited PLMN services

  Standardized 3GPP domains, such as epc.mncXXX.mccXXX.3gppnetwork.org, support the discovery of these services.
- Security Functions: DNS filtering is used to block access to malicious or unauthorized domains. Techniques such as DNS over HTTPS (DoH) and DNS over TLS (DoT) enhance user privacy. Private DNS configurations allow operators or users to enforce specific DNS resolver policies
- Policy Control and Traffic Steering: DNS enables content filtering and routing traffic to local breakout (LBO) locations. It also supports the implementation of traffic steering policies, such as directing traffic for enterprise applications

Given DNS's centrality to network function and service delivery, it is a critical component for both protective and detective cybersecurity measures in telecommunications. Effective DNS monitoring and threat detection can align with organizations' strategic objectives, minimize operational overhead, and provide measurable outcomes that contribute to broader enterprise risk management.

Transport

For the telecommunications network to operate, there must be some wide area network (WAN) that connects each of the individual radio sites to the packet core, related services, and the Internet at large. This is typically known as the transport network. The transport network in telecommunications refers to the underlying routing and switching devices that carry data, voice, and signaling traffic between various parts of a telecom network. The network usually consists of routing and switching devices responsible for establishing point to point links over which the TCPI/IP stack can operate, and the functions that they expose are typically limited on that basis.

Devices within the transport network usually perform the following functions:

- Access Transport:
  - Connects base stations (gNBs/eNBs) to aggregation points
  - Often uses microwave, fibre, or copper links
- Aggregation Layer:
  - Collects and aggregates traffic from multiple access links
  - Uses switches and routers to direct traffic efficiently
- Core Transport:
  - Provides high-capacity backbone linking aggregation networks to core network elements and data centres
  - Uses technologies like IP/MPLS, WDM (Wavelength Division Multiplexing) and Synchronous Digital Hierarchy/Synchronous Optical Network (SDH/SONET)

User equipment, voice, data

In a modern mobile network, the component that performs the RAN function is typically known as the gNB (for 5G) or eNB (for 4G LTE). Due to the need for a physical interconnect to the radio cell towers themselves, RAN devices are usually a Blackbox or set of related Blackboxes that perform a discrete function (enabling User Equipment to connect to the network to make and receive voice calls and to send and receive data). As a result, such devices usually have a limited capability to be managed and to generate telemetry.

Devices within the RAN usually perform the following functions:

- Radio Resource Management:
  - Allocates radio channels and power
  - Handles handovers, interference control
- User Plane Functions:
  - Data transmission between user devices and the core network
- Control Plane Functions:
  - Signaling for session setup, mobility and authentication
- Connectivity with Core Network:
  - Communicates with the 5G Core (5GC) or EPC (in LTE)
- Interface Management:
  - Manages connections to mobile devices via the Uu interface
  - Connects to the core network via NG-C/NG-U (5G) or S1-C/S1-U (4G)

Certificate Authority (CA), Hardware Security Module (HSM), Public Key Infrastructure (PKI)

In a mobile network, PKI ensures that users, user equipment, and network components (like the RAN) can securely communicate and trust each other.

In a typical telecommunications network, a CA backed by HSMs can be responsible for:

- SIM and eSIM authentication
- Mobile devices authenticating to the network using credentials, sometimes tied to PKI certificates
- Network node authentication
  - Base stations (e.g., gNB in 5G) authenticating themselves using certificates to prevent rogue or fake nodes
- Secure Over-the-Air (OTA) updates
  - Software and configuration updates to mobile devices or infrastructure are signed and verified using PKI
- Subscriber identity protection
  - With 5G, subscriber identity (like Subscription Permanent Identifier (SUPI) is protected using encryption mechanisms. These mechanisms can be supported by PKI, which enables transport layer security (TLS).

Visibility

Definition of visibility

Visibility is the lifeblood of a SOC. Without a steady flow of data from across the environment, the SOC is blind to what is happening - unable to detect threats, respond to incidents, or validate security posture.

While the focus of this whitepaper is the timely detection of cybersecurity threats, to ensure the practicality of the detections we will also consider the case of a NOC. While visibility here focuses more on performance, availability, and reliability of systems and networks, rather than security, one of the aims of this paper is to show how the same operational telemetry that provides this visibility can also be of practical support to SOCs.

Examples of Visibility

Alerting - Triggered by events or thresholds, often alert-driven, typically available via telecommunications OSS/BSS infrastructure, where it is used for tasks such as QoS

Logging - Data collected without initiating any action, detailing what is happening on a device, typically available via security capabilities such as AAA and network segmentation controls such as firewalls, application firewalls etc., which protect critical telecommunication network assets

Monitoring - Telemetry that is actively generated by initiating actions or probes to uncover threats, validate controls, or detect weaknesses, before malicious activity is known to exist

Evaluation of telemetry sources

Evaluation criteria

The primary purpose of this evaluation was to evaluate which telemetry sources could best address the detection requirements, but we believe that it is also necessary to consider the cost and benefit of the investment.

Definition of practicality

Given the functionality present in telecoms equipment, particularly those components that are most strongly associated with modern mobile networks, what aspects of their usage, and misuse, can be effectively monitored, and how? Practical monitoring should be based on existing vendor capabilities and/or naturally occurring artefacts rather than high-level concepts of threat, which may be infeasible to monitor in practice.

Examples of practical and impractical

In this regard, we will evaluate potential detective controls from the perspective of:

- Is the data already being collected? For example, with detections based on flow logs from the signaling plane, BGP authentication errors are feasible to build on since they either do not rely on the equipment itself or are already generated for operational reasons
- Does the detection rely on new capabilities? For example, detections based on an EDR (which may not be supported for deployment), or which ask low-level particulars of a protocol to be analyzed and reported on (at least not without specialized application gateways being introduced (e.g., SS7 firewall)
- Can the data support advanced AI use cases such as clustering, predictive, and anomaly analysis detection? For example, could an AI model detect adverse trends in something like call flow logs? The use of AI could help a detective capability scale, which may be critical for high-throughput log sources where an analyst will never be able to review every event

Evaluation of telemetry value

The primary purpose of this evaluation was to evaluate which telemetry sources could best address the detection requirements, but we believe that it is also necessary to consider the cost and benefit of the investment.

Definition of costs and benefits

Whilst implementing technical control may be easy from a purely engineering standpoint, it is likely that any investment in doing so will need to consider the cost and benefit of the approach. This latter dimension is critical from a leadership standpoint, as it considers any potential investment.

Examples of costs and benefits

In this regard, we will evaluate potential detective controls from the perspective of:

- Existence of capability today: Is this something that telecommunications components are already generating? This somewhat overlaps with practicality
- Cost of deployment: Is this something where the capability can easily be deployed?
- Cost of operation: What is the knock-on effect of using it? Does it use masses of storage, does it require cloud, etc.?
- Benefit of results: What kinds of threats will it address, and how critical are they?

