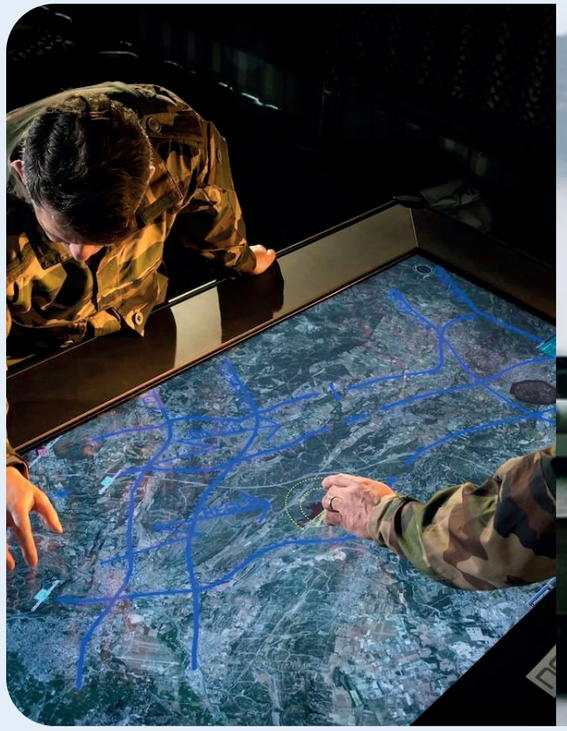
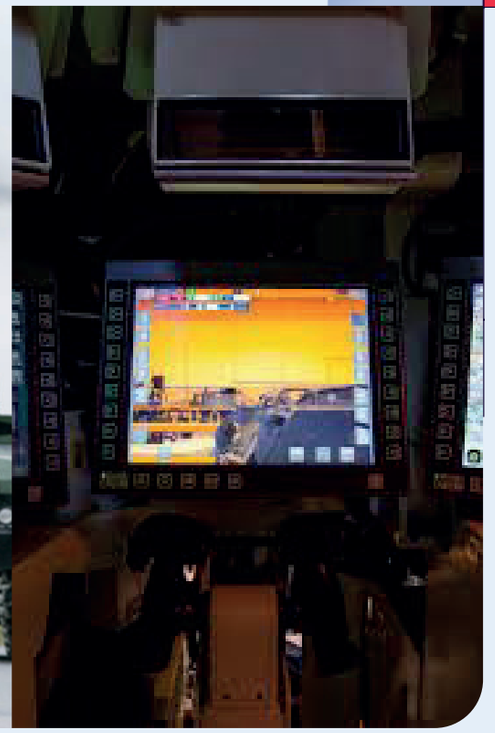
SUCCESS STORY
KNDS





“Gatewatcher’s NDR solution presents numerous advantages, particularly for sectors such as ours that are subject to various constraints, and for companies looking to optimize their detection strategy without impacting production.

BENOÎT MOREAU, CYBERSECURITY DIRECTOR – KNDS France

#NDR #DETECTION

KNDS France is a land defense systems integrator, dedicated to the needs of French and foreign land forces through the design, development and production of complete defense systems, artillery guns and armored vehicles. Its field of activity also extends to the supply of weapons systems for air and naval forces.

BENOÎT MOREAU_

Cybersecurity Director

KNDS France

01

EQUIPMENT FROM KNDS FRANCE IS USED BY OVER ONE HUNDRED ARMED FORCES AROUND THE WORLD. HOW STRINGENT ARE CYBERSECURITY STANDARDS IN MILITARY ENVIRONMENTS?

At KNDS France, we adhere to more rigorous protection standards compared to other sectors, given the persistence and extreme virulence of cyberattacks. Our clients set stringent demands in terms of cybersecurity; they fully understand the importance of security across the entire digital ecosystem. As an international group with 12 sites in Europe, KNDS France must also comply with the regulatory obligations of the countries in which its users operate. Cybersecurity for on-board digital technology has only recently been recognized as a priority. Yet digital solutions represent a major share of our defense product portfolio: in addition to armored vehicles, we offer solutions that interconnect all platforms, weapons systems and infantrymen and allow the sharing of tactical information. This use of digital technology potentially means greater vulnerability.

*Cyber challenges_*

Preserve
all stages of the defense product development cycle

Guarantee
the smooth functioning of defense products

Protect
on-board digital technology

Defend
against espionage

> **Digital components represent a sizeable proportion of our defense product portfolio [...]. This use of digital technology potentially means greater vulnerability.**

02

WHAT CYBERSECURITY CHALLENGES DOES KNDS FRANCE FACE TODAY?

Today, it is clear that cyber incidents can potentially impact the functioning of our weapons systems with varying consequences. The risk is real. We therefore need to be extremely vigilant in the face of cyberattacks and ensure that we have the capacity to act quickly, in other words with a short response cycle in the event of a threat. At the same time, we must protect and strengthen the entire upstream development cycle of our armored vehicles – which is where vulnerabilities can be exploited. It is important that we understand how to take corrective action, and how to detect and protect ourselves from what we don't yet know. And for us the essential question is also to understand where the risk lies so that we can implement appropriate measures, while taking operational constraints into account.

