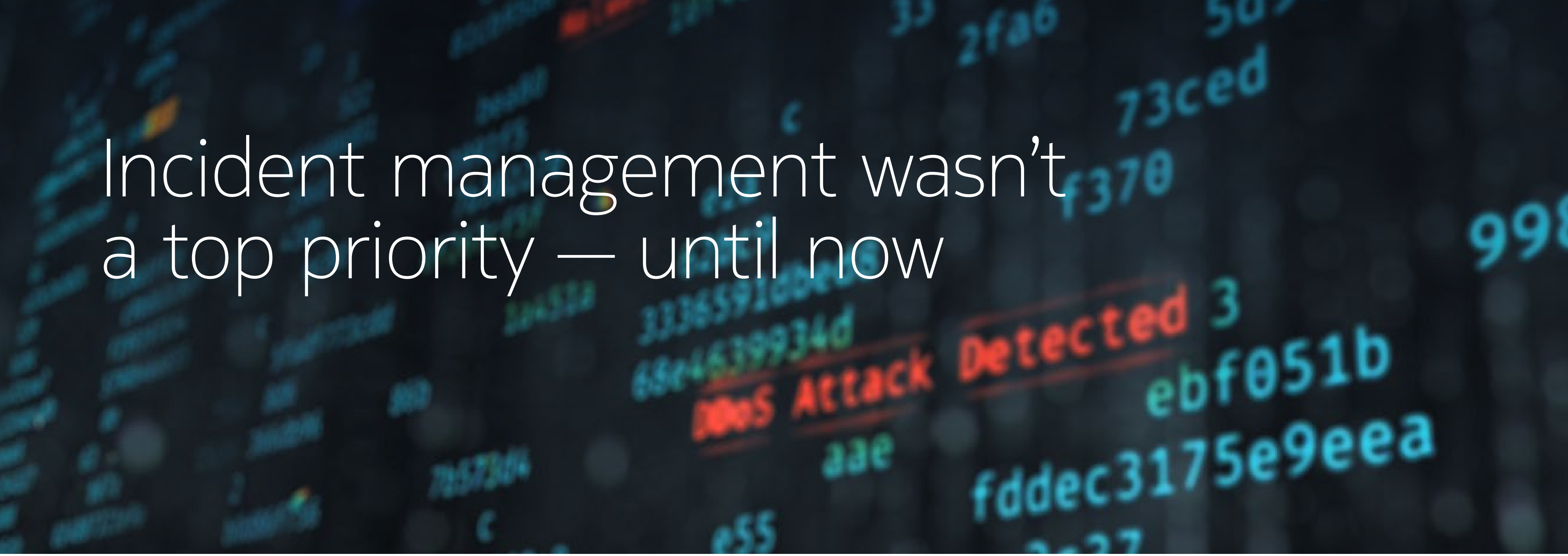
NOKIA

Adapting the incident management process flow for 5G

Cybersecurity in 5G with Nokia Managed Detection and Response (MDR)

Next >



Incident management wasn't a top priority — until now

Communications service providers (CSPs) haven't had to worry much over the years about incident management: the process of identifying, detecting and responding to threats in their networks. Traditional telecom networks enjoyed the twofold protection of being closed, proprietary systems and having historically rock-solid preventative security. Major incidents were few and far between, mostly limited to attackers seeking to disrupt best-effort voice or internet services.

5G is a different story.

5G lets CSPs access emerging opportunities in new verticals, but its openness and interconnectedness are now exposing mission-critical operational technology (OT) such as drones, remotely controlled machines, connected vehicles and other Industry 4.0 applications to the same kinds of cyberthreats usually encountered in the information technology (IT) domain.

With the attack surface growing and targets more lucrative, incident management capabilities are clearly essential. But even though the threats are similar, CSPs can't use IT-style frameworks and best practices for 5G. A new approach to incident management is needed.

