Security Operations with GenAI

Florian Damas
Head of Network and Innovation Policy

15 May 2024

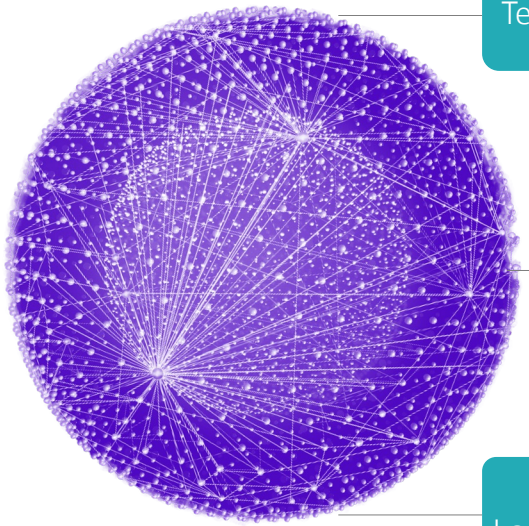
Two worlds of security: IT & Telecom

Identifying distinctive features & challenges

IT security	Telecom network security
What's top of mind – security priorities	
Avoid data thefts, ransomware, PII, etc.	Operational continuity of voice/data networks.
Components	
Industry agnostic such as laptops, Mobile Devices, Intranet, IT application and data center	Purpose-built networks such as Core, RAN, Transport, Access Network, OSS/ BSS
Infrastructure & protocols	
Standard protocols like TCP/IP and TLS	Multi-vendor legacy technologies mixed with latest cloud-based SBA and telco protocols like SS7, Diameter, GTP
Skill sets	
Skills in endpoint security [mobile, desktop servers], app security, firewalls, and secure gateways.	Expertise in telco network topology, communication protocols, attack scenarios for SBA, NE integrations to collect telemetry data and take actions.
Tools and technology	
Homogenous security tools like IT SIEM, IAM, EDR, and laptop antivirus.	Specialized tools like telco XDR, mission critical EDR, telco PAM, cloud-native architecture
Regulatory landscape	
Governed by standards like HIPAA, PCI, and GDPR	Abides by 3GPP, GSMA, and country specific regulations such as NSA and EO in US, TSA in the UK, NIS2 in Europe

© 2024 Nokia

Key trends



Telco network security	Increased attack surface continues to be the biggest driver IT focused security applications are not adequate
Post Quantum security	Several concerns, including “Harvest Now, Decrypt Later”
GenAI and Large Language Models (LLM)	The arms race between Good and Bad usage of AI

© 2024 Nokia

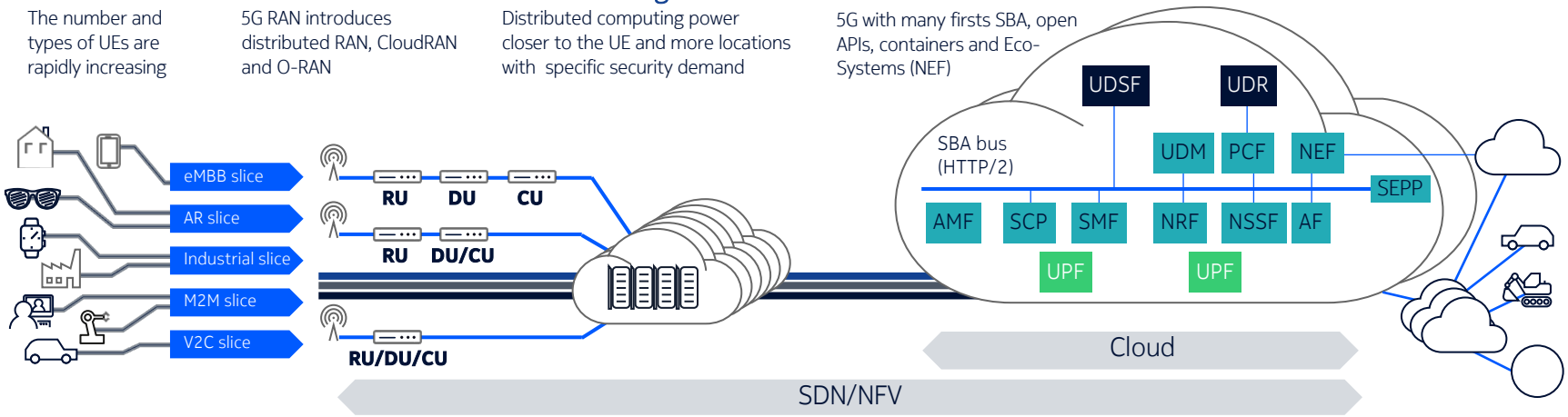
5G network architecture introduces fundamental new challenges in security

