

NOKIA

5G Security

Intelligent
Threat Detection and Response

Intelligent Threat Detection and Response

A network security twin

...monitors, detects and manages with eXtended Detection and Response (XDR) to build trust in 5G services

- **Detection & Response**
for endpoints, cloud and network
- **Intelligence & Analytics**
threat intel, intelligent analytics
- **Automation & Orchestration**
to reduce incident response time



Addressing the increasing risks while keeping critical services running

Nokia XDR Security

Unifying Endpoint, SecOps and Data Protection for telco cloud Security

1. Visibility across networks, cloud infrastructure and endpoints
2. Integrates multiple security tools and security information
3. Artificial intelligence to speed up the detection of new threats
4. Threat intelligence to bring the context
5. Automated response to offload security analysts

-NetGuard-

Cybersecurity Dome

Tool integration

Threat intelligence

Security analytics

Auto-response



Privileged
access and
identity



IoT & end-
device
security



PKI and
lifecycle
management



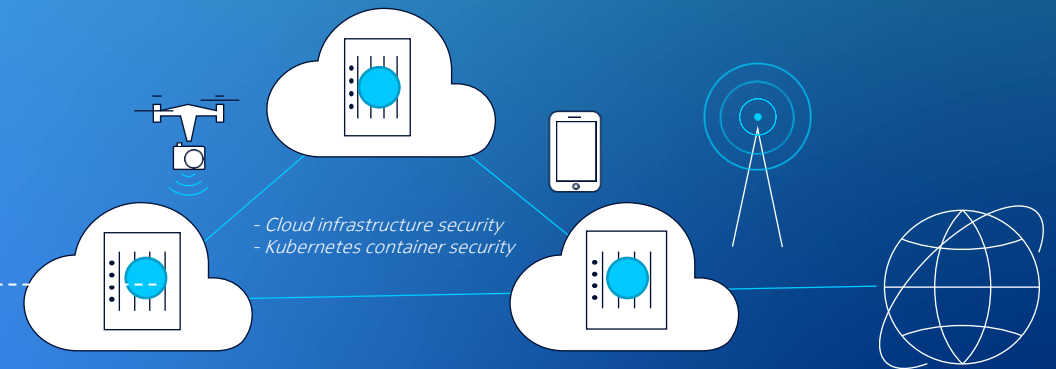
Automated audit
compliance
security



Endpoint
Detection and
Response (EDR)

Why EDR helps to build trust:

- Detects malware, rootkits and entity anomalies
- Threat hunting with AI/ML analysis and auto-response



Intelligent analytics to identify insider threats

TOPOLOGY

causes all incidents raised and mapped to a network element for contextual awareness

5G SECURITY USE CASES

catalogue of 5G specific use cases off the shelf

THREAT SCORING

measures the probability that an element is under attack

BEHAVIOUR ANALYTICS

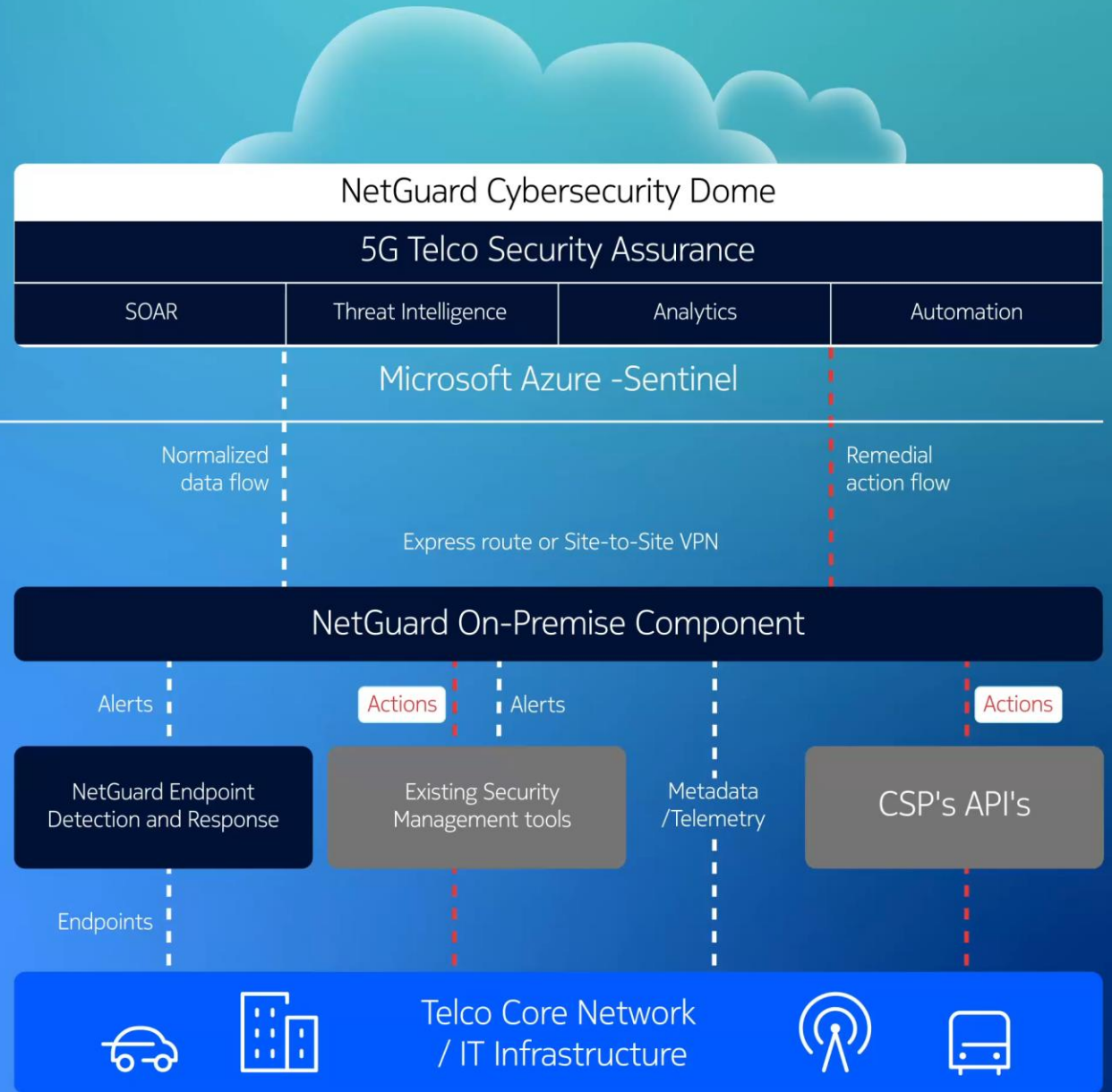
User and entity behavior analytics to detect attempts of compromising user, functions or services.