Back

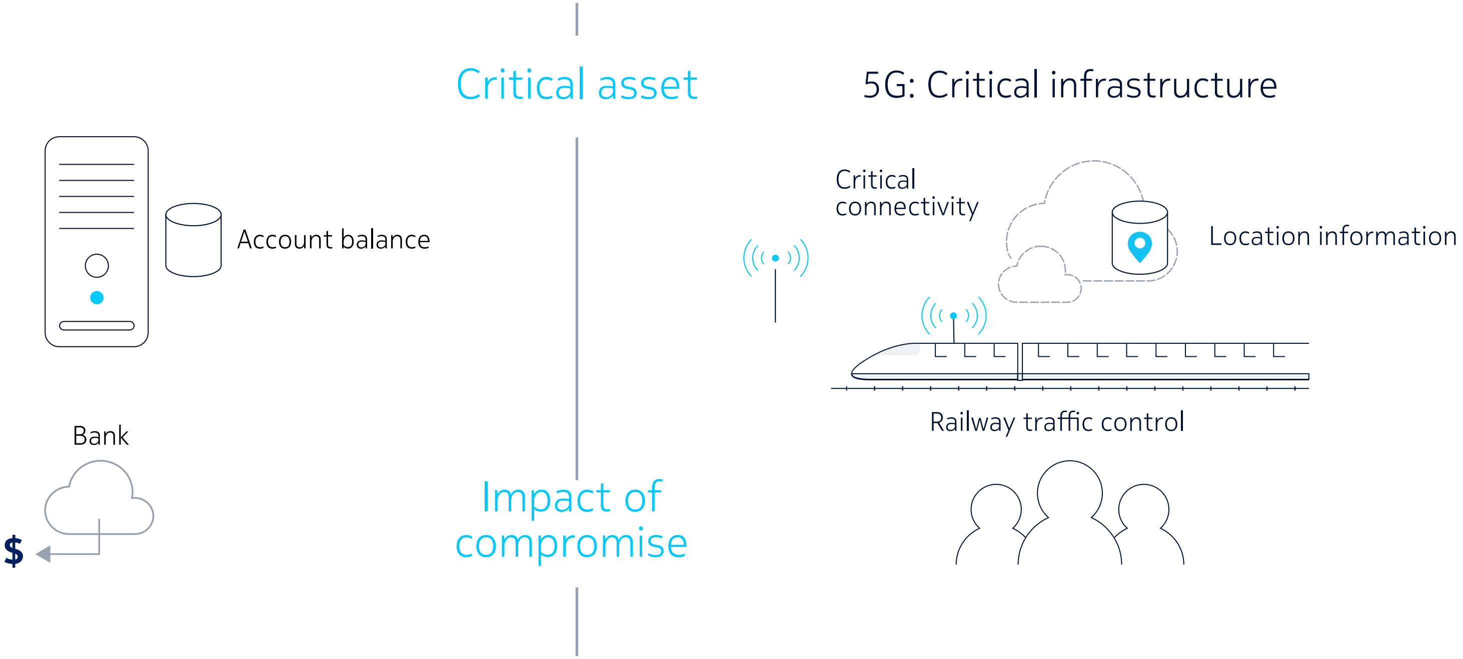
Next

What’s different about 5G security?

Part 1: Critical assets

5G and IT systems face the same general threat: malicious actors seek to exploit vulnerabilities in a critical asset of an organization or enterprise. What’s different is the critical asset being targeted.

In IT, the critical asset is data: sensitive personal or business information, such as bank account details. In 5G, it’s the functional elements of connectivity needed by the systems that control trains, drones, cranes, robotic arms and other critical infrastructure. The critical assets are different, so the impact when the three main tenets of security are compromised — confidentiality, integrity and availability — is also different. If credit card information is stolen, there are financial and reputational consequences. While the location of a train doesn’t need to stay confidential, if there are any gaps in the connectivity between that train and its 5G-powered traffic control system, people’s lives could also be at risk.



Critical asset

5G: Critical infrastructure

Account balance

Bank

Critical connectivity

Location information

Railway traffic control

Impact of compromise

What’s different about 5G security?

Part 2: Security attributes

Because the assets to be protected are not the same, the controls and processes used to secure IT environments can’t be ported directly to 5G. The “how” of cybersecurity needs to be tailored to 5G’s characteristics and attributes.

IT and 5G environments have different network functions and component locations, so they require different skill sets to manage and secure them. The functional elements of telecommunication networks have longer lifecycles than those found in IT infrastructure.

All of this (and more) must be taken into account in 5G incident management.

