Case Study

Enhancing telco security with proactive threat exposure management

NOKIA

In the fast-evolving telecoms industry, cyber threats pose significant risks to network integrity and business continuity.

Reactive security measures are increasingly inadequate against these sophisticated threats. Consequently, it needs a proactive security to mitigate potential attacks, to embrace self-learning defense technologies and to enhance threat hunting capabilities. These technologies can autonomously adapt to the evolving tactics of malicious actors, while threat hunting actively seeks out and identifies hidden and potential threats.

To address this challenge, Nokia has taken incremental steps towards autonomous network capabilities by enhancing telco security with the upgraded **NetGuard Cybersecurity Dome**, a telco-centric **Extended Detection and Response (XDR)** solution powered by generative AI. This case study explores how a large telecoms service provider utilized Nokia's NetGuard Cybersecurity Dome to enhance their security posture through proactive threat hunting and advanced threat intelligence.

Background

The telecom service provider operates a complex telco cloud-native network infrastructure, providing critical communication services to millions of users. The service provider faced numerous challenges in maintaining network security, including outdated security protocols, limited expertise in signaling security, and the need to protect against inter-roaming attacks.

Recognizing the limitations of traditional IT security methods, the telecom service provider sought a comprehensive solution that could proactively identify and mitigate threats before they could cause harm the Operational Technology (OT) network infrastructure.

Solution: Nokia NetGuard Cybersecurity Dome

Nokia's NetGuard Cybersecurity Dome offered a holistic approach to telco security, integrating advanced telco threat intelligence, real-time monitoring, and predictive analytics. The solution is designed to protect mission-critical infrastructure by proactively discovering potential vulnerabilities and optimizing security posture across various telco environments such as Radio Access Network (RAN), Transport and Core.

Key components of Nokia's telco-centric XDR solution include a GenAI-powered assistant for threat hunters and SOC analyst teams, which provides autonomous threat detection and response capabilities.