Threat detection and response with intelligent 5G security



NetGuard Cybersecurity Dome
SaaS Cloud Instance



Monitor, detect and manage

Key criteria to select the right XDR solution



Detection & Integration

Signature and anomaly-based detection to protect endpoints, cloud and networks

Analytics & Intelligence

Threat intel, user, entity behaviour analytics to expand visibility and efficiency

Automation & Orchestration

Orchestration of automated workflows to reduce incident response time

Protect network data and business continuity

AI driven security orchestration across network, cloud and endpoints



Certificate mgmt.	T Mobile	>100K certificates managed
Threat Intelligence	NOKIA	120K daily malware samples collected
Audit compliance	STARHUB	35% more efficient SecOps
Privileged access	airtel	>10.000 network elements
Endpoint security	Zain	80% faster detection of issues

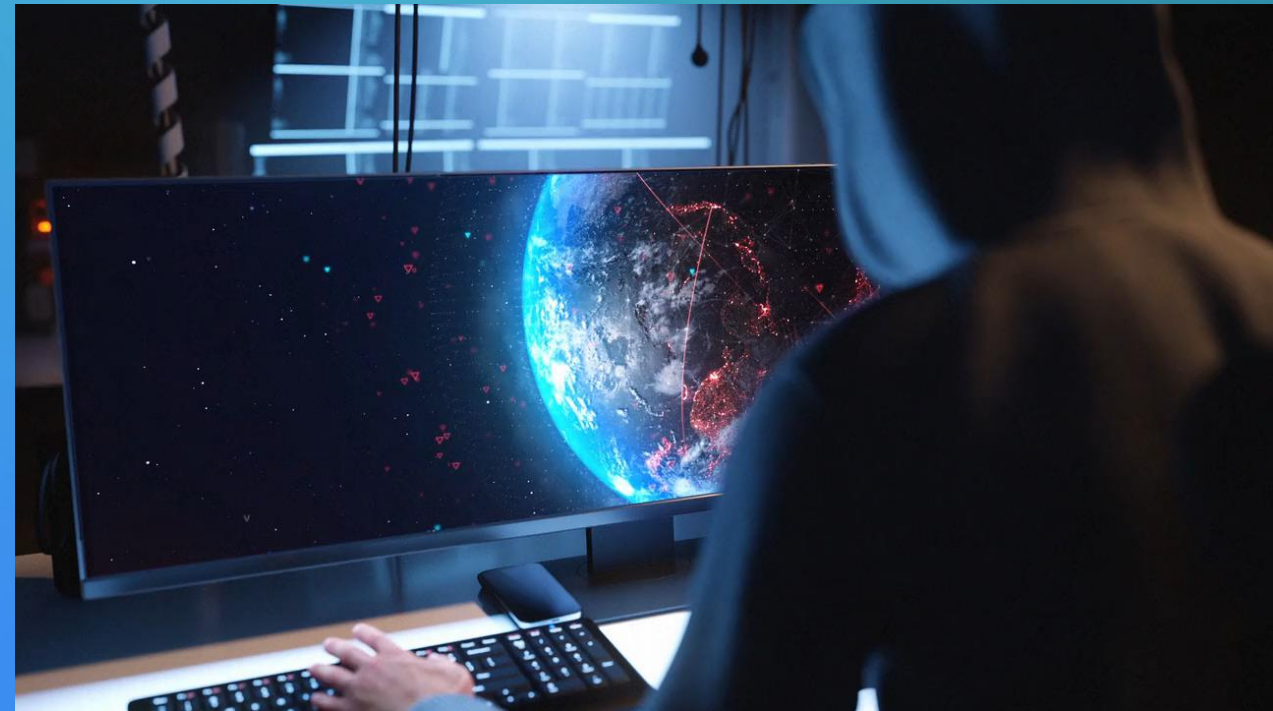
Threat Use Case – Compromised Insider attack

Nokia will demonstrate latest XDR (extended detection and response) capabilities for 5G security to secure the full scope of 5G use cases.

- Our comprehensive single platform NetGuard Cybersecurity Dome offers extended threat detection and response (XDR) capabilities, sensor-based endpoint security, and automated threat score calculation to mitigate threats in 5G networks.

In this demo, gain a deeper understanding for how you can protect your critical infrastructure when a compromised insider tries to attack a cloud-native 5G core network.

- Our use case demonstrates how Nokia's new NetGuard Endpoint Detection and Response (EDR) interlocks with NetGuard Cybersecurity Dome to detect and respond to risky and abnormal user and entity behaviors in the management interface of a cloud-native 5G Core network element.



NOKIA