IT				5G
Temporary downtime acceptable data confidentiality/integrity is essential		Risk management requirements	24/7 365	Downtime not acceptable fault tolerance is essential
Generic hybrid IT infrastructure	IT	Infrastructure & communication protocols	5G	5G-specific network functions and protocols
IT personnel	IT	System management & operation	NW	Network engineering
Automated timely software patches and updates		Software change management		Strict testing requirements sequential deployment in maintenance window
< 5 years	5	Component lifecycle	10	< 10 years can remain in production after end of support
Centralized easy to access	○	Component location	○ ○ ○ ○	Distributed edge clouds
IT standards and regulations COBIT, PCI DSS, HIPA, GDPR		Compliance environment		Telecom standards and regulations 3GPP, IETF, ITU

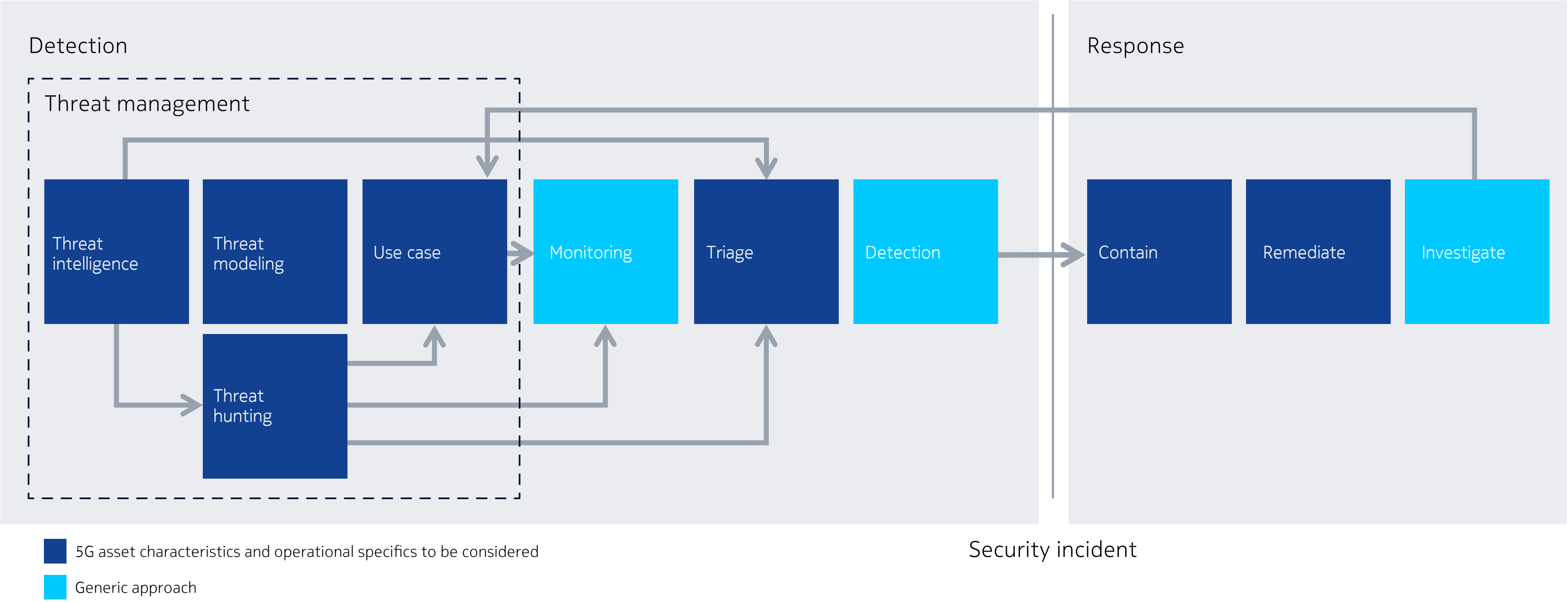
Back

Next

The 5G incident management process flow

At a high level, the incident management process flow is the same for 5G and IT. Applicable threats are identified and threat models are created for critical assets, allowing 5G-specific monitoring and detection use cases to be implemented. Alerts are triaged based on business priorities, and incidents are contained and remediated by automated workflows in the 5G infrastructure or by security analysts with deep 5G operational experience.

But the differences between 5G and IT security are amplified at each stage — making incident management the area in which security processes, technology stacks and skill sets most need to be adapted and modified for the 5G domain.



Adapting the flow for 5G: Threat management

CSPs have access to many sources of threat intelligence. Interpreting that intelligence correctly in the 5G context is key to effective threat modeling and threat hunting — and to creating the monitoring use cases that are vital to the process flow.

Threat modeling is an iterative process that involves the following steps:

Create the security profile

Breaking down the critical asset's architecture, including its network and host infrastructure to create a profile of the vulnerabilities in its design and implementation.

Determine applicable threats

Considering the goals of an attacker and an asset's potential vulnerabilities to identify relevant or probable threats to the asset.

