XDR IN 5G NETWORKS: ENHANCING TELCO SECURITY THROUGH GENERATIVE AI

Michela Menting, Senior Research Director

ABIresearch THE TECH INTELLIGENCE EXPERTS™ NOKIA

CONTENTS

THE EXPANSION OF XDR INTO 5G NETWORKS: XDR MEETS 5G

Cybersecurity technologies continue to evolve and improve, and the world of Extended Detection and Response (XDR) emerges against the continued expansion of the threat landscape. Crucially, cybersecurity innovation is also expanding quickly into non-traditional Information Technology (IT) markets such as telecommunications. In large part, the new 5G architecture is pushing a rethink on how security can be most effectively implemented and deployed, offering an opportunity to leverage the latest technologies such as XDR.

Benefits of XDR

XDR provides a holistic and integrated approach to threat management. Its strength as a solution lies in its ability to see, collect, and correlate telemetry data from various sources in an infrastructure, including endpoints, networks, cloud platforms, applications, etc. Having a bird's-eye view provides a wealth of information that can paint a more accurate picture of a telco's cybersecurity posture at any given time.

Underscoring that process is the use of Artificial Intelligence (AI) and automation, which today are the power lifters in threat investigation. They facilitate the orchestration of an informed and timely response, bringing XDR as close to real time as possible in order to minimize attack windows; something that will be key, especially in 5G mission-critical applications.

One of the advantages of XDR capabilities is that data analysis can be aligned to a security framework, customized by the end user or defined by industry standards. In this vein, the MITRE FiGHT security matrix of adversary tactics and techniques for 5G systems are a great match for telco XDR deployments.

Requirements of 5G

Specificities of 5G

While revolutionary, XDR remains an offspring of the IT world, and to work comprehensively for 5G networks, it has to understand 5G specificities. Implementing XDR already requires complex integration with existing IT and security tools. In the case of 5G, a different infrastructure needs to be learned, spanning the core, transport, and Radio Access Networks (RANs); all of which are distinctive and complex in their own ways.

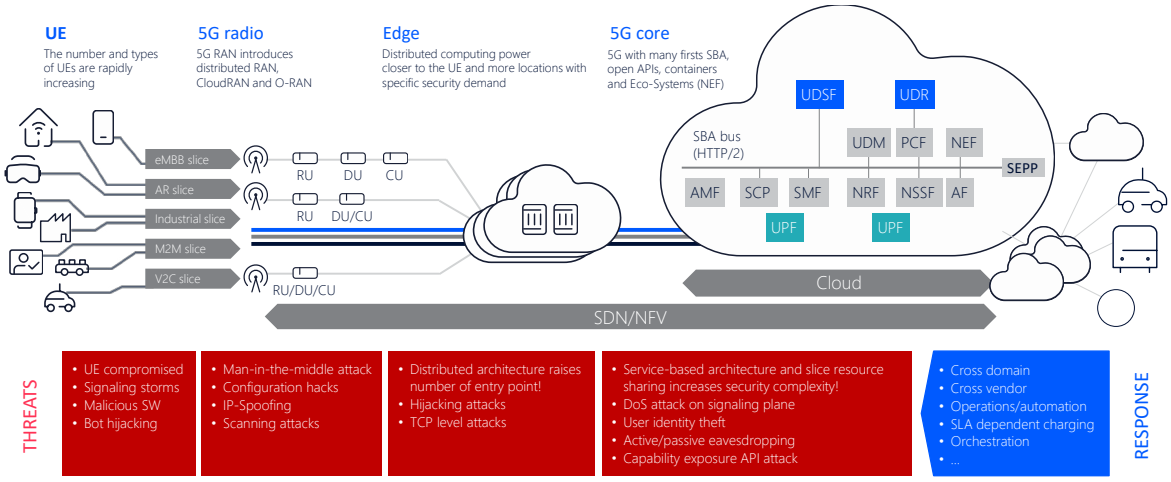
The 5G core, with its software-based architecture, will be home to Cloud Network Functions (CNFs), containers, and open Application Programming Interfaces (APIs). CNFs used in 5G core are compute-intensive and more complex than in traditional settings, with heavy Central Processing Unit (CPU) cycles that can affect service quality. Moreover, Network Function Virtualization (NFV) in 5G should ideally bypass kernel usage as the overhead can impact network performance significantly. The RAN can be implemented in various ways: in a distributed fashion, in the cloud, or based on open interfaces (O-RAN). Mobile Edge Computing (MEC) will distribute computing power to a growing number of user equipment. Network slices can be created ad-hoc with varying topologies and lifecycles. These technologies present a stark departure from the known space where XDR traditionally operates.