UE
The number and types of UEs are rapidly increasing

5G radio
5G RAN introduces distributed RAN, CloudRAN and O-RAN

Edge
Distributed computing power closer to the UE and more locations with specific security demand

5G core
5G with many firsts SBA, open APIs, containers and Eco-Systems (NEF)



THREATS

- UE compromised
- Signaling storms
- Malicious SW
- Bot hijacking

- Man-in-the-middle attack
- Configuration hacks
- IP-Spoofing
- Scanning attacks

- Distributed architecture raises number of entry point!
- Hijacking attacks
- TCP level attacks

- Service-based architecture and slice resource sharing increases security complexity!
- DoS attack on signaling plane
- User identity theft
- Active/passive eavesdropping
- Capability exposure API attack

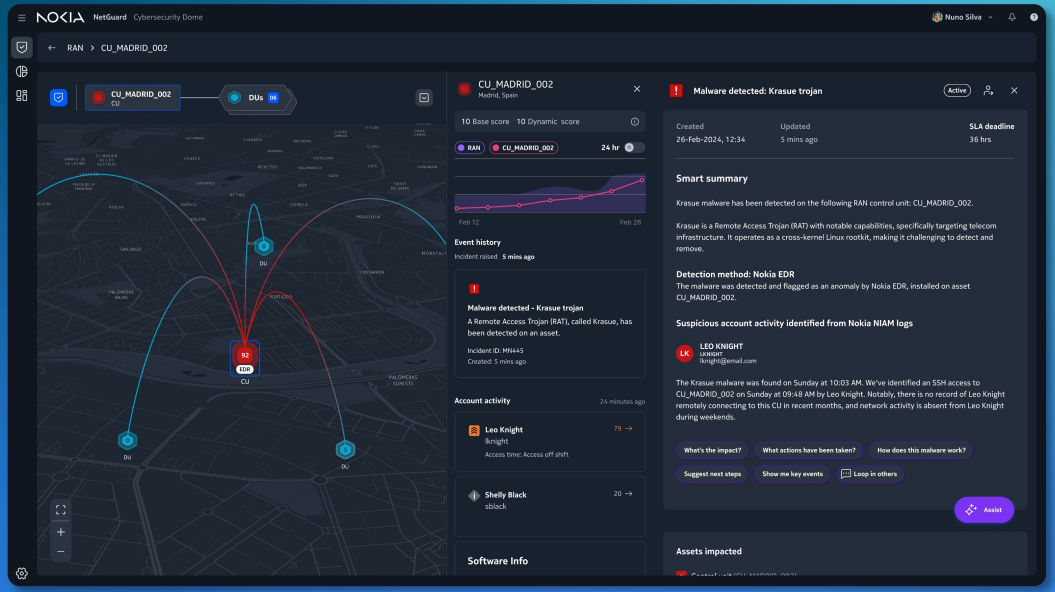
RESPONSE

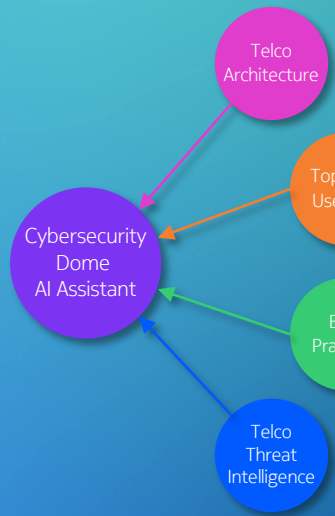
- Cross domain
- Cross vendor
- Operations/automation
- SLA dependent charging
- Orchestration
- …

