analysys mason

NOKIA

Interconnectivity threats and proactive threat discovery

Ralf Rempe, **Adam Salač** and **Oscar Birnbreier**

Executive summary

Dangers of inter-roaming attacks

Inter-roaming attacks exploit vulnerabilities in the signalling protocols (such as SS7 and Diameter) used by mobile networks to enable roaming services. These attacks can lead to severe consequences, including privacy violations, for example location tracking, intercepting calls and SMS, fraud and denial of service attacks that disrupt core network infrastructure. The widespread use of legacy protocols in 2G, 3G and even 4G networks exacerbates these risks, making it crucial for communication service providers (CSPs) to implement robust security measures.

Importance of a balanced security approach

A balanced security approach is essential to effectively mitigate the risks posed in the modern threat landscape, for example by inter-roaming attacks. This approach should integrate:

- **Reactive security measures:** Immediate responses to detected threats, such as isolating affected systems and blocking malicious traffic, are vital to minimise damage and restore normal operations quickly.
- **Proactive threat detection:** Continuous monitoring and analysis of network traffic to identify potential threats before they can cause harm. This includes using behavioural analytics to detect anomalies and insider threats.
- **Automation:** Automating routine security tasks, such as vulnerability scanning and log analysis, to enhance efficiency and allow security teams to focus on more complex issues.

Benefits of AI in security

Artificial intelligence (AI) significantly enhances the effectiveness of security measures by:

- Improving threat detection: AI can analyse vast amounts of data in real-time to identify patterns and anomalies indicative of potential threats.
- Automating responses: AI-driven systems can automatically respond to threats, reducing the time between detection and mitigation.
- Enhancing efficiency: By automating routine tasks, AI reduces the workload on security teams, allowing them to concentrate on strategic activities.

In conclusion, addressing the dangers of inter-roaming attacks requires a comprehensive and balanced security strategy that utilises reactive measures, proactive threat detection as weel as automation and AI plays a crucial role in this strategy.

Importance of interconnectivity in modern telecommunications

Interconnectivity is the backbone of modern telecommunications, ensuring that networks can work together to provide comprehensive and efficient communication services and therefore allowing customers of one network to communicate with customers of another, which is the generic scenario of "roaming", write Dr Ralf Rempe, a senior consultant, Adam Salač, a senior consultant, and Oscar Birnbreier, a director at Analysys Mason.

This interconnection is of such high importance since it is needed to provide a seamless user experience and connectivity and eliminate the need for customers to subscribe to multiple networks to communicate with others. Furthermore, it fosters a competitive marketplace, encouraging innovation and better services as well as supports global commerce activities like electronic banking, e-commerce and mobile roaming, which rely on efficient and reliable network connections. And finally, interconnectivity facilitates the implementation of new technologies, enabling countries to benefit from global connectivity and cost-saving innovations.

Signalling traffic and its critical role in network communication

Signalling traffic in telecommunications refers to the exchange of control information between different network components to establish, manage (= maintain and monitor), and terminate communication connections. This control information is necessary to connect and terminate calls, route data packets and efficiently utilise network resources.

It plays such a critical role in network communications because it allows for efficient resource utilisation by enabling optimal use of network resources by efficiently managing connections. Signalling traffic is also crucial for network security by helping to monitor and control network access to prevent unauthorised activities as well as contributing to and maintaining a high quality of service by ensuring reliable and fast connections.

Threats and risks in interconnectivity with signalling traffic

Overview of signalling traffic

Signalling traffic can be called the command-and-control systems of the telecommunication networks. It enables seamless handover when one subscriber is on the move, assists in location tracking of the subscribers for the purpose of routing calls directly to the correct location and provides various other supporting functions and features.

To develop and establish a system capable of being used worldwide as a standard, SS7 was developed in 1975 by AT&T, was standardised in 1981 and has undergone numerous updates and modifications from time to time. It is a mobile backend protocol used for interconnectivity between mobile operator networks, and here mainly used for communications between the network elements and the networks themselves. It enables roaming and cellular services across operator domains. The main problem with SS7 is that many SS7 systems are outdated and do not support the latest security protocols, because when the SS7 protocol was originally developed in the 1970s, the CSPs were state-owned, access restricted and trust-based, so security threats as we know them today were not considered. While there has been an evolution of SS7 towards better protocols like Diameter, Global Title Translation (GTT) Data Processor (GDP) or HTTP/2 signalling, which pose great leaps in security, these are not immune to threats.