1. Detection Requirements Identification

The following is a table investigating existing guidance from a number of established standards and regulatory sources. Note that section 2 covers a subset of these sources, prioritized based on these evaluation criteria.

Article	Year	Published	Scope	Description	Limitations
Integrating Telecommunications Infrastructure with a SOC	2025	Cisco	SIEM integration	This whitepaper provides a systematic approach to SIEM integration, which is essential, encompassing everything from business requirement gathering to initial planning, use case definition, Key Performance Indicator (KPI) creation, architecture design, and ongoing optimization and maintenance of the security monitoring infrastructure.	While the paper offers priorities based on practical risks that may be present in a telecommunications environment, it does not fully unpack the challenges around practicality, cost, and value There are also no considerations given for existing non-log-based sources of telemetry that may exist within a telecommunications environment
A Vision for Telecommunications Security	2024	ETSI	Service providers	This whitepaper presents a vision for the future of network security standardization and design, emphasizing the need for an Intelligent Trusted Network (ITN) to support the diverse and expanding array of communication technologies, including 4G, 5G, 6G, and satellite systems. The proposed 6G network aims to provide universal access to digital services and voice, leveraging AI to support a wide range of devices and services. It will serve as a "Network of Networks," integrating existing and new infrastructures to maximize wireless connectivity.	Controls are intentionally non-prescriptive to allow flexibility of implementation GRC centric
Enhanced Visibility and Hardening Guidance for Communications Infrastructure	2024	CISA	Transport networks	The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate (ASD), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS) and New Zealand's National Cyber Security Centre (NCSC-NZ) warn that state-sponsored threat actors compromised networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaigns.	Focused on underlying routing and switching fabric Limited guidance on voice, data, and video signaling
FS.57 Mobile Threat Intelligence Framework (MoTIF) Principles	2024	GSMA	RAN and MPC	The Mobile Threat Intelligence Framework (MoTIF) developed within the GSMA's Fraud and Security Group (FASG) is a first version of a framework for describing, in a structured way, how adversaries attack and use mobile networks, based on the TTPs that they use. MoTIF is focused on mobile network related attacks that are not already covered by existing public frameworks like MITRE ATT&CK® and MITRE FiGHT™. MoTIF is intended for GSMA member and non-member use. FS.57 "MoTIF Principles" provides an overview of MoTIF and defines the techniques and sub-techniques used in the framework. It also describes how MoTIF can be represented in STIX, a structured language for describing cyber threat information.	Measures do not map to affected components and expected capabilities There are also no considerations given to underlying routing and switching fabric threats that may exist within a telecommunications environment

Article	Year	Published	Scope	Description	Limitations
FiGHT™ (5G Hierarchy of Threats)	2024	MITRE	5G	FiGHT™ (5G Hierarchy of Threats) is a knowledge base of adversary Tactics and Techniques for 5G systems. FiGHT consists of three types of Techniques: theoretical, proof of concept (PoC), and observed. The theoretical and PoC constitute the bulk of the framework and are based upon academic research and other publicly available documents. Currently, a minority of FiGHT Techniques are based upon real-world observations, documented accordingly. Each FiGHT Technique is labelled as theoretical, PoC, or observed.	No requirement to cite known incidents as evidence –Data sources listed are a mixture of enterprise security functions and operational behavior metrics
Telecommunications Security Code of Practice	2022	UK DCMS	UK service providers with fixed and/or mobile infrastructure	The UK government's Telecoms Supply Chain Review Report ('the Review'), published in July 2019, highlighted the security risks as well as the economic opportunities associated with the next generation of telecommunications networks, particularly 5G and full fibre networks. The Review concluded that a new, robust security framework was needed for the UK telecoms sector, marking a significant shift from the previous model.	Threat model undefined Controls are intentionally non-prescriptive to allow flexibility of implementation, but therefore allow for wide variance in approach with limited standardization
SS7 Interconnect Security Monitoring and Firewall Guidelines	2019	GSMA	SS7	This document describes how to monitor SS7 traffic, including prevention and detection techniques against suspected attacks. It allows an operator to assess if received SS7 MAP or CAMEL messages are legitimate and apply appropriate firewall rules to protect its network.	Covers only SS7 Lack of equivalent guidance for GTP and Diameter
Signaling Security in Telecom SS7/ Diameter/5G	2018	ENISA	RAN and MPC	This study provides a deep dive into a critical area within electronic communications, the security of interconnections in electronic communications (signaling security). Based on the analysis, there is a medium to high level of risk in this area and we do consider that proper attention must be granted by all stakeholders involved so as to find a proper solution.	Measures do not map to affected components and expected capabilities Measures are too broad to be measurable

Table 1: Analysis of Existing Detection Requirements

1.1 Platform

Threat case

Platforms underpin the orchestration and management of telecommunications environments, ranging from virtualization layers (e.g., VMware, Kubernetes, OpenStack) to public cloud tenancies that host virtualized network functions (VNFs) and containerized network functions (CNFs). These platforms are prime targets for attackers due to their elevated privileges and their role as the control plane for multiple downstream functions.

Key threats may include:

- Supply chain risks in cloud or virtualization platforms, where vulnerabilities in the platform software can cascade to hosted network functions
- Credential compromise of administrative accounts leading to unauthorized configuration changes or malicious deployments
- Exploitation of hypervisors or orchestration APIs, enabling attackers to bypass tenant isolation and access sensitive workloads
- Persistence mechanisms implemented via rogue containers, snapshots, or virtual machines templates that evade standard monitoring
- Deployment of hypervisor-aware malware for the purposes of ransomware attacks

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
• Centralized logging of AAA, IAM, and PAM activities for privileged access monitoring • Continuous monitoring of management connection events (e.g., SSH, API calls, web console sessions) • Configuration baseline enforcement to detect unauthorized changes to orchestration templates, hypervisors, or cloud resources • Version and patch management telemetry to track platform updates and identify unpatched vulnerabilities • Integration of security alert events from cloud-native controls (e.g., AWS GuardDuty, Azure Security Centre) into the SOC pipeline • Operational playbooks for isolating compromised tenants or workloads without disrupting service availability	• Investment in platform-native logging and monitoring tools (e.g., vRealize, OpenStack telemetry, or cloud-native monitoring services) • Deployment of flow collectors and SIEM/SOAR platforms capable of ingesting large-scale platform telemetry • Potential licensing costs for advanced orchestration security modules (e.g., Kubernetes security add-ons, cloud workload protection platforms)	• Ongoing administration of telemetry pipelines, including log parsing, storage management, and alert tuning • Training SOC/NOC analysts on platform-specific threat models to distinguish between benign operational events and malicious activity • Regular audit and compliance reporting overheads tied to regulatory requirements for platform security	• Provides centralized visibility into the control plane of the telecom infrastructure • Enables early detection of privilege escalation, persistence, and configuration drift • Facilitates rapid containment of incidents through orchestration-native controls (e.g., VM snapshot rollback, container quarantine) • Enhances compliance with industry regulations by demonstrating platform-level security monitoring	• High data volume from platform logs can overwhelm SIEM solutions if not filtered or prioritized • Reliance on vendor-specific APIs and logging formats creates integration complexity • Advanced attacks targeting hypervisors or supply chain vulnerabilities may remain undetected without specialized detection capabilities • Costly to maintain real-time monitoring across hybrid/multi-cloud platforms due to diverse toolsets and operational overhead

1.2 Compute

Threat case

Compute infrastructure in telecommunications refers to general-purpose servers running operating systems such as Linux or Windows that host network functions, OSS/BSS applications, or supporting workloads. These systems, while hardened by vendors, remain exposed to the same classes of threats as enterprise IT environments, with additional risk due to their integration into critical telecom services.