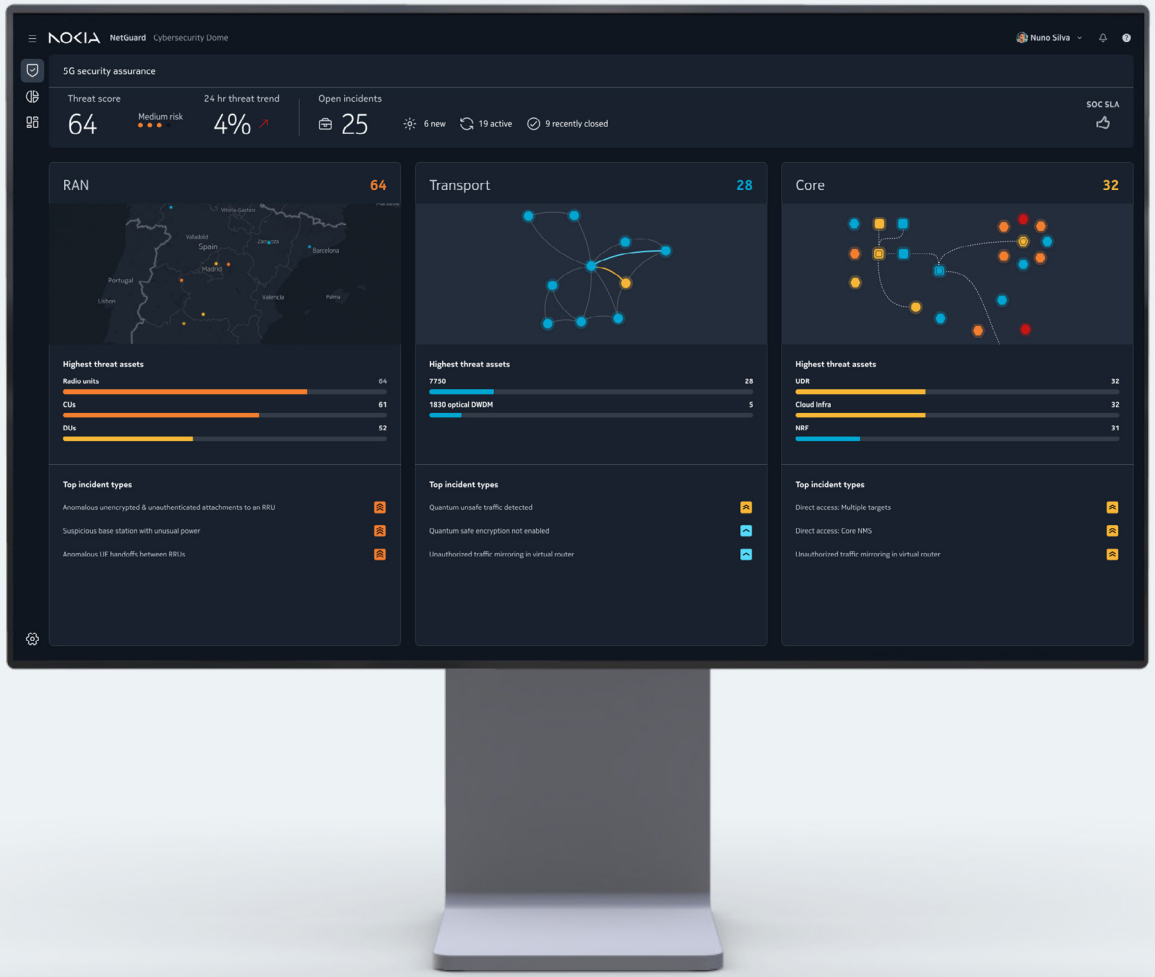


Figure: Dashboard view – NetGuard Cybersecurity Dome

Structured threat discovery

To effectively deploy automated threat hunting, the service provider took advantage of the structured threat discovery process with automated threat hunt assistance. The following steps outline the flow of a structured threat discovery:

Threat Intelligence Ingestion

The integrated GenAI-powered Threat Hunt Assistant automatically ingests the latest threat intelligence feeds (e.g. signaling 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 telecom network. The integration with MITRE ATT&CK and MITRE FiGHT models enhances the understanding of telecom-specific threats.