These signalling protocols still have many vulnerabilities that can be exploited by malicious actors. Despite there being an obvious need to enhance the resilience of these mobile networks against cyberattacks by switching from SS7 to an evolved infrastructure, this is often difficult and costly to upgrade, leaving critical gaps in network security[1]. Therefore, most operators update their network infrastructure gradually to avoid service interruption and optimise the return of investment of their infrastructure. Also due to the limited capital of operators, especially in developing countries, these upgrades are not prioritised worldwide as they probably should be. Which in summary leads to the complex nature of roaming infrastructure that can be found in reality.

[1] S. Holtmanns, S. P. Rao and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality," 2016 IFIP Networking Conference (IFIP Networking) and Workshops, Vienna, Austria, 2016, pp. 315-322, doi: 10.1109/IFIPNetworking.2016.7497239.

Threats and risks in interconnectivity with signalling traffic

Inter-roaming threats

Inter-roaming attacks exploit vulnerabilities in the roaming agreements between mobile network operators (MNOs) and in the signalling protocols they use for interconnection. These attacks can be particularly stealthy and harmful due to the complex nature of roaming infrastructure. The arising problem is that to provide seamless user experience and connectivity to roaming partners who might have interconnections only over SS7, irrespective of the mobile technology used (UMTS, LTE or 5G), operators are expected to support the SS7 protocol. And when it comes to exploiting the vulnerabilities of signalling protocols the main attack vector is SS7, because it is still used by approximately 3.9 billion subscribers and can also be used to connect to more modern mobile technologies, since the operators are expected to support the SS7 protocol. So even with the transition to the Diameter protocol in LTE or GTP in 5G networks, inter-roaming attacks remain a concern due to the need for backwards compatibility with SS7.

Types of inter-roaming threats[2]

The mentioned backwards compatibility is used as attack point from hackers, since they only need access to a less secure SS7 network as the entry door for inter-roaming attacks that can be exploited for:

- **Eavesdropping and interception**[3]: Intercept and listen to calls and SMS messages
- **Location tracking**[4,5]: Track the location of a mobile phone by accessing the location data used by mobile operators and shared during roaming
- **Fraud and identity theft**[6]: By intercepting SMS messages, attackers can capture two-factor authentication codes and gain access to bank accounts and other sensitive information
- **Call manipulation**[6]: Redirect or block calls by manipulating signalling or inject malicious signalling messages between mobile networks

As you can see all these threats have been used in real-live attacks[3,4,5,6], but most prominent are those where individual subscribers have been tracked by hackers, like the former German chancellor Angela Merkel[4] or more currently fighter movements in the Ukrainian war to execute attacks[5]. And the subscriber is not aware of these attacks, because they misuse features essential for routing calls directly to the correct location.

[2] K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash and H. Abbas, "SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1337-1371, Secondquarter 2020, doi: 10.1109/COMST.2020.2971757.
[3] https://www.linkedin.com/pulse/hackers-can-access-every-call-message-you-send- world-mayur-agnihotri/
[4] https://www.reuters.com/article/world/us-spy-agency-tapped-german-chancellery-for- decades-wikileaks-idUSKCN0PI2AD/
[5] https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-3/
https://www.sueddeutsche.de/wirtschaft/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

Threats and risks in interconnectivity with signalling traffic

Impact of inter-roaming threats

Inter-roaming attacks can have serious consequences for both mobile network operators (MNOs) and their subscribers. The key impacts are:

Privacy Violations
Intercepted calls and SMS messages can lead to breaches of personal and sensitive information

Service Disruptions
Significant disruptions to communication services can occur by blocking or manipulate signalling messages

Location Tracking
Tracking the location of mobile users is also a privacy violation and can be particularly dangerous for high-profile individuals such as politicians, journalists and activists.

Denial of Service Attack
Overloading the network infrastructure can lead to service outages that affect millions of subscribers

Fraud and Identity Theft
Enabling attackers to access bank accounts and other sensitive services can result in financial or reputational damage

National Security Risks
Inter-roaming attacks can be used for espionage, attackers to spy on other countries by intercepting and manipulating network traffic

These consequences highlight the importance of and improving and expanding the security measures in place for roaming to help prevent inter-roaming attacks.

The need for proactive threat discovery

Intrusion detection systems (IDS) are crucial components in cybersecurity, designed to monitor and analyse network traffic for signs of malicious activity or policy violations. Typically, these systems are placed out of the direct flow of network traffic, often using mirrored traffic for analysis. They in general work either signature-based, where known threats are detected by comparing network traffic against a database of known attack signatures, or anomaly-based, where a baseline of normal network behaviour is established and deviations from this norm are flagged.