© 2024 Nokia

Cybersecurity Dome AI Assistant

Specialized LLM for Telco Cybersecurity Operations





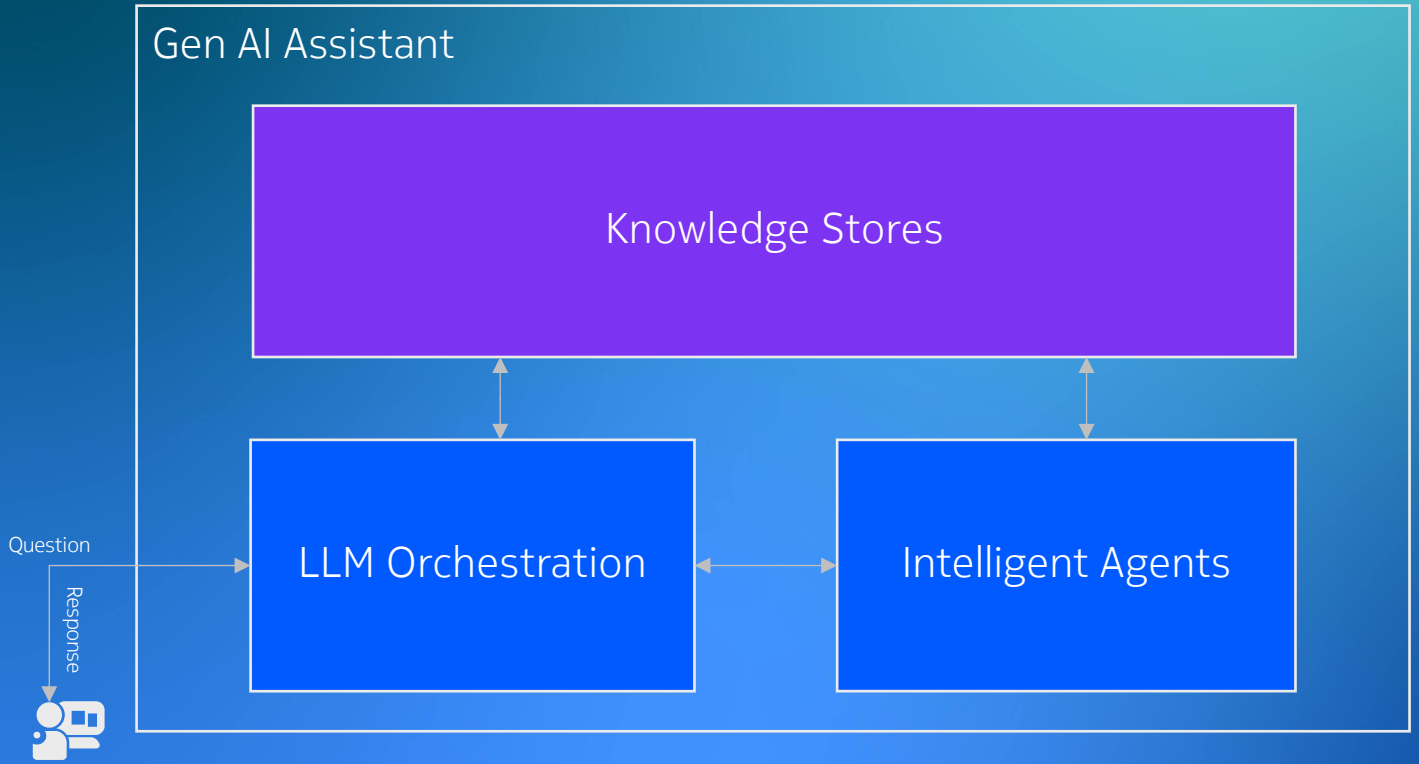
- 3GPP Core, RAN, Transport specs
- Cloud Infra, Security Controls
- Cybersecurity Dome
- 3GPP, NIST
- Nokia recommendations
- MITRE FiGHT
- Bhadra (Bell Labs)

AI Assistant Features

- Smart Summary
- IoC / IoA Analysis
- Chat: Guided Resolution
- Chat: Report Generation

© 2024 Nokia

High Level Architecture



Gen AI Assistant uses a RAG (Retrieval Augmented Generation) model

Intelligent Agents provide Telco-context knowledge to the Assistant from a variety of both static and dynamic data sources

An LLM orchestration block allows the original user prompt to be augmented and refined to the final response

Strict data isolation ensures that data from a particular tenant is never used to improve the LLM itself or leak to other tenants

© 2024 Nokia

Sample journey for a SOC analyst

A prompt–based user experience with NCYD Gen AI Assistant

Start

Prepare

- What is my latest high priority incident?
- Is this related to other incidents I worked on?
- Who else has worked on similar incidents?

Learn

Understand problem

- What 5G services are affected? (AMF)
- Explain to me the role of the AMF
- Show me the Alerts history and MITRE mapping
- Show me the perimeter defenses (firewalls)
- Who are the internal users involved?
- Is there a data exfiltration concern?
- What are the suggested responses?

Decide

Choose response

- Show me the success rate for response X
- Show me the workflow for response X
- What approvals are needed for response X?
- Is there any downtime required for path X?

Act

Resolve issue

- Execute response X
- If approval was denied in Step Y, what was the reason?
- If failed, what was the reason for failure?
- If failed, what is the next best option?
- Start a Teams session with another analyst (collaborate)
- Repeat until resolved

End

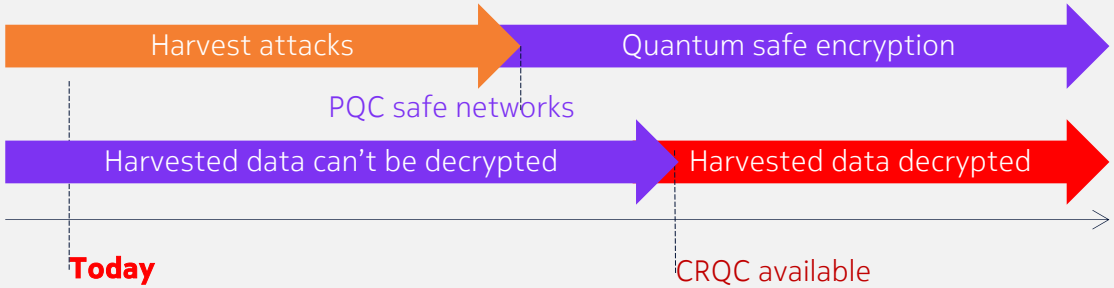
Report

- Generate an Incident report PPT and mail it to my supervisor
- Resolve the incident with my comments