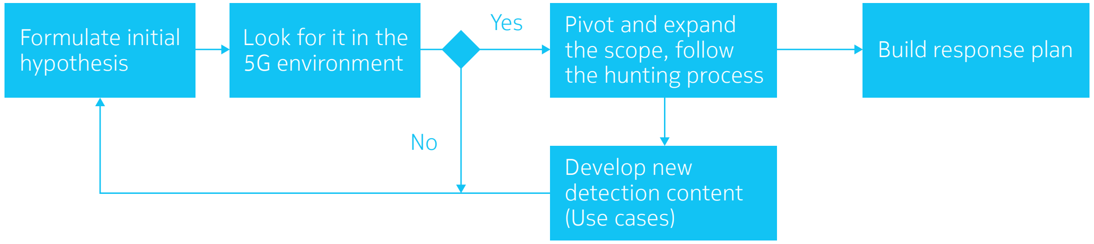
Identify countermeasures

Performing an asset-specific risk assessment and then identifying the preventive and detective security controls that should be implemented to block the identified threats.

Develop rules and dashboards

Determining events of interest, developing correlation scenarios and documenting the resulting 5G monitoring use cases based on the outcomes of the previous three phases.

CSPs can also use threat hunting to proactively uncover threats that have passed through automated preventative controls. This is about looking for unusual or malicious activity that might indicate signs of intrusion or compromise to the 5G environment, which can then inform detection and response plans.



Formulate initial hypothesis

Look for it in the 5G environment

Yes

No

Pivot and expand the scope, follow the hunting process

Build response plan

Develop new detection content (Use cases)

Adapting the flow for 5G: Detection and response

Timely detection and remediation of any attacks that get through preventative security controls have always been the most challenging part of cybersecurity, even in a simple and mature IT environment. That challenge is even greater for 5G.

Monitoring and detection processes in 5G are built on the use cases and indicators of attack/compromise defined via threat modeling and threat hunting.

Event monitoring is based on log sources collected from the 5G infrastructure through a modern security operations center (SOC). The SOC is equipped with the latest technology stack, typically with an extended detection and response (XDR) platform at its spearhead.[1] The SOC's tools and technologies are configured according to the 5G-specific use cases.

Once an alert is received, the incident triage process prioritizes them according to the business impacts on the enterprise's 5G environment.

The **incident response** processes used in IT security, including containment, analysis, remediation, reporting and forensics, are still valid in the 5G environment. But with 5G incident response being mainly an operational task (e.g., reloading network functions from backup or changing configuration or loading SW update to contain a security incident), it requires deep network architectural and operational competences that most IT security personnel don't have.

Such expertise is especially important when incident response is automated through digitized workflows orchestrated in the 5G environment. Response workflow automation is typically implemented in the SOC's XDR platform, which aims to minimize false positives and repetitive tasks so security teams can focus on 5G threat hunting and high-priority alerts.

[1] See the following page for more on XDR.

Back

Next

Two approaches to 5G incident management

CSPs have two options for implementing an effective incident management process flow in their 5G environments:

"DIY" with XDR

Some CSPs may prefer a "do it yourself" approach to ensure their security reflects the unique requirements of the 5G environment. For those that do, tools and technologies built around the XDR concept are key.

Designed to accommodate the ever-growing volumes of data coursing through 5G networks, XDR-based security operations are anchored by a robust data pipeline. That makes it possible for CSPs to collect more data from more sources, then process and analyze that data through one cohesive security management system — so they can act on threats faster and more effectively than ever before.