Vodafone Portugal experienced widespread service disruption in February 2022 on its 4G/5G network as a result of a massive DDoS attack against its infrastructure, impacting service to 4.7 million customers over a 48 hour period.

Telco Threats

The 5G environment is exponentially more complex than traditional enterprise networks, marrying large telecoms infrastructure and processes with new and open IT architectures. This will undoubtedly introduce IT threat vectors into the 5G space. Moreover, 5G Non-Standalone (NSA) bridges the gap with previous cellular generations, meaning legacy cellular threats will port over to new 5G radio networks.

5G network architecture introduces fundamental new challenges in security



In 2022, Optus Australia was the target of a high-profile data breach, which leaked personal information on 10 million customers. An API vulnerability was exploited by the threat actors to obtain access to the network and customer information.

Many of these existing telco threats primarily target the signaling plane: Malware such as GTPDOOR (a malware that leverages the General Packet Radio Service (GPRS) tunneling protocol), the well-known vulnerabilities in Diameter and SS7 protocols allowing for man-in-the-middle attacks to eavesdrop on subscriber and network data, Distributed Denial of Service (DDoS) attacks on the signaling plane, and spikes in control signaling resulting in signaling storms; all of these are already manifest in 5G networks. Beyond that, new threats will increasingly focus on exploiting roaming interfaces, network functions, and APIs, as these grow in usage.

Role of 5G as a Critical Infrastructure

Threats against telecoms infrastructure have always been constant, if somewhat muted, but now with many of the new 5G architectural features derived from IT environments, attacks are expected to increase considerably. This poses serious issues, especially because of the nature of telecommunications networks as part of a nation's critical infrastructure. Telcos play a determinant role in society and the myriad industries they serve. What's more, 5G evolution is set to connect ever more businesses and services, further cementing their role as providers of the fundamental building blocks of modern connected societies. Any interruption to or degradation in telco networks would have serious adverse effects to entire nations, which could be economically disruptive, physically damaging, and even life-threatening.

5G-Specific Standards & Regulations

For this reason, the telco space is highly standardized and regulated. During the 5G standards development phase, stakeholders made a concerted effort to integrate security mechanisms within the new architecture, much more so than in any previous cellular generation. A dedicated work group within The 3rd Generation Partnership Project (3GPP), the TSG SA WG3 (SA3), was specifically responsible for defining protocols and other requirements in security and privacy for 5G. These include signaling encryption and integrity, mutual authentication between the user equipment and the network, and subscriber identity protection through concealment, among other measures.

Beyond that, the criticality of 5G networks has been increasingly recognized by governments, resulting in new regulations reinforcing security assurance in telecom networks, for example in many European Union countries, in North America and in Asia Pacific.

Both standards and regulation entail compliance, which can differ significantly based on region (for the regulations) and on deployment models (for the standards, as some of the security requirements are mandatory to integrate, but optional to deploy).

Therefore, XDR Must Be Adapted

ABI Research expects GenAI in telco security applications to experience explosive growth in the 2024-2028 rollout period, with a CAGR of 336% as mobile network operators embrace the technology.

So what does this mean for XDR solutions? In large part, it will require substantial adaptation of existing commercial XDR solutions, many of which have been designed for enterprise IT networks. XDR solutions must not only understand the very different architecture that is 5G, but also learn to recognize the specific threats and vulnerabilities derived from this infrastructure, while taking into account the distinctive standard requirements for 5G security, and the growing regulation emerging in the space.

A telco-centric XDR must, therefore, be crafted differently and be positioned as a distinct solution from existing XDRs, rather than as an extension of them. It inevitably brings different capabilities to the fore, with a different user base at the helm—Mobile Network Operators (MNOs).