Key threats may include:

- Exploitation of operating system (OS) vulnerabilities (kernel, libraries, or middleware) leading to remote code execution or privilege escalation
- Credential abuse via SSH, RDP, or API access, often enabled by weak or reused passwords
- Insider threats, where operators with legitimate access modify configurations or extract sensitive subscriber data
- Malware deployment and persistence through rogue processes or unauthorized binaries
- Compromise of virtualization/container runtimes (Docker, Kubernetes nodes) to pivot into other workloads
- Collection of sensitive subscriber data at points of aggregation such as the API gateways, databases, and logs that are used for wider operational and business integration

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
• OS-level telemetry (system logs, kernel logs, audit events, process creation data) • Deployment of EDR agents (where supported) for endpoint-level visibility and detection of persistence mechanisms • Firewall and IDS logs correlated with server telemetry to detect anomalous inbound or outbound connections • Configuration monitoring (baseline enforcement, file integrity monitoring) to identify unauthorized changes • Vulnerability data ingestion for prioritizing patching cycles across heterogeneous compute environments • Integration with management connection events (SSH, RDP) for detection of brute-force, credential stuffing, or anomalous login behavior	• Licensing and deployment of EDR/XDR solutions across supported compute nodes • Investment in centralized log aggregation tools (SIEM/SOAR pipelines) to collect diverse OS and application logs • Optional acquisition of privileged access management (PAM) solutions to enforce least-privilege access to compute resources	• Continuous patch and vulnerability management operations across hundreds or thousands of servers • SOC overhead in alert triage, as compute telemetry often generates high false positive rates without tuning • Ongoing rule and signature management for EDR, IDS, and firewall solutions • Administrative effort for maintaining access control lists and PAM configurations	• Provides granular visibility into server-level threats, including insider activity and malware execution • Enables early detection of anomalies that may not be visible at higher abstraction layers (e.g., packet core or platform) • Supports regulatory compliance by generating auditable logs of user activity and security events • Facilitates advanced analytics, such as AI-based clustering of process data to highlight abnormal behavior	• High operational overhead due to volume and diversity of logs from heterogeneous compute environments • EDR coverage may be inconsistent, as many telecom-specific appliances do not support endpoint agents • Integration complexity when correlating OS-level telemetry with telecom-specific applications • Detection effectiveness may depend on rapid patching, which is often constrained in production telecom networks due to uptime requirements

1.3 OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Transport

Threat case

This visibility domain represents the heart of the telecommunications ecosystem, where customer-facing services and core network operations converge. Threat actors frequently target these components to disrupt service availability, exfiltrate subscriber data, or gain control over signaling and authentication functions.

Key threats may include:

- Signaling abuse (e.g., SS7, Diameter, GTP) to track subscribers, intercept traffic, or perform fraud
- Application-level attacks (e.g., Structured Query Language (SQL) injection, API exploitation) against OSS/BSS portals or customer databases
- Denial-of-service attacks on subscriber databases or core elements, disrupting registration and call setup
- Fraudulent provisioning of services or SIM profiles through compromised OSS/BSS workflows
- Credential compromise of operators or administrators with access to packet core or subscriber management interfaces
- Misuse of signaling protocols for exfiltration and command and control
- Insider threats, where malicious or negligent staff exploit privileged access to manipulate subscriber data or billing records

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
This visibility domain can be broken down into various standard technologies following a traditional 3-tier architecture. However, access to each tier is likely to be limited to whatever the vendor deems appropriate. While actual implementation will vary, for the purposes of this paper, we have considered the following types of technology as being capable of generating some or all of the required telemetry: • WAF/LB/API gateway • Web server • Application • API • Database This domain will likely benefit from and/or contribute to the platform visibility domain. However, it may also offer additional benefits where effectively integrated. For example, it may be possible to see the actual requests that make up a given call flow, or to extract additional data from a subscriber database depending on the level of customization offered.	• Procurement of signaling firewalls (SS7, Diameter, GTP) to provide visibility into interconnect traffic • Investment in database monitoring tools to log queries, detect anomalies, and prevent exfiltration • Deployment of application security controls such as WAFs, API gateways, and fraud detection platforms • Expansion of data storage and SIEM capacity to handle high-volume signaling and database logs	• Continuous tuning of fraud detection and signaling firewall rules, requiring highly skilled analysts • Database log management, including parsing, normalization, and retention for regulatory audits • Ongoing updates to application-layer defences (e.g., WAF signatures, API schema validation) • Higher incident response overhead, as alerts in these domains often require deep domain expertise to triage effectively	• Provides deep visibility into subscriber activity, provisioning, and billing, which is critical for detecting fraud and insider abuse • Enables monitoring of end-to-end service flows, from user registration to billing, improving both security and service assurance • Facilitates detection of signaling-based attacks, which are unique to telecommunications and invisible in standard IT telemetry • Supports regulatory compliance for lawful interception auditability, fraud detection, and subscriber data protection	• Vendor lock-in often restricts the granularity of logs and may require proprietary tools for integration • High cost of ownership, as signaling firewalls and specialized database monitors require significant investment • Complexity of correlation, since OSS/BSS, packet core, and subscriber databases generate diverse telemetry streams that must be normalized for detection • False positives in fraud detection or anomaly-based signaling monitoring can create alert fatigue if not properly tuned

1.4 DNS

Threat case

DNS is a foundational component in telecommunications networks, supporting not only standard internet resolution but also critical functions such as service discovery, roaming, and access to operator services (IMS, VoLTE, 5G SA). Compromise or misuse of DNS can lead to severe security and operational risks.