© 2024 Nokia

Post Quantum Security

Harvest now, decrypt later threat



Harvest Now, Decrypt Later

Store sensitive data with the goal to decrypt when quantum computers are available

Rewriting History

Compromise the integrity of digitally signed data e.g contracts

Code-Signing and Digital Signatures

Compromise service authentication leading to vulnerabilities in software updates

Key Management Attacks

Long-term data storage can be vulnerable by attacking key management

GSMA

The transition to Post-Quantum Cryptography has started

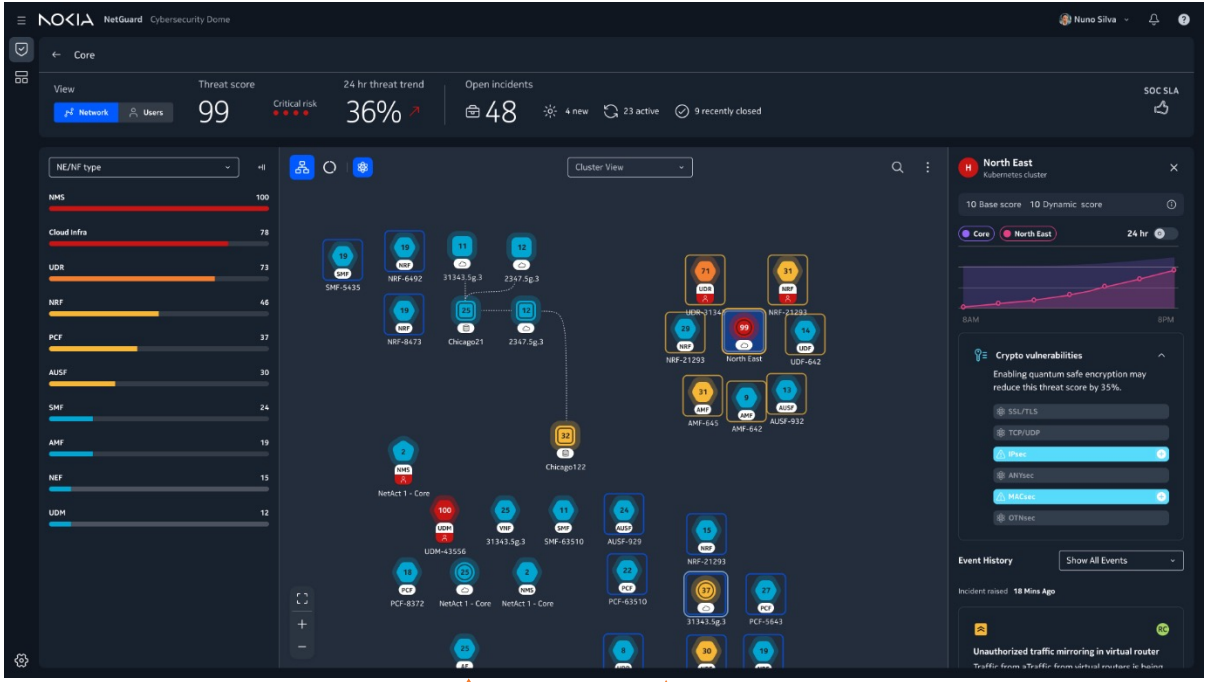
Quantum Computing has great potential, but also brings business risk with far reaching consequences on telco networks and customers. Governments have begun planning and issuing guidance to mitigate these risks.

How can operators prepare?

- Establish a *cryptographic inventory*: understand where cryptographic algorithms are used in systems or vendor products
- Plan a cryptography risk assessment
- Develop expertise in Post-Quantum Cryptography and security
- Support standardisation & open-source
- Support related research.
- Engage with customers and vendors for requirements
- Develop a Post-Quantum Cryptography transition plan

NOKIA

Quantum safe network topology



Topology views for network, network admin, connectivity link and vulnerabilities

Quantum unsafe paths are highlighted over the topology map

Ensure quantum secure connections

- Cyberdome delineates the transport topology and its associated connections, distinguishing between those that already provide quantum security and those that do not.
- Cyberdome will propose upcoming routes to attain quantum security

Security of optical links

- Cyberdome will oversee connection links and issue alerts for potential security breaches, including:
  - Mechanical disturbances
  - Optical anomalies
  - Fiber oscillations/vibrations

© 2024 Nokia


NOKIA