In large part, MNOs' use of XDR solutions will be primarily as part of a Security Operations Center (SOC). A first expansion on Network Operations Centers (NOCs) into the telco space to optimize business transformation is now evolving into NOC/SOC convergence, with the new demands from 5G in terms of security and privacy of their infrastructure. In turn, telcos will be able to leverage these SOCs to provide security services to enterprise clients. XDRs, and in particular telco-centric XDR solutions, are the key to augmenting 5G SOC capabilities.

GEN AI TO THE RESCUE: LEVERAGING LLMS TO ENHANCE 5G XDR

The Role of AI & ML in Automating Detection and Response

One of the advantages of leveraging AI in threat detection is to autonomously activate threat analysis and dynamic threat scores, which can be used to qualify the severity of a particular theat.

One of the primary tenets of XDR is the aggregation and correlation of telemetry data from many sources—of which there may be hundreds of thousands in 5G networks. The number of datapoints is exponentially greater than in any existing enterprise IT network. For this reason, AI and Machine Learning (ML) are crucial to identifying and responding to threats in a timely manner. They can allow for faster threat detection, ideally in real time, and initiate a number of standardized responses through automated playbooks for common and well-known attacks.

For example, one of the advantages of leveraging AI in threat detection is to autonomously activate threat analysis, and dynamic threat scores are often used to this end to qualify the severity of a particular theat. A scoring system allows for effective prioritization to be communicated quickly, and an appropriate response mechanism can be triggered. These technologies can significantly help to streamline the response process.

However, traditional AI and ML have their limitations. There is the perennial issue of obtaining high-quality labeled data to train the models that can perform accurate threat scoring and reduce the noise of false positives, for example. Furthermore, manual intervention is still required for any high-level alert or events that are out of the ordinary, and for 5G networks, that may well be the vast majority of them because much of the threat landscape is unknown. Certainly, as a critical infrastructure, telco networks will have a much higher instance of manual supervision, as a missed threat could potentially cause service disruption or an outage.

Solving the Pain Point with Gen AI

LLMs assist security analysts in threat management by detecting nuanced patterns and simplifying complex data.

One of the most promising technologies that could enhance XDR's ML capabilities for threat detection and response is Gen AI, and specifically Large Language Models (LLMs). A fast-maturing technology, it is significantly superior at data ingestion and analysis, enabling more complete and rapid examination of situations, rapidly suggesting suitable mitigation strategies and improving automated response mechanisms.

LLMs are especially useful in discovering new patterns in all kinds of data (including unlabeled data), therefore greatly improving anomaly detection. And because XDR aggregates and correlates data from many different sources, it becomes particularly useful in conjunction with LLMs, providing deep visibility into every aspect of a network and, therefore, a rich dataset on which to train the model.

When trained on specific domains, such as cybersecurity in telco, LLMs are especially performant, with increased accuracy in complex pattern detection. It is this particular ability to contextualize that differentiates LLMs from traditional ML, which tends to focus more on pattern matching, often leading to false positives and overfitting.

Contextual understanding allows LLMs to actually see nuances in patterns, rather than just comparing them to a known set. It can derive meaning from that pattern, and use that to create new information on different aspects of an attack, such as vectors or origins. LLMs are not constrained in the manner that traditional ML is, because they can use this new, additional information for novel threat detection. This is especially useful in threat simulation.

But where LLMs really allow XDRs to improve is in the response mechanism. Not only does an LLM's key ability lie in processing natural language, but it can also translate machine language (such as logs and API call functions) into natural language. It can act as an intermediary between complex and diverse cybersecurity tools (e.g., Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), Security Orchestration, Automation, and Response (SOAR), firewalls, etc.) and relate that information simply to an analyst.

Take, for instance, a dynamic threat scoring done with the contextual understanding of the network. A more meaningful level of analysis when qualifying the threat can emerge, which can then be used to fine-tune the response playbooks (often derived from SOAR tools)—a unique playbook can, therefore, be created for each event, every time.

The playbooks are generated autonomously in response to each flagged event, assisting SOC analysts in their response by aggregating the pertinent information and suggesting the various remediation steps that can be taken. Leveraging the LLM in an XDR offers a much faster and more centralized process for an SOC analyst than having to individually investigate the different data sources and then undertake all the necessary steps to contain the threat.