Key threats may include:

- DNS hijacking or poisoning, redirecting users or network functions to malicious infrastructure
- Tunneling attacks, where adversaries exfiltrate data or establish command-and-control channels through DNS queries
- Exploitation of recursive resolvers to amplify denial-of-service attacks
- Targeted manipulation of telecom-specific domains (e.g., epc.mncXXX.mccXXX.3gppnetwork.org) to disrupt roaming, authentication, or core service discovery
- Abuse of misconfigured resolvers to gain unauthorized visibility into subscriber activity
- DNS over HTTPS/TLS misuse, where encrypted DNS traffic bypasses enterprise-level monitoring and filtering

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
• Centralized logging of DNS queries and responses, with specific focus on 3GPP-defined telecom domains • Deployment of DNS anomaly detection tools to identify tunneling or exfiltration patterns • Integration of DNS firewalling and filtering to block known malicious domains via threat intelligence feeds • Monitoring of resolver integrity, ensuring configuration consistency and detection of unauthorized changes • Correlation of DNS logs with NetFlow and AAA events to link suspicious queries with subscriber sessions or signaling flows • Capacity planning and monitoring to prevent DNS-based DDoS from degrading telecom services	• Investment in DNS logging and security appliances, capable of operating at telecom scale • Procurement of threat intelligence feeds for DNS-based blocking and enrichment • Deployment of redundant DNS infrastructure (resolvers, IPAM solutions) to ensure high availability and resilience	• Continuous signature and threat feed updates for DNS filtering engines • Analyst training to differentiate between benign anomalies (e.g., new roaming partners) and malicious DNS behavior • Regular audit and integrity checks on DNS configurations, zones, and IPAM systems • Ongoing correlation and tuning of DNS telemetry with other sources to reduce false positives	• Provides early detection of C2, tunneling, and phishing activity, often before payload execution • Enhances telecom-specific visibility, particularly for roaming and service discovery attacks • Supports blocking of malicious traffic at scale with minimal performance impact • Offers cross-domain correlation value, linking subscriber behavior, signaling flows, and malicious resolution events	• High log volume, particularly in large-scale subscriber environments, creates storage and analysis challenges • Attackers may evade detection via encrypted DNS traffic (DoH/DoT), reducing visibility unless countermeasures are deployed • DNS telemetry alone lacks context and must be enriched with subscriber, signaling, or NetFlow data for actionable detection • Reliance on third-party feeds introduces cost and dependency risks if not supplemented by in-house analysis

1.5 Transport

Threat case

The transport network forms the backbone of telecommunications, carrying signaling, user data, and control traffic between radio sites, packet core, and external interconnects. As such, it is a high-value target for adversaries seeking to disrupt availability, intercept communications, or manipulate routing.

Key threats may include:

- Firmware manipulation or supply chain attacks, inserting malicious code into routing devices
- Insertion of rogue devices or taps into fibre/microwave links for passive interception
- BGP hijacking or route leaks, redirecting traffic to malicious or unauthorized paths
- Exploitation of MPLS or SDH/SONET vulnerabilities to disrupt services
- DDoS attacks on routers or switching fabric
- Exploitation of weak management plane security, such as SNMP abuse or unauthorized SSH access
- Misuse of VPN and routing protocols for exfiltration and command and control
- Widespread corruption and wiping of devices to disrupt services

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
Routing and switching devices will typically have a locked down interface to enable specific administration functions, such as configuring basic networking, configuring MPLS and BGP, and establishing a topology within the wider mobile network, but it is not typical for this interface to allow for extended customization. Beyond any device or firmware specific telemetry that may be generated, any telemetry that the routing and switching devices generate is likely to relate to the health of the routing, capacity warnings, and errors triggered by communications with other nodes. Routing and switching devices may be centrally managed with a platform but can typically be configured individually via a based SSH or web-based interface.	• Acquisition of flow monitoring infrastructure (NetFlow/IPFIX collectors) to provide visibility into traffic patterns • Procurement of routing security solutions, such as BGP monitoring tools or RPKI validation services • Investment in redundant routing and switching hardware to provide resilience against outages and attacks • Specialized firmware integrity monitoring solutions to detect tampering or unauthorized updates	• Ongoing management of routing policies and validation of BGP configurations to prevent accidental leaks • Regular firmware patching and upgrades, requiring maintenance windows across a distributed network • Analyst training to interpret transport-level anomalies (e.g., sudden route flaps, link saturation) • Operational overhead of correlating transport telemetry with higher-layer data (e.g., signaling, subscriber activity)	• Provides critical visibility into backbone stability, ensuring early detection of routing or switching anomalies • Enables detection of man-in-the-middle or hijacking attempts at the network layer • Enhances resilience of service delivery, as monitoring supports rapid failover and rerouting during incidents • Supports compliance with government-mandated telecom security frameworks, which increasingly mandate transport-level monitoring	• High telemetry volume from backbone routers and switches may overwhelm monitoring infrastructure • Transport logs often lack application or subscriber context, requiring enrichment with other domains for actionable detection • Vendor heterogeneity complicates standardization of log formats and monitoring approaches • Advanced attacks (e.g., optical layer taps) may remain invisible without additional specialized monitoring

1.6 User equipment, voice, data

Threat case

User Equipment (UE) such as mobile phones, IoT devices, and customer-premises equipment (CPE) represent one of the most diverse and least controlled parts of the telecommunications ecosystem. They interface directly with the RAN and are often the entry point for adversaries to launch attacks on both users and the wider network.

Key threats may include:

- Deployment of cell phone farms, utilizing cycling of valid physical and eSIMs for the purposes of phishing and similar campaigns against legitimate subscribers
- Malware on UE leveraging data, voice, or signaling channels for command-and-control or fraud
- IMSI/IMEI manipulation to evade billing, tracking, or blacklisting controls
- Exploitation of weak protocols (e.g., 2G fallback, SS7-based authentication) for interception or impersonation
- Signaling storms generated by misconfigured or malicious UEs, overwhelming cell towers and packet core
- VoIP and voice fraud, including robocalls, call injection, or toll bypass attacks
- IoT device exploitation, where poorly secured devices are used for botnets or lateral movement within enterprise networks
- Widespread corruption and wiping of devices to disrupt services

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
Beyond any device or firmware-specific telemetry that may be generated (e.g. kernel logs if it's based on a Linux distribution or uses a Linux kernel), any telemetry that the RAN devices generate is likely to relate to the health of the cell tower, capacity warnings, and errors triggered by communications with individual User Equipment. RAN devices may be centrally managed with a platform but can typically be configured individually via a based SSH or web-based interface.	• Investment in probe-based monitoring solutions for subscriber signaling, including IMSI/IMEI tracking • Procurement of voice fraud detection platforms, capable of analysing call patterns in real time • Deployment of RAN analytics tools to capture and analyze UE-related anomalies • Expansion of data storage and compute infrastructure to handle the high volume of CDRs (Call Detail Records) and data session logs	• Continuous fraud monitoring and case management, requiring skilled analysts to distinguish between malicious and benign subscriber behavior • Maintenance of probes and analytics platforms, including frequent updates to fraud and anomaly detection signatures • High incident response overhead due to false positives in signaling or fraud detection alerts • Ongoing coordination between security, fraud management, and operations teams to address cross-domain UE issues	• Provides subscriber-level visibility, critical for detecting fraud, impersonation, and device-based anomalies • Supports early identification of large-scale UE issues, such as malware outbreaks or botnet activity • Enables real-time fraud detection in voice and data channels, reducing financial and reputational damage • Enhances roaming security, by monitoring unusual UE behavior across different geographies	• Massive data volume from UE and RAN telemetry creates scalability challenges for collection and analysis • High dependence on probe-based solutions, which are costly and can introduce complexity in integration • Privacy concerns when monitoring subscriber-level activity, requiring strict compliance with regulations • Attackers may leverage device encryption and obfuscation to conceal malicious behavior from network-level detection

1.7 CA, HSM, PKI

Threat case

IAM systems enforce authentication, authorization, and accountability across telecom platforms, OSS/BSS systems, and supporting IT infrastructure. Because IAM sits at the heart of privilege management, it is a prime target for adversaries seeking unauthorized access or persistence.