While signature-based IDS are effective for identifying known threats, they may struggle with new or unknown attacks. On the other side anomaly-based IDS can detect unknown threats but may generate false positives[7]. Independent if they are signature- or anomaly-based, IDS employ primarily reactive security measures and thereby play a vital role in the overall security posture by providing timely alerts after detecting suspicious activity and detailed insights into potential security incidents by logging detailed information about the detected threats, which is crucial for forensic analysis and understanding the nature of the attack.

Despite the huge importance of reactive security measures in modern cybersecurity, they have also several limitations so many organisations are shifting towards a more proactive security approach, which involves anticipating and preventing threats before they occur. This allows these organisations to stay ahead of cyber threats and ensure a more secure and resilient environment, because these proactive threat discovery measures can mitigate some of the limitations of reactive security measures. But for a robust cybersecurity strategy it is crucial for mobile network operators to balance proactive threat detection and reactive security measures.

Only a combination of reactive security measures with proactive threat detection functionalities can help protect the complex global mobile network infrastructure from the continuously evolving threat landscape. When we look at inter-roaming threats for example, they exploit essential functionalities to establish, manage and terminate communication connections. The control information send via the SS7 protocol is necessary to connect and terminate calls, route data packets and efficiently utilise network resources. So proactive threat discovery may be a way to quicker detect a potential incident, but once it is detected the reactive security measures are the way to better understand the nature of the attack and help in choosing the best mitigation strategy.

To be effective, most IDS are interworking with intrusion prevention systems (IPS), which can be configured to take automated actions, such as blocking traffic from suspicious IP addresses or isolating affected systems, to mitigate the impact of an attack. IPS include anti- virus/anti-malware software, firewall, anti-spoofing software and network traffic monitoring. An IPS security service is typically deployed "in-line" where they sit in the direct communication path between the source and the destination, where it can analyse in real-time all the network traffic flow along that path and take automated preventive action.

Modern threat incident management platforms (e.g. Nokia's 'NetGuard Cybersecurity Dome') are combining all these features.

[7] Alkasassbeh, M., Al-Haj Baddar, S. Intrusion Detection Systems: A State-of-the-Art Taxonomy and Survey. Arab J Sci Eng 48, 10021–10064 (2023). https://doi.org/10.1007/s13369-022-07412-1
[8] https://www.nokia.com/networks/security-portfolio/netguard/cybersecurity-dome/

The need for proactive threat discovery in a balanced approach with reactive security measures

Implications for security operations centre processes

All the described aspects on the previous page can be seen when considering the current workflow in a security operations centre (SOC) of a CSP. When, for example a location tracking attack via SS7 takes place, the IDS detects a potential security incident via proactive threat discovery and alerts the responsible personnel. The agent then could use the IPS to block the traffic from the SS7 network by updating the Access Control List of the Firewall. As a result, the threat and/or its impact is mitigated.

The blocking of all traffic from the SS7 network is a good way to end the attack, so if we are talking about an inter-roaming attack, this may mean to block a complete range of global titles from CSPs. While this is, from a security perspective, the right mitigation strategy, it does not consider all the other implications this measure may have.

Blocking a complete range of global titles from CSPs can result in:

- **Revenue loss:** Affected customers cannot be reached while roaming, which may lead to customer churn and reduced sales
- **Reputational damage:** By negatively affecting customers
- **SLA fails:** Service level agreement cannot be fulfilled which also may have a financial impact by contractual fines that will be executed.

These are some of the reasons why blocking global titles is usually executed time-based, so the traffic will be blocked for eight or 24 hours. This also gives the SOC time to analyse the attack and maybe take additional precautions or adapt their mitigation strategy.

This is also a hint, that proactive threat discovery should be employed in a balanced approach with reactive security measures. So, if the CSP use protective threat discovery, they may be able to quickly detect the attack, which enables them to take actions against the attack. And, by employing the reactive security measures they have in place, they may be able to better understand the nature of the attack, have more insight what the best mitigation strategy might be and how to harden their systems to prevent similar attacks in the future.

Therefore, a combination of proactive threat detection and reactive security measures can provide a better basis for the necessary decisions in choosing the best feasible mitigation strategy. The early detection by proactive threat detection enables the SOC on the one side to quickly limit the impact of the incident and on the other side to collect and provide more data for the needed decisions in a secure way, because reactive security measures are often placed out of the direct flow of network traffic using mirrored traffic for analysis, that cannot further harm the network.