This is particularly pertinent in the SOC space, where Tier Three security analysts are few and far between. An LLM could extend the skill capacity of Tier One and Tier Two analysts, lightening the workload of more expert analysts.

Consequently, LLM-powered XDRs are an excellent fit in SOC environments, as they can radically improve response times by cutting out a lot of the manual intermediary steps. Coupled with its superior capacity in threat detection, they can mitigate some of the pressures on SOCs in a field where there is a massive skills shortage.

How LLMs Can Be a Game Changer for XDR in 5G

Even with LLM capabilities, training and maintaining of a telco GenAI model is crucial to detect 5G-related threats.

So what is the benefit specifically for 5G networks? Well, LLMs require accessible training data of a large size and diversity. And 5G networks are a great fit because they are large and complex, spanning countries and continents, serving many different use cases and applications (from Enhanced Mobile Broadband (eMBB) to Massive Machine-Type Communication (mMTC), to Ultra-Reliable Low Latency Communication (URLLC)), and with diverse network topologies.

They are perfect for providing the large amounts of data needed to feed LLMs. But their successful deployment is contingent on the ability to train the model effectively on 5G networks. Understanding the context and the specifics of 5G network topology, and fitting it to the operational parameters of an XDR, is an important first step for data analysts.

To 5G's advantage, LLMs can significantly improve a number of XDR capabilities that are crucial to the telco ecosystem, such as threat impact simulations and compliance reporting. While there are plenty of existing security tools that can provide these capabilities, almost none are trained on 5G networks. A telco-focused approach is, therefore, essential for effectively implementing XDR in a 5G security network. This requires a specialized adaptation of XDR to 5G networks for optimal performance. Even with the inclusion of LLM capabilities, it is crucial to maintain a permanent telco-trained model to ensure that security analysts obtain data relevant to 5G and can swiftly comprehend critical threat situations.

From an attack perspective, the 5G threat landscape is still nascent and unknown, and therefore, LLM-powered threat simulation will play a crucial role in uncovering vulnerabilities and potential

weak links before they are actively targeted. LLMs can focus on simulations specific to the telco space, and ingest relevant sectoral threat intelligence, as well as incorporate models such as the MITRE FiGHT (5G Hierarchy of Threats) matrix for adversary tactics mapping.

The MITRE FiGHT model provides theoretical examples of threatening behavior in the context of 5G systems, specifying the critical assets that could be affected and outlining possible mitigation techniques and detection methods. With this information ingested, LLMs can expand upon that and identify new threats targeting 5G networks. With increased AI-enabled threat proliferation, using LLMs can allow XDRs to "fight fire with fire."

Beyond that, the LLM models are highly adaptable and can easily be continuously trained on new regulatory instruments, as well as technical manuals through their various updates. This specific capability can allow LLMs to incorporate and contextualize the various emerging telco regulations as they emerge, as well as network and security architecture specifications from standardization bodies such as 3GPP, the GSMA, and the U.S. National Institute of Standards and Technology (NIST), among others. The result is that an XDR can be fully capable of understanding 5G topologies that span the RAN, transport network, and the core, both from a technical and compliance perspective, and remain up-to-date without significant redesign or retraining of the model.

Future-Looking

The telecoms industry needs to become more familiar with XDR technology first, and LLM capabilities second, before entrusting them fully with autonomous response.

But beyond that, what makes LLMs really exciting for telco XDR is the potential in automating the response mechanisms. While automated playbooks are relatively common in the industry, they still require a level of manual development and supervision in deployment. This step is easily being overcome today as LLMs are especially useful in being able to craft responses based on feature recognition and relational understanding of raw data. Because they can semantically comprehend the context and, therefore, more accurately detect threats and anomalies, they provide true contextual assessment for an SOC analyst.

Today, the centralization of the response mechanism serves as a precious assistant to an SOC analyst, drastically cutting down on response times. Theoretically, the LLM could undertake that threat response itself in an autonomous capacity. But that would mean that AI is directly intervening on a live network in lieu of an analyst; this is still delicate today because of the critical nature of 5G networks. Defaulting to fully automated responses is a risk, even though it may be the LLM's guided response that the analyst is implementing.