Key threats may include:

- Credential compromise through phishing, password reuse, or brute-force attacks
- Privilege escalation by exploiting misconfigurations or excessive entitlements in IAM policies
- Abuse of dormant or orphaned accounts, especially those with elevated privileges
- Supply chain risks, where third-party integration into IAM exposes telecom environments
- Insider threats, where legitimate access is abused to manipulate subscriber data, billing systems, or network configurations
- Exploitation of federated identity providers, enabling adversaries to pivot into multiple domains once a trust boundary is compromised

Operational requirements	CAPEX	OPEX	Benefits	Drawbacks
• Centralized logging of authentication and authorization events across telecom and IT systems • Deployment of Privileged Access Management (PAM) for accounts with administrative rights • Enforcement of Multi-Factor Authentication (MFA) across critical systems, especially for remote access • Continuous identity lifecycle management, including detection and removal of dormant accounts • Anomaly detection for unusual access patterns (e.g., time-of-day anomalies, geo-velocity checks) • Segregation of duties to prevent abuse of combined roles or access rights	• Investment in enterprise IAM platforms with telecom-grade integrations (e.g., SSO, LDAP, RADIUS, Diameter) • Procurement of PAM solutions capable of auditing and controlling privileged sessions • Acquisition of user behavior analytics (UBA) or identity threat detection tools to enhance anomaly detection	• Ongoing policy management and entitlement reviews, requiring close coordination between security and HR/operations • Continuous user support overhead (e.g., MFA resets, account provisioning/ de-provisioning) • SOC analyst effort to tune identity-related alerts and reduce false positives • Regular audit and compliance reporting, especially in regulated telecom markets	• Provides centralized visibility into who is accessing what, when, and how • Enables early detection of insider threats and credential misuse • Strengthens compliance posture, aligning with regulatory mandates for privileged access monitoring • Enhances resilience by reducing the blast radius of compromised accounts through least-privilege enforcement	• High integration complexity, especially across heterogeneous telecom and IT environments • Potential for alert fatigue if anomaly detection is poorly tuned • Costly to maintain in environments with large user bases and frequent staff/ contractor turnover • IAM cannot prevent all attacks — compromised privileged accounts can still bypass many detection mechanisms without layered controls

2. Priority Telemetry Sources

The subsections below provide an overview of priority telemetry sources, drawing from the evaluation summary in Appendix D: Summary of Telemetry Evaluation.

In particular, telemetry sources that are natively generated, operationally integrated, and aligned with real-world threat vectors have been prioritized. Sources such as AAA, IAM, and PAM logs form the backbone of credential and access monitoring across domains, while health events and NetFlow data provide high-value insight into the behavior of subscriber and signaling infrastructure.

A more detailed evaluation of telemetry sources, scoring them against practicality, cost of deployment and operation, suitability for AI-driven analysis, and overall detection value across visibility domains is available. This section summarizes the findings, highlighting those sources that offer the highest operational and security benefit in telecommunications environments.

2.1 AAA logs

Authentication, Authorization, and Accounting (AAA) logs are consistently identified as one of the most critical telemetry sources across telecommunications domains. They capture the fundamental records of subscriber authentication, operator logins, service usage, and access control decisions.

Key value

- Provide visibility into credential misuse, privilege escalation, and unauthorized access attempts
- Enable correlation with IAM and PAM logs to strengthen identity-centric detections
- Support fraud detection through anomalous usage patterns at the subscriber level
- Already natively generated by telecom systems such as RADIUS and Diameter servers, making them practical to collect

Considerations

- High log volume requires strong ingestion and filtering pipelines
- Native availability across packet core, OSS/BSS, compute, and platform domains supports broad coverage
- AI/ML models can enhance detection by clustering normal login behavior and flagging anomalies

2.2 PAM logs

PAM logs are indispensable for monitoring the activities of administrative users across telecom systems. They capture session initiations, command executions, and access elevation events, offering granular insight into privileged operations.

Key value

- Detect misuse of high-value accounts (e.g., root, administrator, or operator accounts)
- Provide evidence for insider threat detection and regulatory auditability
- Useful for correlating with configuration change events to validate whether changes were authorized
- Practical to integrate with SOC pipelines through PAM platforms already deployed in many operator environments

Considerations

- Coverage depends on maturity of PAM deployment; gaps exist in legacy or vendor-specific systems
- Generates lower data volumes compared to AAA logs but carries disproportionately high security relevance
- Alerts often require enrichment with IAM or AAA logs to confirm malicious activity

2.3 IAM logs

IAM logs cover the broader authentication and authorization activities across telecom infrastructure, including federated identity systems, directory services, and cloud-native identity providers.

Key value

- Detects credential compromise, brute-force attempts, and privilege escalation across domains
- Complements PAM and AAA logs by adding visibility into normal user accounts and federated identities
- Valuable for tracking dormant or orphaned accounts that may be abused for persistence
- Supported by most enterprise-grade IAM solutions, enabling straightforward collection and integration

Considerations

- Integration complexity increases with multiple identity providers across hybrid telecom environments
- High false positive rates possible without contextual correlation (e.g., geo-velocity anomalies)
- Critical for compliance with telecom regulations requiring centralized access monitoring

2.4 Register health events

Register health events provide visibility into the operational state of subscriber and signaling registries, such as the HSS, UDM, or Authentication Centre (AuC). These events are primarily generated for operational purposes but are of dual value for security monitoring.

Key value

- Detect anomalous registration failures, which may indicate signaling abuse (e.g., SS7 or Diameter exploitation)
- Highlight subscriber database manipulation or fraud attempts through abnormal registration patterns
- Support detection of large-scale denial-of-service conditions where malicious signaling floods overwhelm register capacity
- Provide native, low-cost telemetry as part of routine NOC monitoring, which can be extended to SOC use cases

Considerations

- Event data may lack detail on the root cause (e.g., whether failures are malicious or operational)
- Requires correlation with AAA, signaling, and NetFlow data for actionable detection
- High operational value due to overlap with availability monitoring but limited direct forensic depth

2.5 NetFlow events

NetFlow is a protocol developed by Cisco Systems to capture metadata about IP traffic flows. Instead of full packet payloads, it records summaries of communications between endpoints, providing high-value insights into network behavior.