Adding proactive threat discovery to the reactive security measures of IDS/IPS

Limitations of reactive security measures

Reactive security measures, as employed by IDS/IPS, have several logical limitations, since they can only respond to threats after they have been detected:

Delayed Response Significant damage can be caused before the response even has begun

Higher Recovery Costs The aftermath of an attack can be costly, both in terms of financial loss and time required to restore systems and data

Operational Disruption Significant disruptions to business operations, leading to downtime and loss of productivity

Limited Scope Focuses often on mitigating the immediate threat without addressing underlying vulnerabilities that could be exploited in the future

Regulatory and Compliance Risks Failing to prevent attacks can lead to regulatory penalties and damage to an organisation's reputation

Inadequate for Unknown Threats Often rely on known threat signatures and patterns, so that new or sophisticated attacks that do not match these patterns can go undetected

Benefits of proactive threat discovery

Combining reactive security measures with proactive threat discovery offers several significant benefits for organisations by mitigating the limitations of reactive security measures:

Early Detection Identifying potential threats early on helps prevent them from causing significant damage

Reduce Impact By addressing threats immediately, organisations can minimise the amount of data compromised and reduce the overall impact of an attack

Cost Savings Preventing attacks can save significant costs associated with data breaches, including recovery expenses and potential regulatory fines

Operational Continuity Maintaining business operations by preventing disruptions caused by cyberattacks

Improved Security Posture Gain and provide visibility into vulnerabilities, allowing organisations to strengthen their security posture

Enhanced Risk Management Accessing risks before they materialise enables better control over cybersecurity strategies and risk management

Prevent Regulatory Complications Avoiding breaches can prevent regulatory oversights and/or penalties

Reputation Protection Avoiding breaches helps protect an organisation's reputation and maintain the customer's trust

Automation as means for enhanced proactive and reactive security measures

Automation for mitigation

Automation supports organisations in enhancing their ability to detect, respond to and recover from security breaches. It does that by offering the possibility to continuously monitor network traffic, user behaviour and system activities. This real-time surveillance helps in the early detection of anomalies that could indicate a security breach, for example by analysing user behaviour patterns to detect unusual activities that may indicate compromised accounts.

Flagging these anomalies and employing an automated incident response tool can quickly isolate affected systems, lock affected accounts, block malicious traffic and initiate predefined response protocols. This rapid action minimises the impact of breaches and reduces recovery time. Furthermore, automation can integrate threat intelligence feeds to stay updated with the latest threats. By automatically correlating this data with internal logs, organisations can identify and respond to potential threats faster. Additionally, automated tools can regularly scan systems for vulnerabilities and apply patches or updates as needed. This proactive approach ensures that known vulnerabilities are addressed promptly, reducing the risk of exploitation. And lastly, automated systems can generate compliance reports and audit logs, ensuring that organisations meet regulatory requirements and maintain a clear record of security activities. All these automations not only improve overall security posture but also free up human resources to focus on more strategic tasks.

By embracing automation, CSPs can enhance their ability to detect, respond to and mitigate inter-roaming attacks, ultimately improving the overall security of their mobile networks. Employing automated systems to continuously monitor network traffic for unusual patterns or anomalies that may indicate an inter-roaming attack would allow for immediate detection and response, reducing the time attackers have to exploit vulnerabilities. And here an automated incident response can quickly isolate affected network segments, block malicious traffic and initiate remediation processes to minimise the impact of the attack and preventing it from spreading.

Automation can additionally be used to analyse the behaviour of devices and users on the network. By identifying deviations from normal behaviour, automated systems can flag potential threats and take preemptive actions. To ensure that the network defenses are always up-to-date and capable of countering new threats, automated systems can integrate with threat intelligence feeds to stay updated on the latest attack vectors and techniques. In addition, automation reduces the reliance on manual processes, which are prone to human error, so using automated systems to consistently apply security policies and procedures, ensures a more robust defence against inter-roaming attacks. Automated solutions can scale to handle large volumes of network traffic and numerous devices, making them ideal for managing the complexities of inter-roaming scenarios.

Using generative AI (GenAI) for threat discovery

Role of GenAI in cybersecurity

Generative AI (GenAI) is playing an increasingly important role in enhancing CSP's cybersecurity strategies and can help with leveraging the full potential of threat databases as well as help in assessing the risk holistically. It excels at identifying patterns and anomalies in vast amounts of data, which helps detecting potential threats more quickly and accurately as well as assists to identify, classify and prioritise vulnerabilities, ensuring that the most critical issues are addressed first.