Team up with an expert MDR provider

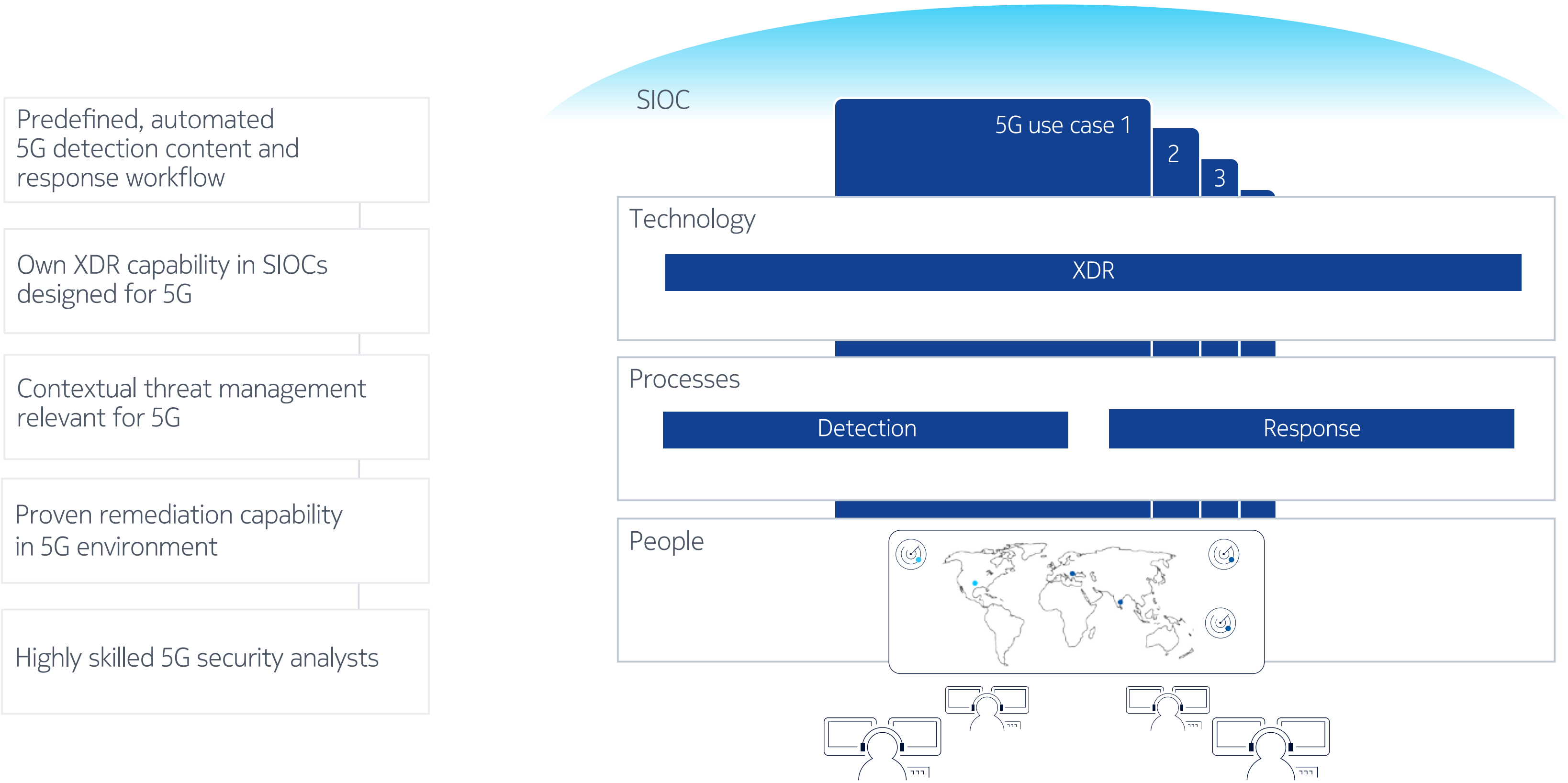
Not every CSP will have the in-house skills or resources to detect and respond to complex cyber threats on their own. With managed detection and response (MDR), XDR capabilities are delivered as a managed service by a highly experienced service provider.

By partnering with a skilled and capable MDR provider, CSPs can get the scalable, end-to-end incident management necessary in the 5G era without placing any additional burden on their already overwhelmed security operations teams.

Why Nokia is the best choice for MDR

Implementing high-performing incident management capabilities in 5G requires massive investments in security transformation, including upgrades to various security processes, tools and skill sets. At Nokia, we've already completed our own transformation in these critical areas, including bringing XDR capabilities into our security intelligence and operations centers (SIOCs). When combined with the best practices developed through security and 5G projects completed for customers around the world, we can offer MDR services at scale and in line with 5G's unique requirements.

As part of the broader Nokia Managed Security Services portfolio, MDR provides a holistic, end-to-end solution for incident management in the 5G era — delivering all the capabilities CSPs need to protect enterprise customers in every industry vertical 5G enables.



Predefined, automated 5G detection content and response workflow

Own XDR capability in SIOCs designed for 5G

Contextual threat management relevant for 5G

Proven remediation capability in 5G environment

Highly skilled 5G security analysts

Back

Visit our website to learn more about Nokia MDR services.

Next

NOKIA

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Document code: CID210577 (June)

About Nokia
We create technology that helps the world act together.

As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

Back