Key value

- Enables detection of anomalies in signaling traffic (SS7, Diameter, GTP) and backbone routing (e.g., BGP peering)
- Provides visibility into behavioral deviations that may indicate attacks, even without packet payloads and/or cases where the payload is encrypted, as is typically the case in modern mobile networks
- Practical for large-scale telecom environments, as most modern routing and switching fabric supports NetFlow and NetFlow-like collection
- Passive collection method minimizes performance impact on production systems

Considerations

- Requires deployment of flow collectors and supporting infrastructure for ingestion and analysis
- Analysts must train collectors on normal behavior and maintain playbooks for suspicious deviations, particularly for telecom-specific protocols
- SOC integration may be limited if responsibilities are separated between security and network operations teams
- By default, collectors may not prioritize telecom-critical protocols, requiring tuning for effectiveness
- Generates high data volume, demanding scalable storage and analysis pipelines

2.6 Radio health events

Radio health events capture the operational status of RAN devices such as gNodeBs and eNBs. While primarily generated for NOC purposes, they are valuable for detecting anomalous behavior in user connectivity and signaling.

Key value

- Provide visibility into signaling storms or malicious UE activity overwhelming cell towers
- Early indicators of jamming, interference, or misconfiguration impacting service availability
- Useful for correlating subscriber anomalies with radio-level failures
- Naturally occurring telemetry, already monitored by NOC teams, that can be extended to SOC use cases

Considerations

- Limited forensic detail – events typically indicate failure but not root cause
- Requires correlation with subscriber, AAA, and NetFlow data for actionable detection
- May produce high volume of benign alerts due to normal operational variability
- Vendor-specific formats can complicate integration into centralized monitoring systems

2.7 DNS logs

DNS logs record queries and responses at recursive resolvers and authoritative servers. In telecom environments, they underpin critical functions including roaming, service discovery, and subscriber access.

Key value

- Detect tunneling, exfiltration, and command-and-control traffic
- Provide insight into attacks targeting telecom-specific domains (e.g., IMS, EPC, 5G service discovery)
- Early detection of DNS hijacking or poisoning attempts impacting subscriber connectivity
- Strong cross-domain value when correlated with AAA, NetFlow, and register events

Considerations

- Requires investment in DNS security appliances and enrichment via threat intelligence feeds
- High log volume in large subscriber networks demands scalable collection and analysis infrastructure
- Encrypted DNS traffic (DoH/DoT) reduces visibility unless mitigated.
- Standalone DNS logs lack context – must be enriched for actionable insights

2.8 IDS logs

Intrusion Detection System (IDS) logs provide visibility into suspicious or malicious network traffic patterns. In telecom environments, IDS solutions are often deployed at interconnect points, transport layers, and critical data centres.

Key value

- Detects known attack signatures (e.g., signaling abuse, lateral movement, brute-force attempts)
- Provides early warning of anomalous network activity not captured by higher-level telemetry
- Complements NetFlow and firewall logs by adding payload-level visibility
- Supports compliance requirements for monitoring external interconnects and peering arrangements

Considerations

- Signature-based IDS requires frequent updates to remain effective against evolving telecom-specific threats
- High false positive rates unless tuned for telecom protocols (SS7, Diameter, GTP)
- May require specialized appliances or virtual sensors for scalability in large operator networks
- Generates significant alert volume, demanding efficient triage and correlation with other telemetry sources

2.9 Application logs

Application logs originate from OSS/BSS platforms, subscriber management portals, and API gateways. They provide fine-grained visibility into service workflows and user interactions.

Key value

- Detect application-layer attacks such as SQL injection, API misuse, and fraud attempts
- Provide visibility into subscriber provisioning, billing, and service access patterns
- Enable detection of insider misuse or misconfigurations in OSS/BSS workflows
- Complement database and protocol logs for a full picture of application activity

Considerations

- Volume and diversity of application logs vary widely across vendors
- Normalization is required before they can be integrated into Security Information and Event Management (SIEM) pipelines
- May lack standardization, requiring vendor-specific parsing and enrichment
- False positives are common unless baseline behavior is well understood

2.10 Behavioral anomaly events

Behavioral anomaly events are generated by analytics platforms or AI/ML systems that baseline normal activity and flag deviations. These can apply to signaling flows, user sessions, or network performance data.

Key value

- Enable early detection of unknown or novel attack techniques not covered by signatures
- Scale to high-volume telemetry such as NetFlow, AAA, and Call Detail Records (CDRs), reducing analyst workload
- Valuable for detecting slow-and-low adversary techniques that evade traditional tools
- Enhance fraud detection by correlating anomalies across multiple domains

Considerations

- High risk of false positives if baselines are not tuned to telecom-specific workloads
- Requires significant compute resources and skilled staff to manage models
- May create “black box” detections that are difficult for analysts to interpret
- Dependence on AI/ML requires continuous training and validation as environments evolve

3. Conclusion and Recommendations

The evaluation of detection requirements and telemetry sources demonstrates that effective threat detection in telecommunications cannot rely on theoretical frameworks alone. Instead, it must be grounded in practical, operationally feasible telemetry that leverages what is already present in networks, platforms, and subscriber systems.

Several clear conclusions emerge from this study:

Practicality outweighs theory – While frameworks such as MITRE FiGHT™, GSMA MoTIF, and ETSI guidance provide essential context, many of the controls they describe are not operationally achievable without major architectural changes. Practical detections must be built on natively available logs and events (e.g., AAA, DNS, NetFlow, register health).

Dual-use telemetry is the most valuable – Data streams already collected by NOC teams for service assurance (e.g., radio health, SNMP, register events) provide strong security insights when integrated into SOC workflows. This reduces CAPEX/OPEX and accelerates deployment.

Credential and access monitoring is foundational – IAM, PAM, and AAA logs consistently provide high detection value across all visibility domains. Without strong identity-centric telemetry, adversaries can escalate privileges or persist undetected.

Network-centric telemetry underpins visibility – NetFlow, IDS, and protocol logs remain critical for detecting signaling abuse, route manipulation, and lateral movement. These sources are particularly important in interconnect and transport domains where subscriber context is limited.

AI/ML will be required at scale – High-volume telemetry (e.g., NetFlow, CDRs, DNS logs) cannot be effectively reviewed manually. Automated anomaly detection, clustering, and predictive models are essential to ensure scalability while maintaining detection fidelity.

Blind spots remain – Domains such as RAN and transport provide limited native telemetry. These gaps must be mitigated by complementary monitoring solutions (e.g., probes, signaling firewalls) or by correlating indirect indicators across domains.

Regulatory drivers must not be ignored – Governments and standards bodies increasingly mandate visibility into signaling, lawful interception, and subscriber identity protection. Aligning telemetry priorities with these requirements strengthens compliance and justifies investment.