GenAI also supports setting up continuous network monitoring that potentially evolves over time regarding detecting attacks and breaches. Another use case of GenAI is analysing email patterns and content to detect and block phishing attempts, which are becoming increasingly sophisticated. By analysing historical data and threat intelligence feeds, GenAI can minimise the time needed to detect unknown threads and/or predict future threats and vulnerabilities, allowing CSPs to take proactive measures to secure their systems. In addition, GenAI can automate responses to security incidents, reducing the time it takes to mitigate threats and minimising the impact on systems. Lastly, GenAI can streamline and enhance the efficiency of SOCs in several ways by making it more efficient, accurate and proactive in handling security threats.

Impact on security operation centre processes

The following benefits of GenAI may be used to enhance the processes within the SOC of a CSP:

- **Automating repetitive tasks:** Automate routine tasks such as log analysis, threat detection and incident response to allow security analysts to focus on more complex and critical issues, improving overall efficiency
- **Enhanced threat detection:** By analysing vast amounts of security data to identify patterns and anomalies that might indicate a security threat
- **Dynamic incident response:** Assisting in creating dynamic and adaptive incident response plans based on the nature of the threat and historical data, so the security engineers just need to adapt and improve it
- **Threat hunting:** By continuously scanning for potential vulnerabilities and threats, even before they are exploited
- **Improved decision making:** By providing real-time insights and recommendations, SOC can make informed decisions more quickly, which is crucial in mitigating the impact of incidents
- **Integration with security platforms:** Integrate the GenAI capabilities in the existing security platforms which results in more accurate and timely alerts

While GenAI offers many benefits, it also introduces new challenges, such as the potential for attackers to use the same technology to enhance their capabilities. Therefore, using GenAI seems to become more and more essential to just even the playing field.

Proactive threat discovery with GenAI (I)

When looking at the benefits of GenAI that may enhance the processes within the SOC of a CSP, proactive threat discovery is one area where GenAI can offer several benefits. The first benefit is the use in real-time analysis. GenAI can process vast amounts of data in real-time, identifying potential threats as they occur and this immediate analysis allows for swift detection and response by the SOC team, minimising the window of opportunity for attackers.

Secondly, it can enhance anomaly detection by using machine learning algorithms. Establishing a baseline of normal network behaviour may empower GenAI to detect deviations that may indicate malicious activity, and this helps in identifying unknown threats that traditional signature-based systems might miss. And when we look again at inter-roaming threats, especially at malicious location tracking, the attackers exploit essential functionalities needed to locate the mobile device so a call can be established. Therefore, to distinguish the legitimate from the malicious traffic can be difficult and GenAI might support the security analysts in detecting such threats. Since GenAI continuously learns from new data, its ability to detect and respond to emerging threats is improving over time. This adaptive capability ensures that the system remains effective against evolving attack vectors.

The third benefit is using GenAI to automate response actions, such as isolating affected systems or blocking malicious traffic, so a further enhancement of the speed and effectiveness of threat mitigation is possible. And since GenAI offers adaptive learning capabilities, it also offers the possibility for an automated playbook generation of how to mitigate the identified threats and vulnerabilities. The security engineers would just have to review and, if needed, adapt the proposed solution, which would allow them to focus on more complex and critical issues, thereby improving resource utilisation as well as overall efficiency.

A fourth benefit GenAI can offer is to significantly enhance the integration with external threat intelligence sources. GenAI can automatically collect and aggregate data from multiple threat intelligence feeds, ensuring a comprehensive view of the threat landscape. This helps in identifying patterns and correlations that might be missed when analysing data from a single source. It can normalise data from different formats and enrich it with additional context, making it easier to analyse and act upon, which ensures that the threat intelligence is consistent and actionable. This also may further enhance threat hunting to proactively detect potential vulnerabilities and threats in their mobile network before they are exploited by malicious actors.

In addition, GenAI can automate the integration of threat intelligence with security systems, such as firewalls, intrusion detection prevention systems and so on. This enables automated responses to detected threats, reducing the time and effort required for manual intervention by the SOC team. And of course, the integrated threat intelligence data can be used as additional input for the continuous learning capability of GenAI.