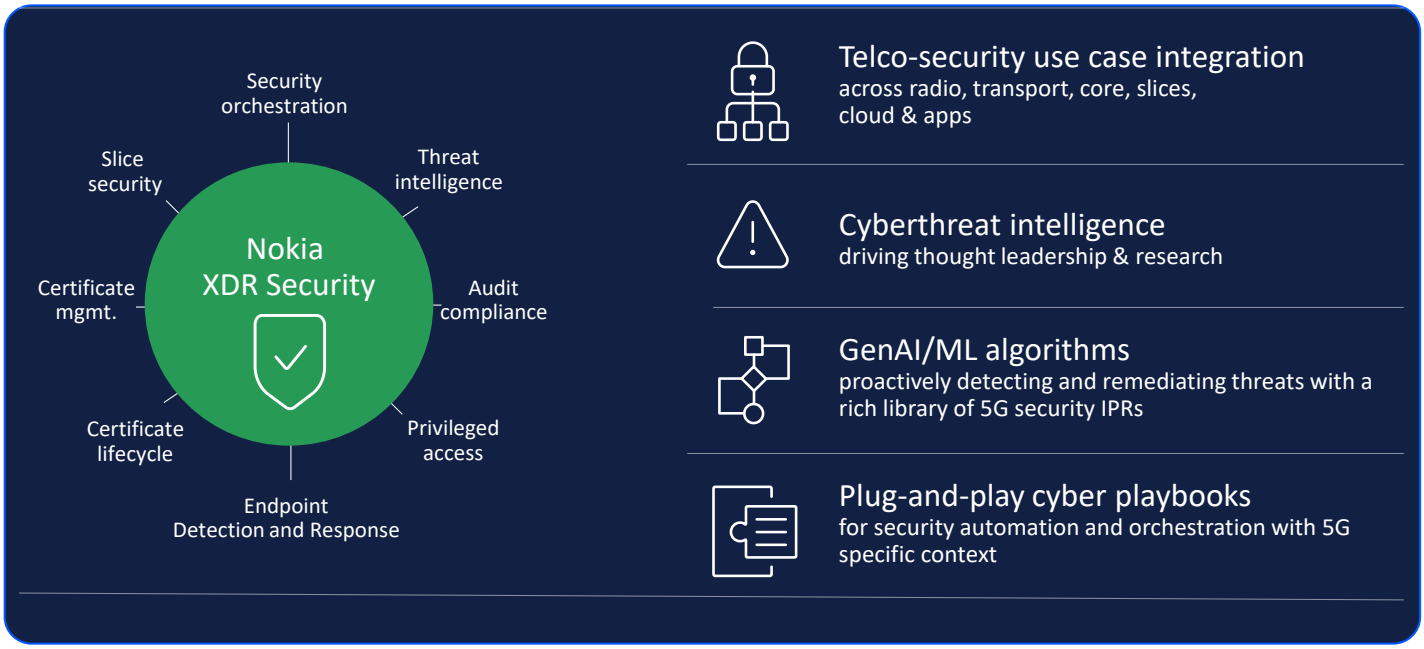
The telecoms industry needs to become more familiar with XDR technology first, and LLM capabilities second, before entrusting them fully with autonomous response. There are many elements to take into consideration, from a critical infrastructure, and technical and compliance perspective, as well as from a security assurance perspective, notably around AI trust and protection against adversarial manipulation of ML models, for example. In fact, the key step to overcome is to arrive at a level where analysts are confident enough in the contextual understanding of an LLM that they can relinquish manual oversight.

It is important to remember that LLMs, and Gen AI more broadly, are still nascent technologies, albeit rapidly evolving ones. In a similar vein, we are still at the inception phase with 5G networks. The future possibilities for what LLMs can potentially achieve are endless within a telco-centric XDR with the right development toolset and expertise.

STRENGTHENING 5G SECURITY WITH NOKIA XDR SECURITY

Nokia has been leading the charge in developing comprehensive cybersecurity solutions for 5G. Its NetGuard Cybersecurity Dome is a cloud-based security orchestration and incident response solution offering a host of capabilities, including detection and response, data correlation, investigations, and dynamic threat scoring.