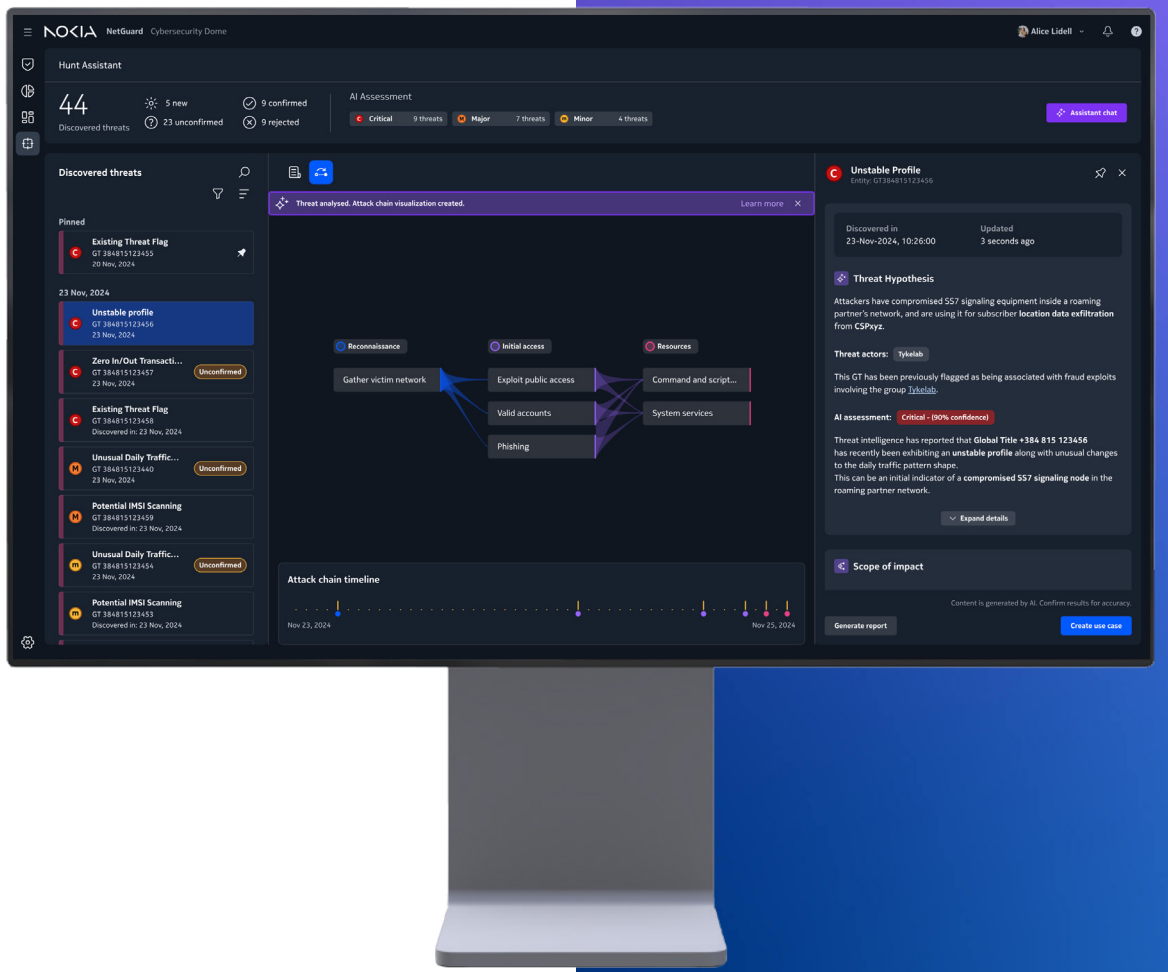


Figure: Threat Hunt Assistant with threat hypothesis – NetGuard Cybersecurity Dome (demo view)

Potential Threat Identification

The Hunt Assistant identifies suspicious activity in a segment of the network that aligns with the behavior of the new suspicious profile. It generates a detailed hunt hypothesis report of its findings, including 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, the Hunt Assistant utilizes 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 telecom 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 telecom service provider's network.

Benefits and value proposition

The implementation of Nokia's NetGuard Cybersecurity Dome has provided the telecom service provider with numerous advantages, significantly enhancing their overall 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 multi-vendor environment. This integration leverages 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 telecommunication regulations.

AI-Driven Detection and Response

Leveraging AI and automation, NetGuard Cybersecurity Dome enhances the detection and response process with automated workflows for remediation. Nokia's investment in a telco-centric GenAI, ensures top-tier support for security analysts. The GenAI assistant tool offers summarization, proactive threat analysis, guided resolution, and automated reporting, streamlining security operations.

By leveraging advanced threat intelligence and GenAI-powered threat hunting, the telecom service provider was able to stay ahead of emerging threats.

Key benefits include:

60%
reduction of analyst workload

40%
reduction in mean time to detect

Summary

Thanks to the proactive threat discovery capabilities of Nokia's NetGuard Cybersecurity Dome and its GenAI-enabled Assistant, the telecom service provider successfully identified and mitigated potential threats before they could cause any damage to their network. The solution's comprehensive visibility, integrated threat management, and AI-driven detection and response capabilities significantly enhanced the telecom service provider's security posture.

This case study demonstrated the value proposition of Nokia's NetGuard Cybersecurity Dome in transforming threat intelligence into actionable security measures, enabling telecom providers to maintain continuous business operations and protect their critical infrastructure.