Based on these conclusions, the following recommendations are proposed for telecommunications service providers:

Prioritize high-value telemetry sources such as AAA, IAM, PAM, DNS, NetFlow, and register health events, which consistently deliver strong detection coverage at relatively low cost.

Leverage operational telemetry already in use by NOC teams, repurposing it for SOC functions to minimize additional overhead.

Invest in correlation and enrichment platforms that combine multiple streams (e.g., DNS + NetFlow + AAA) to reduce false positives and increase detection fidelity.

Adopt AI/ML analytics for high-throughput data sources, ensuring that anomaly detection models are continuously trained and tuned for telecom-specific workloads.

Mitigate blind spots in transport and RAN domains by deploying specialized probes or signaling firewalls, ensuring that adversary activity cannot bypass monitoring.

Embed security in platform and compute infrastructure by enforcing IAM and PAM controls, monitoring configuration changes, and integrating with cloud-native security services.

Align with regulatory frameworks (e.g., ETSI, GSMA, CISA) not only for compliance but also as a means of prioritizing investments that are both mandatory and high value.

Develop cross-domain operational playbooks that integrate SOC and NOC workflows, enabling coordinated responses to events that impact both performance and security.

In summary, the most effective strategy for telecommunications threat detection is one that balances practicality, scalability, and regulatory alignment. By focusing on naturally occurring telemetry and integrating it into a layered detection architecture, operators can achieve meaningful visibility into adversary tactics while minimizing cost and operational disruption.

Bibliography

- Integrating Telecommunications Infrastructure with a SOC, Cisco
- A Vision for Telecommunications Security, ETSI
- Enhanced Visibility and Hardening Guidance for Communications Infrastructure, CISA
- FS.57 Mobile Threat Intelligence Framework (MoTIF) Principles, GSMA
- FiGHT™ (5G Hierarchy of Threats), MITRE
- Telecommunications Security Code of Practice, UK DCMS
- FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines, GSMA
- Signaling Security in Telecom SS7/Diameter/5G, ENISA

Appendix A: Descriptions of Telemetry Sources

The following is a table describing the individual telemetry sources. Note that section 2 covers a subset of these sources, prioritized based on these evaluation criteria.

Telemetry Source	Description	Example
AAA logs	Records of authentication, authorization, and accounting activities for subscribers and operators	RADIUS/Diameter logs showing subscriber session authentication and service usage
PAM logs	Logs from Privileged Access Management systems capturing administrative account activity	Session recordings, command execution logs, and access elevation attempts
IAM logs	Identity and Access Management logs covering user authentication, role assignments, and authorization checks.	Active Directory login attempts, SSO token issuance, or LDAP binds
Register health events	Operational events reflecting the status and availability of subscriber registration systems	HSS or UDM reporting abnormal registration failures or capacity issues
NetFlow events	Flow-level metadata capturing source/ destination, ports, and traffic volumes across the network	NetFlow/IPFIX data showing unusual signaling traffic between peer operators
IDS logs	Alerts and logs generated by intrusion detection systems monitoring network traffic	Suricata/Snort logs detecting anomalous Diameter or SS7 packets
Radio health events	Telemetry reflecting the performance and stability of radio access equipment	gNodeB or eNodeB alarms reporting cell congestion or interference
DNS logs	Logs of DNS queries and responses used for service discovery and internet resolution	Queries for `ims.mnc001.mcc001.3gppnetwork.org` or abnormal tunneling attempts
Application logs	Logs generated by OSS/BSS applications and telecom service platforms	Provisioning system activity, billing API access logs

Table A-1: Telemetry Source Descriptions (Part 1)

Telemetry Source	Description	Example
Behavioral anomaly events	AI/ML-driven outputs highlighting deviations from normal activity patterns	Anomaly detection model flagging unusual signaling flow patterns
Config change events	Records of changes to configuration files, parameters, or device policies	Router ACL modification or Kubernetes manifest update
Protocol logs	Logs capturing interactions of telecom-specific signaling or service protocols	SS7 MAP message traces, SIP INVITE logs
Process data	Operating system-level process creation and execution details	Linux audit logs showing unauthorized binary execution
Radio logs	Detailed logs of radio signaling and performance metrics	Call setup failures or abnormal handover patterns in eNodeB logs
Asset data	Inventory and state information about devices, systems, and components	CMDB records of base stations, routers, and virtual network functions
Management connection events	Logs of administrative connections to devices or platforms	SSH login attempts to routers or API access to orchestration platforms
Vulnerability data	Reports and scan results identifying system or software weaknesses	Nessus scan results showing unpatched CVEs in packet core servers
MFA logs	Multi-factor authentication system logs capturing verification events	OTP validation success/ failure for operator console logins
OS logs	Logs generated by operating systems for general activity and errors	Windows Event Logs, Linux syslog entries
EDR events	Endpoint Detection and Response logs from monitored servers or endpoints	Alerts for persistence mechanisms or malicious binaries
Security auditing events	Logs created to satisfy compliance or regulatory auditing requirements.	Privileged user access reports, file integrity audit logs.
VPN logs	Logs of virtual private network session activity	IPsec tunnel establishment logs, remote operator login attempts

Table A-1: Telemetry Source Descriptions (Part 2)

Telemetry Source	Description	Example
SNMP health events	Device health and performance metrics collected via SNMP	Router CPU/memory utilization or interface errors
Firewall logs	Records of traffic allowed, denied, or filtered by firewall rules	Dropped GTP traffic from unauthorized peer network
Certificate logs	Logs of certificate issuance, renewal, or revocation	PKI issuing TLS certificates for gNodeB authentication
Security alert events	Alerts from security tools and monitoring platforms	Cloud-native alert for abnormal IAM role usage
System logs	General operating system or application system events	Kernel crash logs, service startup messages
Version data	Information on software and firmware versions across infrastructure	Router firmware version inventory for patch management
Threat intel data	External or internal feeds describing known adversary TTPs, IoCs, or domains	STIX/TAXII feeds listing malicious signaling endpoints
Config data	Stored system and device configuration baselines	Backup of BGP router configs for integrity comparison

Table A-1: Telemetry Source Descriptions (Part 3)

Appendix B: Telemetry Source Matrix

The following is a table detailing the source components and visibility domains individual telemetry sources enable. Note that section 2 covers a subset of these sources, prioritized based on these evaluation criteria.