The NetGuard Cybersecurity Dome utilizes Nokia's XDR components, including threat detection and response on critical network functions, privileged access management, and audit compliance modules, with expansion capabilities into the 5G domain for greater usability. It automates the mapping of security incidents to telco network inventory, streamlining the triaging process.



Nokia Integrated Gen AI in XDR

Nokia leverages Microsoft Azure's OpenAI to enhance its XDR technology with GenAI assistance. The LLM technology has undergone extensive training using data pertaining to 5G network architecture and security practices, assimilating valuable information from multiple standardization and regulatory bodies, including 3GPP and NIST.

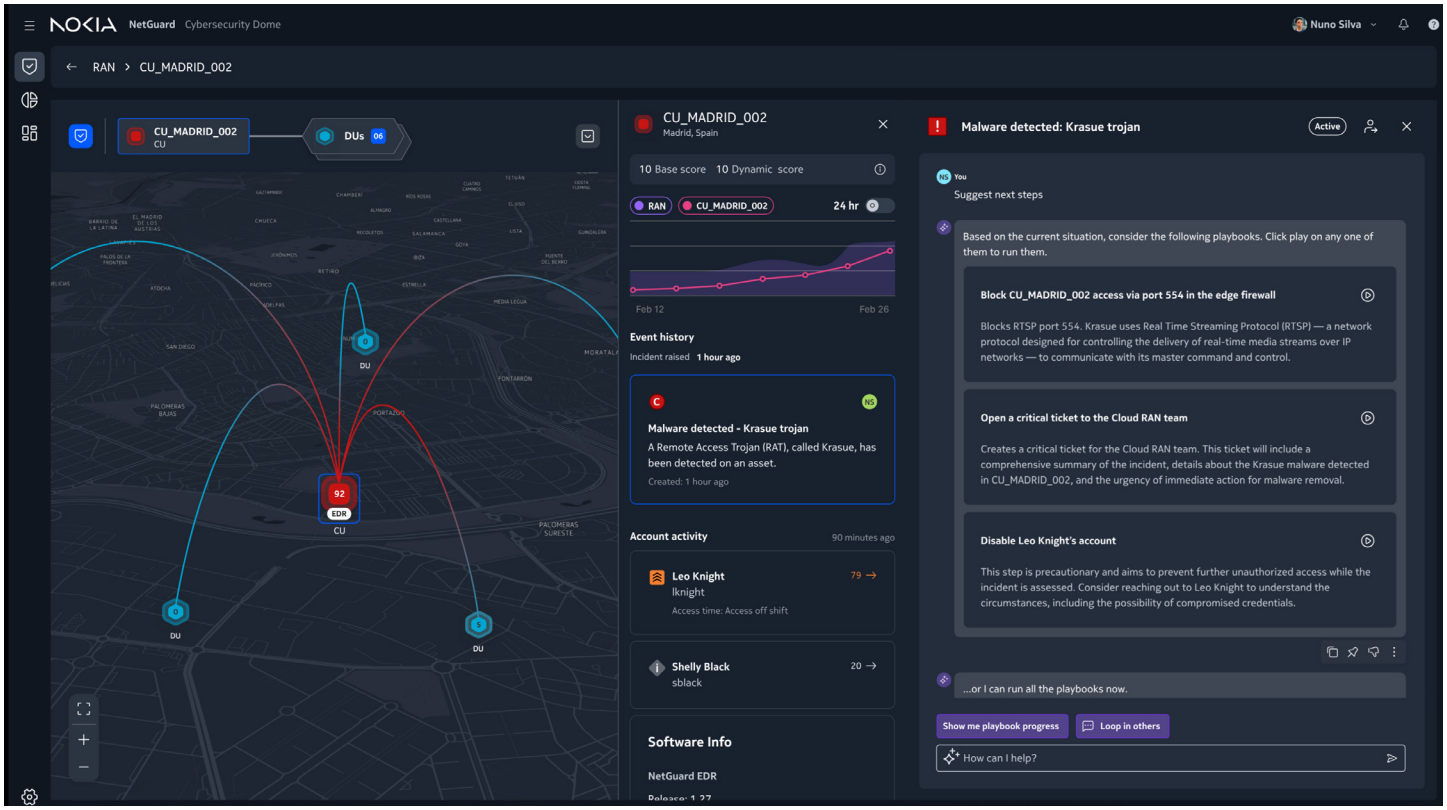
Nokia enhanced its XDR technology with telco GenAI assistance, pre-building over a hundred 5G-specific use cases for RAN, transport, and core networks.