Attacks and threats are constantly evolving – if we don't adapt, the security in place to counter these threats will decrease. We need to maintain a high level of technological agility.

03

WHAT FORM DOES CYBER RISK TAKE?

The risk concerns the entire upstream ecosystem as well as on-board digital technology. In concrete terms, this involves threats to availability (which is critical in operations), threats to integrity (essential, among other things, for the precision of firepower) and confidentiality issues, particularly for command communications. Digital technology is therefore crucial for maintaining vehicle performance and to KNDS France's business activities. Our industry also faces a major threat that remains largely ignored, namely espionage and entrapment. We consequently need to anticipate and avert attempts by cyberattackers to gain access to the local network in order to compromise the confidentiality of our data, contracts and know-how.

04

HOW HAS GATEWATCHER TECHNOLOGY REPLIED TO THIS SPECIFIC DIVERSIFIED CHALLENGE?

Given the rapid pace of change in cybersecurity, both in terms of attacks and defense solutions, the need for agility and modularity is greater now than ever. A monolithic solution just does not work. That is why we prefer a 'building block' solution, like the OpenXDR approach for example, which covers an interoperable range of cybersecurity technologies. At KNDS France, we have deployed EDR technology to supervise workstations, a sandbox to control incoming data and Gatewatcher's NDR technology to monitor traffic flowing east-west (internal) and north-south (external data entering the IT network). Gatewatcher's NDR solution presents numerous advantages, particularly for sectors such as ours that are subject to various constraints, and for companies looking to optimize their detection strategy without impacting production. The NDR technology offered can be used on premise for sensitive entities subject to regulations, or in the cloud.

HEAD OFFICE
Versailles

BUSINESS SECTOR
Air-land defense

4 500
employees

12
sites in Europe

250
product references

100+
armed forces using the equipment

NDR AT THE HEART OF XDR APPROACH_

05

COULD YOU GIVE US AN OVERALL OUTLINE OF THE PROJECT?

Our cybersecurity strategy was implemented in three key stages: **understanding the challenges facing our field** in terms of regulations, **solution deployment model** (whether cloud-based or not) and sector-specific requirements; **awareness of potential threats**; and finally, knowledge of the defense resources available.

We then ‘created the need’, adopting an incremental approach: before drawing up the specifications, we had different solutions tested on perimeters perfectly controlled by the end users [the teams] and assessed the relationship with future partners. This enabled us to choose the best combination and solution for us. We involved the CIO in this process to address integration issues; we also made sure that the NDR solution was interoperable with existing technologies: perimeter solutions, sandboxes, EDR.

06

WHAT SELECTION CRITERIA DID YOU HAVE AND WHAT TRIGGERED YOUR PROJECT?

The primary driver behind this project was, and still is, **daily cyber threats**. We need to equip our teams, give them the means to detect and respond, and it is also essential that we master operational security internally. That is why NDR was identified as a key solution for meeting these challenges.

Regulatory compliance was also taken into account, as was **product sovereignty**. The latter required reinvesting in France and involves close links with the selected publisher – an advantage as we want to avoid any ‘cultural gaps’. To achieve this, we have specifically strengthened digital and cyber governance at KNDS France by forging closer collaboration between the CIO and the CISO.

07

HOW IS THIS A FOUNDATION FOR THE FUTURE?

XDR is an approach, an operating model, that meets the need for modularity and constant agility in the face of changing threats. Once we have reached this new level of maturity, we enter a virtuous circle of continuous improvement; complete control of each building block enables us to challenge the others in the event of threat detection.

Beyond these aspects, we also strive to automate everything possible, because humans are fallible. Where this is not feasible, we seek to implement tooling that assists the expert’s ability to react.

“We need to equip our teams, give them the means to detect and respond, and it is also essential that we master operational security internally. That is why NDR was identified as a key solution for meeting these challenges.

*Benefits_*

Gatewatcher technology enables:

High visibility
of as yet unknown vulnerabilities and threats concealed deep within the network

Optimization
of the detection strategy without impacting production

Flexibility
of the solution: NDR's technology can be used on premise or in the cloud, depending on the level of sensitivity of the entities to be protected

4 tips from the CISO

> **Expertise – know your sector:** IT, obviously, but also regulatory constraints, business needs and your organization's degree of exposure.

> **Skills – develop human and technology skills:** Organize teams of expert end users to consolidate know-how internally and build on this to construct the technological foundation (and to do so, I recommend testing solutions and the relationship with potential partners).

> **Community –** Don't isolate yourself, discuss ideas with peers, collaborate with partners, learn about possible approaches and best practices from your cyber community.

> **Pragmatism –** Adopt an incremental and empirical approach, taking things one step at a time and gradually putting individual building blocks in place so that you can learn how to use and interconnect them.

THE GATEWATCHER SOLUTION

Gatewatcher's NDR platform offers cyber-threat mapping and behavioral analysis to ensure enhanced detection of targeted attacks, even in the case of encrypted data flow. It combines machine learning with static and dynamic analysis.