Source Component	Visibility Domain	AAA logs	Application logs	Asset data	Certificate logs	Config data	Config change events	EDR events
DNS	DNS							
PKI	CA, HSM, PKI				Certificate logs			
Cloud	Platform	AAA logs		Asset data		Config data	Config change events	
Platform	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport	AAA logs		Asset data		Config data	Config change events	
Database		AAA logs						
API	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Transport	AAA logs	Application logs					
Application		AAA logs	Application logs	Asset data		Config data	Config change events	
Web server			Web server logs					
WAF/LB/API gateway			Web server logs					
PAWS	Compute	AAA logs		Asset data		Config data	Config change events	EDR events
Servers	Compute	AAA logs		Asset data		Config data	Config change events	EDR events
RAN device	User Equipment, Voice, Data	AAA logs		Asset data		Config data	Config change events	
R+S device	Transport	AAA logs		Asset data		Config data	Config change events	
Network	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport							

Table B-2: Telemetry Source Matrix (Part 1)

Source Component	Visibility Domain	Firewall logs	IDS logs	Management connection events	NetFlow events	OS logs	PAM logs	IAM logs	System logs
DNS	DNS								
PKI	CA, HSM, PKI								
Cloud	Platform			Management connection events	NetFlow events		PAM logs	IAM logs	
Platform	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport			Management connection events			PAM logs	IAM logs	
Database				Management connection events					
API	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Transport			Management connection events					
Application				Management connection events					
Web server									
WAF/LB/API gateway									
PAWS	Compute	Firewall logs		Management connection events		OS logs			System logs
Servers	Compute	Firewall logs		Management connection events		OS logs			System logs
RAN device	User Equipment, Voice, Data	Firewall logs		Management connection events					System logs
R+S device	Transport	Firewall logs		Management connection events					System logs
Network	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport		IDS logs		NetFlow events				

Table B-2: Telemetry Source Matrix (Part 2)

Source Component	Visibility Domain	Process data	Protocol logs	Radio logs	Security auditing events	Security alert events	Behavioral anomaly events	Register health events	SNMP health events
DNS	DNS								
PKI	CA, HSM, PKI								
Cloud	Platform				Security auditing events	Security alert events	Behavioral anomaly events		
Platform	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport				Security auditing events	Security alert events	Behavioral anomaly events	Register health events	SNMP health events
Database					Security auditing events	Security alert events			
API	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Transport		Protocol logs		Security auditing events	Security alert events		Register health events	
Application			Protocol logs		Security auditing events	Security alert events		Register health events	
Web server									
WAF/LB/API gateway			Protocol logs						
PAWS	Compute	Process data			Security auditing events	Security alert events			
Servers	Compute	Process data			Security auditing events	Security alert events			SNMP health events
RAN device	User Equipment, Voice, Data		Protocol logs	Radio logs	Security auditing events	Security alert events			SNMP health events
R+S device	Transport		Protocol logs		Security auditing events	Security alert events			SNMP health events
Network	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport								

Table B-2: Telemetry Source Matrix (Part 3)

Source Component	Visibility Domain	Radio health events	Version data	Vulnerability data	Threat intel data	DNS logs	MFA logs	VPN logs
DNS	DNS					DNS logs		
PKI	CA, HSM, PKI							
Cloud	Platform		Version data	Vulnerability data	Threat intel data			
Platform	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport	Radio health events	Version data	Vulnerability data	Threat intel data			
Database								
API	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Transport							
Application			Version data	Vulnerability data	Threat intel data			
Web server					Threat intel data			
WAF/LB/API gateway								
PAWS	Compute		Version data	Vulnerability data	Threat intel data		MFA logs	VPN logs
Servers	Compute		Version data	Vulnerability data	Threat intel data			
RAN device	User Equipment, Voice, Data	Radio health events	Version data	Vulnerability data	Threat intel data			
R+S device	Transport		Version data	Vulnerability data	Threat intel data			
Network	OSS/BSS, Radio Access Network, Packet Core, Subscriber Databases, Compute, Transport							

Table B-2: Telemetry Source Matrix (Part 4)

Appendix C: Summary of Telemetry Evaluation

The following is a table summarising how each telemetry source performs against the various evaluation criteria with respect to practicality, costs, and benefits. Note that section 2 covers a subset of these sources, prioritized based on these evaluation criteria.

Telemetry Source	Existing Capability	Naturally Occurring	AI Suitability	Cost of Deployment (Changed Required)	Cost of Operation (Expected Throughput) Efficacy of Ingestion	Efficacy of Ingestion
AAA logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	High	High	High
Application logs	Varies	Yes	Clustering, Predictive and Anomaly Analysis	Medium	High	Low
Asset data	No	No	Clustering and Anomaly Analysis	High	High	Low
Behavioral anomaly events	Varies	No	Clustering, Predictive and Anomaly Analysis	Medium	High	Medium
Certificate logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	Low	Medium	Low
Config change events	No	No	Clustering, Predictive and Anomaly Analysis	High	High	Medium
Config data	Varies	Yes	Rules	High	High	Low
DNS logs	No	Yes	Clustering, Predictive and Anomaly Analysis	High	High	Medium
EDR events	Yes	Yes	Native	High	High	High
Firewall logs	Varies	Yes	Clustering, Predictive and Anomaly Analysis	High	High	Medium
IAM logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	Medium	High	High
IDS logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	Medium	High	High
Management connection events	No	No	Clustering, Predictive and Anomaly Analysis	High	High	Medium

Table C-1: Telemetry Evaluation Summary (Part 1)

Telemetry Source	Existing Capability	Naturally Occurring	AI Suitability	Cost of Deployment (Changed Required)	Cost of Operation (Expected Throughput) Efficacy of Ingestion	Efficacy of Ingestion
MFA logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	Low	Medium	High
NetFlow events	Varies	Yes	Clustering, Predictive and Anomaly Analysis	Medium	High	Medium
OS logs	Varies	Yes	Clustering, Predictive and Anomaly Analysis	High	High	Low
PAM logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	Medium	High	High
Process data	No	No	Clustering, Predictive and Anomaly Analysis	High	High	Low
Protocol logs	Varies	Yes	Clustering, Predictive and Anomaly Analysis	Medium	High	Medium
Radio health events	Varies	Yes	Native	Medium	High	High
Radio logs	Varies	Yes	Clustering, Predictive and Anomaly Analysis	High	Medium	Medium
Register health events	Varies	Yes	Native	Medium	High	High
Security alert events	Yes	Yes	Clustering, Predictive and Anomaly Analysis	High	High	High
Security auditing events	Varies	No	Clustering, Predictive and Anomaly Analysis	High	High	Medium
SNMP health events	Varies	No	Native	High	High	Medium
System logs	Varies	Yes	Clustering, Predictive and Anomaly Analysis	High	High	Low
Threat intel data	Varies	Yes	Clustering, Predictive and Anomaly Analysis	High	High	High
Version data	Yes	Yes	Clustering, Predictive and Anomaly Analysis	High	High	Medium
VPN logs	Yes	Yes	Clustering, Predictive and Anomaly Analysis	Low	Medium	High
Vulnerability data	Varies	No	Clustering, Predictive and Anomaly Analysis	High	High	High

Table C-1: Telemetry Evaluation Summary (Part 2)

GLOBAL CYBERSECURITY FORUM

stc