Beyond that, Nokia has been able to leverage its deep expertise in the telco space to further improve the model with its own knowledge base, enabling it to pre-build over a hundred 5G-specific use cases for the RAN, transport, and core networks.

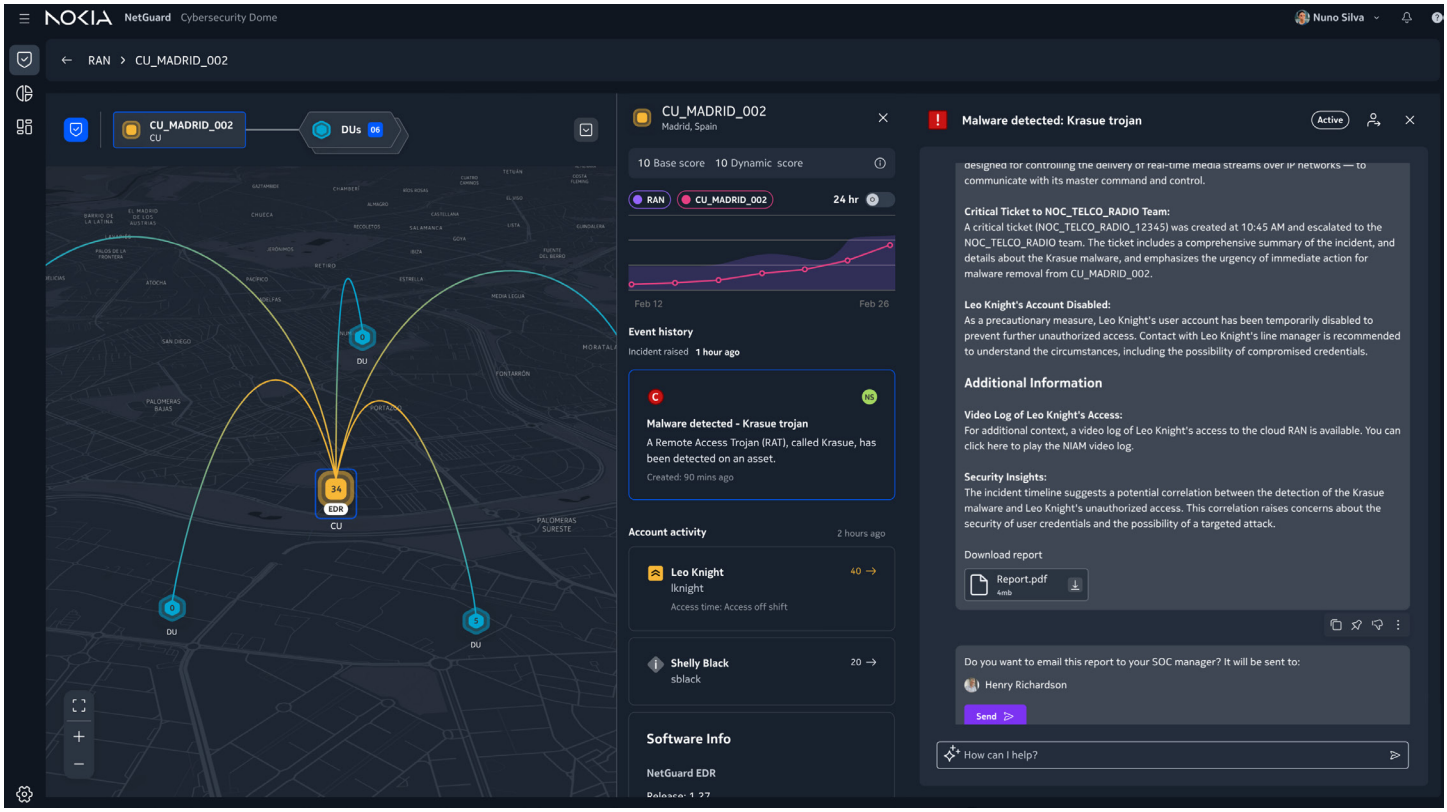
With the advanced integration of telco-centric Gen AI, the NetGuard Cybersecurity Dome empowers security analysts to enhance their skillset and capabilities, enabling faster contextualization and mitigation of cyberattacks and making them much more efficient in responding to incidents in the 5G environment.