Proactive threat discovery with GenAI (II)

Proactive threat detection, especially when enhanced by GenAI, can significantly reduce dwell time — the period between an initial breach and its detection — by continuously monitor network traffic and analyse vast amounts of data in real-time. And since GenAI excels at recognising complex patterns and correlations that might be missed by traditional systems, it can identify subtle indicators of compromise. This allows for the immediate identification of anomalies and potential threats earlier in the attack lifecycle, reducing the time attackers can remain undetected. And by automating the process of threat hunting the reliance on manual efforts by the SOC team can be reduced. In addition, employing GenAI in formulating and executing a rapid response, including isolating affected systems, mitigating the threat, and initiating recovery processes can help minimise dwell time. Integration of GenAI with the existing security platforms to enhance their capabilities, may reduce the needed effort by the SOC team and streamline the threat mitigation. This integration ensures a more cohesive and efficient threat detection and response strategy to reduce dwell time, limiting the window of opportunity for attackers and minimising potential damage. All these benefits of GenAI can directly impact the limitations of reactive security measures and further improve the several significant benefits for organisations offered by proactive threat discovery[9].

Benefits of Gen AI in Proactive Threat Discovery

Proactive Threat Detection and Analysis Allows to minimise the amount of data compromised and reduce the overall impact of threads by early detection and predictive analytics

Financial Benefits Early detection helps avoid the costly aftermath of an attack, both in terms of financial loss associated with data breaches, including recovery expenses and potential regulatory fines as well as and time required to restore systems and data

Operational Continuity and Improvements Maintaining business operations by preventing disruptions caused by cyberattacks as well as freeing up resources by automated incident responses to further improve and strengthen cybersecurity

Improved Security Posture and Enhanced Risk and Vulnerability Management Predictive analytics, automated response and playbook generation as well as the possibility to automatically simulate and test these scenarios will strengthen cybersecurity and freeing up resources to further enhance security

Regulatory Compliance Preventing attacks by proactive threat detection and predictive analytics will minimise regulatory interference, protect the organisation's reputation and maintain the customer's trust

Emerging Threats Continuous learning capabilities of GenAI lead to effectiveness enhancements over time, constantly identifying and adapting to new threat patterns, evolving its detection and response strategies and increase the detection rate of new or sophisticated attacks that would otherwise go undetected

[9] https://arxiv.org/abs/2403.08701

Proactive threat discovery with Nokia NetGuard Cybersecurity Dome's GenAI- enabled Hunt Assistant

Modern threat incident management platforms reflect the need for a balanced approach combining proactive threat detection and reactive security measures as well as using automation to employ a robust cybersecurity strategy. One prime example of such a platform is Nokia's NetGuard Cybersecurity Dome, a security orchestration software suite with several pre-built 5G use cases for telecommunications service providers and critical infrastructure enterprises. It offers visibility across various networks, cloud infrastructure and endpoints and unifies security control points, offers security telemetry and provides analytics and operations in a single view8. The suite was recently augmented with the GenAI-enabled Hunt Assistant, which provides AI-generated benefits for threat detection and may help minimise and mitigate the risks of incidents, including inter-roaming attacks..

Let us see how this could translate in the real world and the processes in the SOC of a CSP: A large telecoms service provider has recently implemented Nokia's NetGuard Cybersecurity Dome with the new GenAI-enabled Hunt Assistant. The security team is tasked with proactively identifying potential threats in their telco network infrastructure before they can cause harm. Here are the different steps that the Hunt Assistant and the SOC team goes through in this endeavor.

Threat intelligence ingestion
The integrated GenAI-powered Threat Hunt Assistant automatically ingests the latest threat intelligence feeds, such as signalling threat intelligence information, with vast amounts of telemetry data from the service provider's telecom network and maps it to potential tactics, techniques, and procedures (TTPs) that could be used in the telecoms network. The integration with MITRE ATT&CK and MITRE FiGHT models enhances the understanding of telecom-specific threats.

Potential threat identification
The Hunt Assistant identifies suspicious activity in a segment of the network that aligns with the behavior of the new suspicious unstable profile. It generates a detailed report of its findings, including the specific data points that triggered the alert.

Human validation
A senior security analyst validates the AI-generated hypothesis based on logical facts and findings and triggers the next step.

Automated use-case generation
Based on the validated threat hypothesis, theHunt Assistant utilises its large language model (LLM) capabilities to automatically generate a new security use-case artifact. This includes detection rules, response procedures and mitigation strategies specifically tailored to the telecoms service provider's network architecture.

Testing and deployment
The generated security use-case is tested in a dynamic simulated environment to ensure its effectiveness and to avoid potential false positives. Once validated, it is deployed across the telecoms service provider's network.

This scenario demonstrates how Nokia's solution uses Gen AI technology to transform threat intelligence into actionable security measures, enabling telecoms service providers to stay ahead of emerging threats in an increasingly complex cybersecurity landscape. The entire process, from threat intelligence ingestion to deployment of a new security use-case is completed in a matter of hours rather than days or weeks, significantly enhancing the telecoms service provider's security posture.

Proactive threat discovery with Nokia NetGuard Cybersecurity Dome's GenAI- enabled Hunt Assistant

Benefits and value proposition

The implementation of Nokia's NetGuard Cybersecurity Dome has provided the telecom service provider with numerous advantages, significantly enhancing itsoverall security posture and operational efficiency. The entire process, from threat intelligence ingestion to deployment of a new security use-case, is completed in a matter of hours rather than days or weeks.

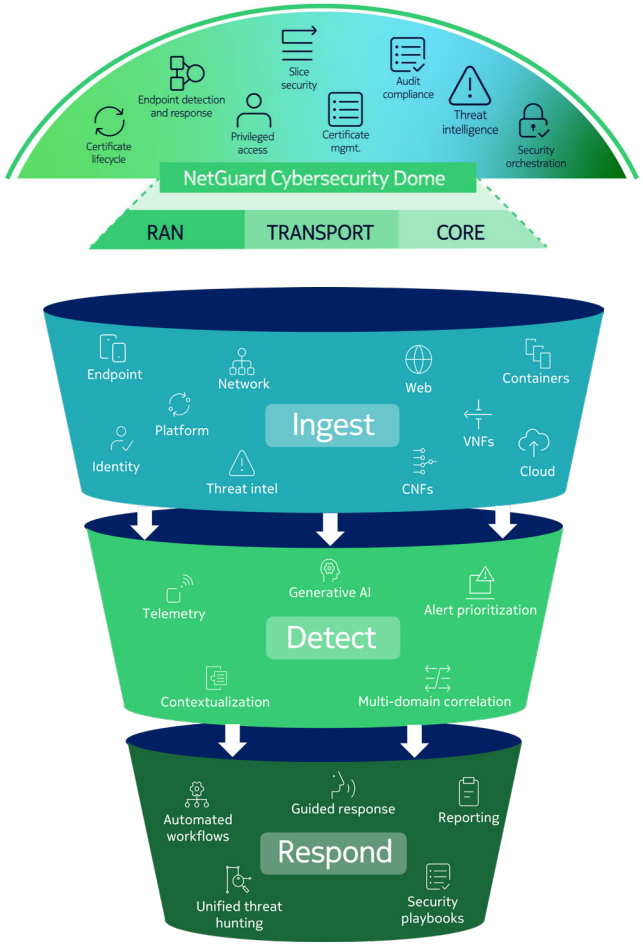
Integrated threat management: By integrating with SIEM, SOAR and UEBA systems, NetGuard Cybersecurity Dome provides a unified view of threats and alerts, enabling coordinated responses across the entire environment. This integration utilises real-time threat intelligence, endpoint and network-based sensors to effectively prevent, detect, identify and investigate threats.

Tailored for telco and mission-critical use cases: NetGuard Cybersecurity Dome is specifically designed to address telco-centric and mission-critical scenarios, protecting critical network functions while adhering to global and local telecommunications regulations.

AI-driven detection and response: Using AI and automation, NetGuard enhances the detection and response process with automated workflows for remediation. Nokia's investment in a telco-centric GenAI, SaaS hosted on Microsoft Azure, ensures top-tier support for security analysts. The GenAI assistant tool offers summarisation, proactive threat analysis, guided resolution and automated reporting, streamlining security operations.

By utilising advanced threat intelligence and GenAI-powered threat hunting, the telecoms service provider was able to stay ahead of emerging threats in an increasingly complex cybersecurity landscape, reducing the data breach gap by up to 80%.

Figure 1: Solution Overview – NetGuard Cybersecurity Dome



Industry collaboration for enhanced security

Importance of collaboration

With the interconnected mobile networks infrastructure, where an attack in a way easily threatens the whole industry, industry collaboration is crucial for various reasons, especially when it comes to enhanced security. By sharing threat intelligence, best practices and fostering transparency, MNOs can gain a broader understanding of potential threats and use this collective knowledge in identifying and mitigating risks more effectively. Plus, pooling resources and expertise to find solutions or mitigations of potential threats can result in enhanced problem solving by bringing together diverse perspectives and expertise, leading to more innovative and effective solutions that require a smaller investment per organisation. Another aspect can be, that collaboration allows for a faster incident response, because collaborative efforts enable quicker communication and coordination during incidents, which may result in faster detection, response and recovery, minimising the impact of attacks. Enhanced policy development can also be a benefit of collaboration between various stakeholders, including industry, academia and regulatory bodies, because collaboration helps in developing comprehensive and effective security policies and standards.

Impact of collaboration on mitigating inter-roaming attacks

Since inter-roaming attacks are cyber threats that exploit the roaming agreements between different network operators and are based on exchanging control information between two mobile networks, collaboration is essential to mitigate and prevent the incidents. By sharing threat intelligence, network operators can stay informed about the latest attack vectors and tactics used by cybercriminals, which helps in identifying and mitigating those threats more effectively. Collaboration also enables a coordinated response to inter-roaming attacks, because cooperating MNOs can quickly isolate and neutralise threats, minimising the impact on networks and customers. Also, collaboration can lead to the development of advanced monitoring and detection systems capable of identifying suspicious activities across different networks. Collaboratively developing and adhering to standardised security protocols across different networks ensures a consistent level of protection. This reduces the chances of vulnerabilities being exploited during roaming. And since inter-roaming attacks often involve multiple jurisdictions, the international cooperation between regulatory bodies, law enforcement and MNOs is essential for tracking and prosecuting cybercriminals.

By fostering a collaborative environment for enhanced security in the mobile network industry, organisations can build a more resilient and secure infrastructure, better equipped to handle the evolving threat landscape.

Further enhancing proactive and reactive security measures with GenAI

As mentioned before, balancing proactive threat detection and reactive security measures is crucial for a robust cybersecurity strategy and additionally using automation to efficiently and effectively mitigate security breaches can further enhance cybersecurity10. By additionally employing the capabilities of GenAI these measures can be further enhanced.

Sophisticated breach / attack simulations employing GenAI

The new possibilities generated by GenAI even allow launch of sophisticated breach and attack simulations and that may provide ongoing assessments of an organisation's security posture by simulating real-world cyberattacks. This continuous testing may help identify vulnerabilities and weaknesses in defenses before they can be exploited and allow the SOC to identify and prioritise vulnerabilities based on their potential impact, which enables the CSPs to allocate resources more effectively and this targeted approach ensures that the most critical risks are addressed first. These simulations will also allow testing of the reactive security measures offered by the IDS/IPS and enhance them. Simulating a wide range of attack vectors in realistic scenarios ensures that defences are functioning as intended and highlights areas that need improvement. And simulating these attacks may help SOC teams understand how attackers might exploit their systems and prepare accordingly and even refine their security team's incident response plans by providing insights into how attacks unfold. So, security teams can practice and improve their response strategies, leading to quicker and more effective mitigation of real incidents.

Improving automation with GenAI

By utilising the capabilities of GenAI we have mentioned before, automation benefits can be further enhanced.

- Continuous real-time surveillance for early detection of anomalies
- Automated incident response
- Integration of threat intelligence feeds
- Automated vulnerability scans and patching
- Generating compliance reports and audit logs

Probably the biggest impact will be improvements to the incidence response by GenAI-driven decisions and suggestions. These will support the SOC teams of CSP in choosing the right strategy to mitigate the incident. GenAI can also help automating the response by use case and playbook creation and documentation of incidents for further uses, for example to automatically post them in threat intelligence feeds.

Plus, GenAI offers here the opportunity for continuous improvement through feedback loops and incorporating the vast amount of data it can access, like intelligence threats and the real-time monitoring of the CSP's (mobile) network.

Conclusion

The way to go forward is a balanced approach combining proactive threat detection and reactive security measures as well as using automation to employ a robust cybersecurity strategy. This approach helps organisations maintain resilience against evolving threats while ensuring they can respond swiftly and effectively when incidents do occur.

But in today's interconnected mobile network landscape, besides a balanced approach combining proactive threat detection and reactive security measures, it is also essential to foster industry collaboration to enable CSPs to build a more resilient and secure infrastructure, better equipped to handle the evolving threat landscape. And the emerging and evolving of GenAI will offer the opportunity to further strengthen cybersecurity by enhancing the possibilities of proactive threat detection and reactive security measures as well as supporting an intensified industry collaboration by automatically implementing threat intelligence and industry best practices.