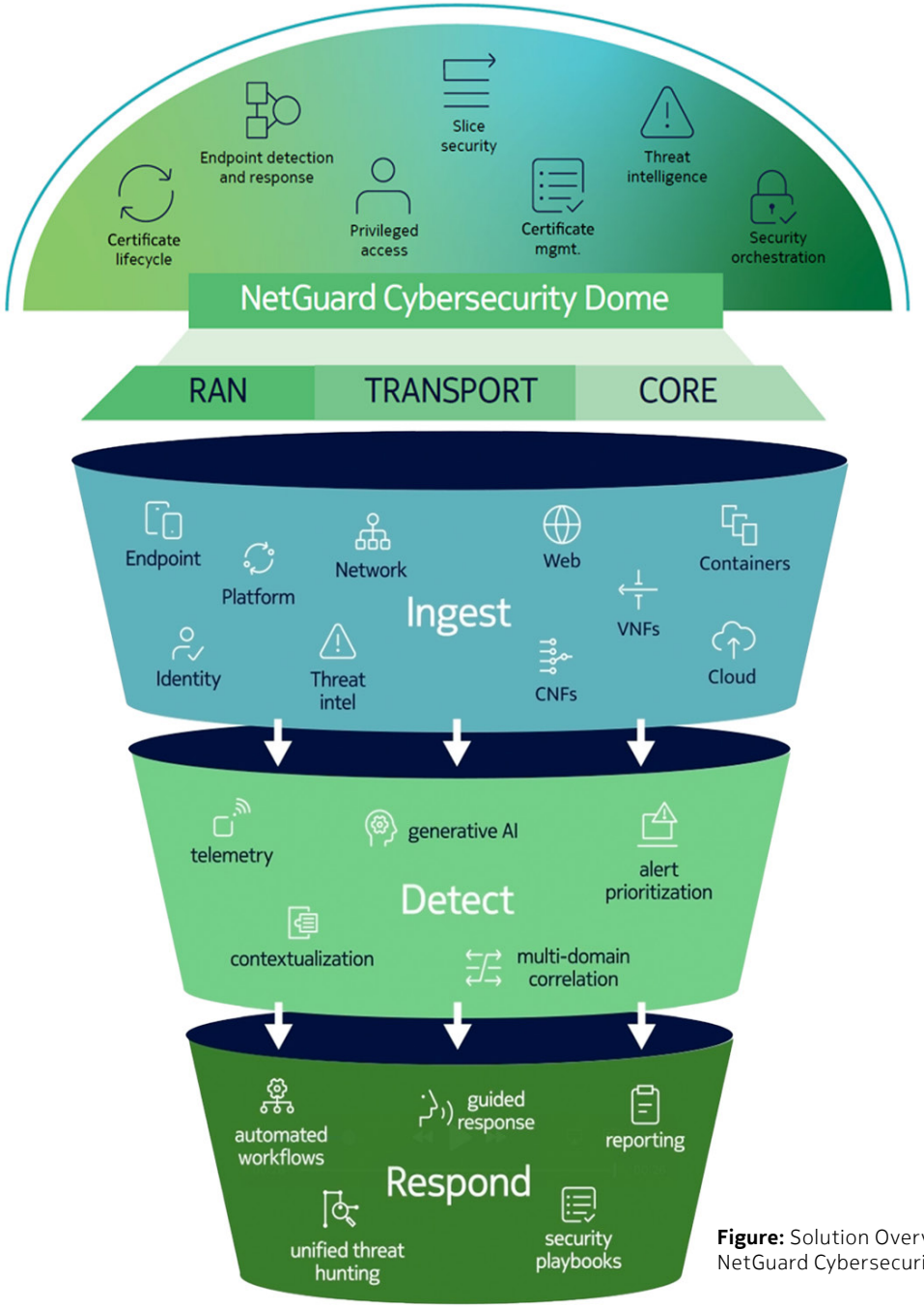


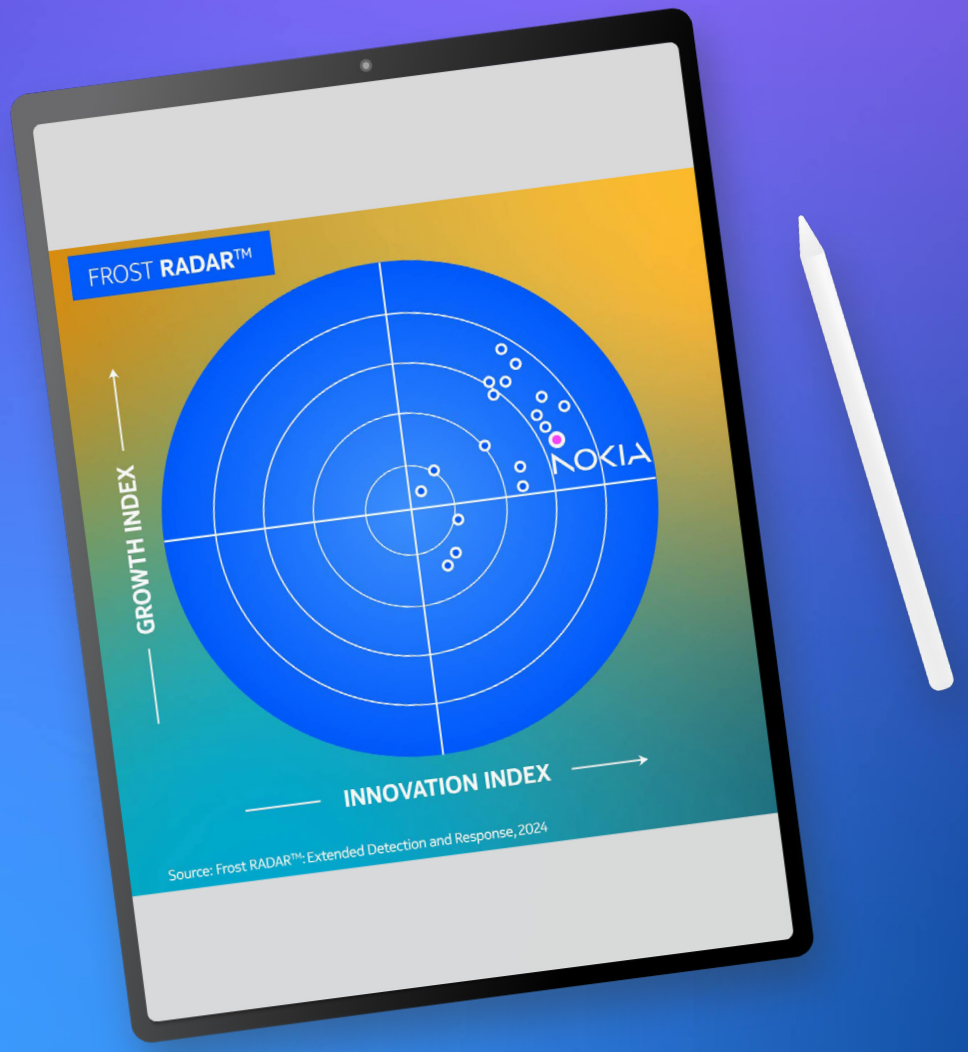
Figure: Solution Overview – NetGuard Cybersecurity Dome

The leader in telco network security

Nokia NetGuard Cybersecurity Dome sets the benchmark for telco network security, backed by our deep industry expertise. Recognized by GigaOm as a leader in the XDR market, NetGuard Cybersecurity Dome integrates advanced threat intelligence, AI, and automation to defend critical infrastructures and enhance SOC operations.

Our solution provides robust, real-time insights while streamlining operations through intelligent automation. By minimizing manual tasks and reducing response times, NetGuard empowers CSPs and mission-critical businesses to manage threats effectively, reducing the overall cost and impact of security events. With Nokia NetGuard Cybersecurity Dome, organizations gain a flexible, adaptive security framework that ensures resilience in an ever-evolving threat landscape.

Visit our website or contact us today to learn more about Nokia Cybersecurity Dome.



Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214683

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.