Enhancing SOC Analyst Capabilities with Nokia's GenAI Assistant

The SOC analyst's role can, therefore, be greatly enhanced using Nokia's GenAI assistant. Generating an initial smart summary of an event, it provides more contextual information about the detection method, including correlation between various sources. It then offers up a number of AI-suggested questions for an analyst to choose from, or alternatively, the ability to input their own question. The analyst can ask the assistant to query the various security tools at the XDR's disposal to provide additional information to help them in the decision-making process. The analyst can also request recommended remedial next steps, and ask the assistant to outline and run through the relevant playbooks.



Once the event has been successfully handled and closed, the assistant can automatically generate a report to be shared with SOC managers and Chief Information Security Officers (CISOs), and saved for compliance and auditing purposes. In test use cases, the assistant was able to cut down the entire response time by half, enabling telcos to really optimize analyst time. More than anything, it can greatly simplify the workload, a significant advantage for analysts as SOCs tend to be highly complex.



Modularity & Flexibility with NetGuard Cybersecurity Dome

Ultimately, incorporating new technologies such as LLMs can greatly improve the security of 5G networks. Their vast complexity and unique topology are not easy for traditional XDRs to understand, let alone secure. But more than that, 5G network operators have competing demands from an operational perspective that can make security assurance difficult to implement. The enormous investments in deploying 5G networks has been slow in showing a Return on Investment (ROI), as enterprise use cases have not yet fully emerged. Beyond that, there is the enduring issue of seeing security costs as an expenditure, rather than as a value add.

The natively integrated components of Nokia's XDR provide an advantage in creating a modular offering. Nokia has translated its extensive security expertise in telco networks into pre-defined use cases, enhancing the capability to detect security threats specific to telco networks. The Security Assurance Service offers access to pre-built security use case packages tailored to technology domains, encompassing the core, RAN, and transport, each with its set of security use cases. These are designed to identify specific network threats and offer predefined actions for handling security incidents and implementing remediations. The NetGuard Cybersecurity Dome's use case catalog is organized into packages corresponding to each domain: security assurance for core, RAN, and/or transport.

The incorporation of Gen AI technologies, coupled with Nokia's deep telco intelligence, allows for considerable streamlining and improvement of SOC operations.

The implementation of these use cases leverages features and functionalities from the Cybersecurity Dome platform, ensuring the detection of threats, the initiation of relevant incident response, and the provision of one or more remediation actions that can be triggered either manually by an analyst or automatically. In essence, a use case includes information about the necessary data collection required from the telco network, along with rules or Gen AI models to identify actual threats and automatically generate incident response actions containing all pertinent information for subsequent analysis.

This catalog of use cases also means that pricing is modular, which can significantly ease budgetary constraints. Telcos can test the potential ROI for enterprise use cases in small, incremental steps, making the solution an appealing one in a notoriously risk-averse and investment-pressed sector. The Dome's Software-as-a-Service (SaaS) model lends itself particularly well to demands for business agility, enabling rapid scaling or downsizing in comparison to traditional CAPEX models.

Further, telco security teams can keep up with data control and privacy requirements (such as for Personally Identifiable Information (PII)), while also providing a high level of flexibility and up-to-date threat intelligence through a dedicated public cloud instance for XDR intelligence, for example.

Ultimately, the incorporation of Gen AI technologies, coupled with Nokia's deep telco intelligence, allows for considerable streamlining and improvement of SOC operations. Combined with a flexible and modular deployment model, Nokia's Cybersecurity Dome makes for a compelling offering in the 5G space where security assurance is a costly, but necessary requirement.

Published September 2024
157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

We Empower Technology Innovation and Strategic Implementation.

ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers.