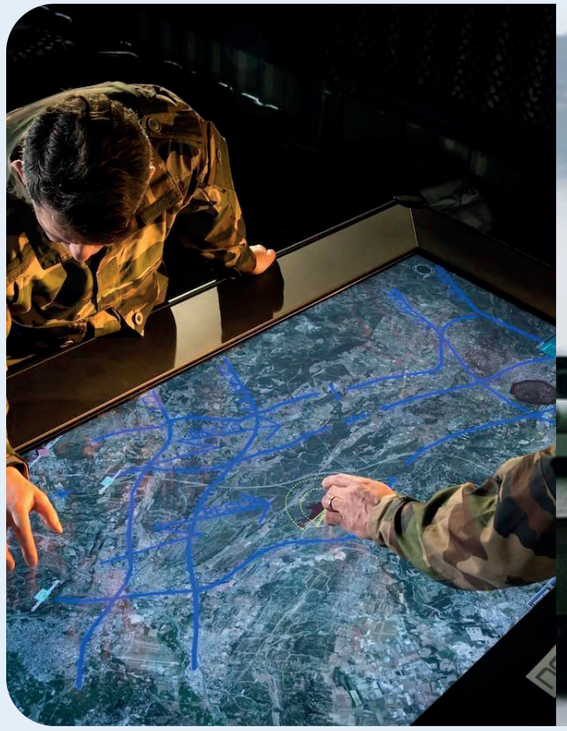
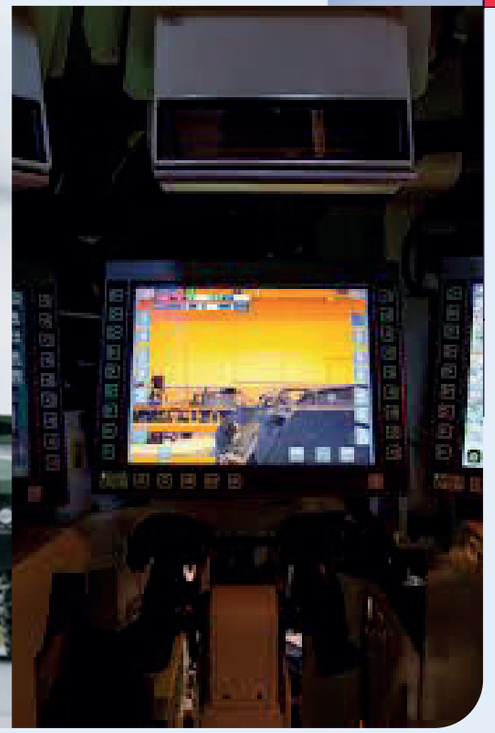
CUSTOMER STORY
KNDS





“La solution NDR de Gatewatcher dispose de nombreux avantages, notamment pour les secteurs comme le nôtre qui présentent certaines contraintes, et pour les entreprises qui cherchent à optimiser leur stratégie de détection sans impacter leur production.

BENOÎT MOREAU, DIRECTEUR CYBERSÉCURITÉ – KNDS France

#NDR #DETECTION

Systémier intégrateur de défense terrestre, KNDS France a pour vocation de répondre aux besoins des armées de Terre française et étrangères, à travers la conception, le développement et la production de systèmes complets de défense, canons d'artillerie et engins blindés. Son domaine d'activité s'étend à la fourniture de systèmes d'armes pour les forces aériennes et navales.

BENOÎT MOREAU_

Directeur Cybersécurité
KNDS France

01

LE MATÉRIEL KNDS FRANCE EST UTILISÉ PAR PLUS D'UNE CENTAINE D'ARMÉES DANS LE MONDE. QUEL EST LE NIVEAU D'EXIGENCE CYBER DANS LE MILIEU MILITAIRE ?

Chez KNDS France, nous avons des exigences de protection en matière de cybersécurité plus élevées que la moyenne par rapport à d'autres secteurs, compte-tenu de la persévérance et de la virulence élevée des cyberattaquants. On observe ainsi un très fort niveau d'exigence cyber de la part de nos clients; la notion de sécurité de tout l'écosystème numérique est bien comprise. En tant que groupe international, avec 12 sites en Europe, KNDS France doit aussi être conforme aux obligations règlementaires des pays de ses utilisateurs. Sur la cyber embarquée, la compréhension est plus récente. Pourtant, les solutions numériques représentent une part importante de notre catalogue de produits de défense: outre les véhicules blindés, nous proposons les solutions permettant de connecter en réseau toutes les plateformes, systèmes d'armes et les fantassins et de partager des informations tactiques. Cette utilisation du numérique implique potentiellement plus de fragilités.

*Challenges cyber_*

Préserver
tout l'amont du cycle de développement des produits de défense

Garantir
le fonctionnement des produits de défense

Protéger
le numérique embarqué

Se prémunir
contre l'espionnage

> **Les composants numériques représentent une part importante de notre catalogue de produits de défense[...]. Cette utilisation du numérique implique potentiellement plus de fragilités.**

02

QUELS SONT AUJOURD'HUI LES ENJEUX POUR KNDS FRANCE EN CYBERSÉCURITÉ ?

Aujourd'hui, on observe qu'un problème cyber pourrait avoir un impact plus ou moins majeur sur le fonctionnement de nos systèmes d'armes. Le risque est réel. Nous avons donc besoin d'être très vigilants face aux cyberattaquants et d'avoir des capacités d'action rapide, c'est-à-dire un **cycle court de réaction à la menace**. Parallèlement, nous avons besoin de protéger et de renforcer tout l'amont du cycle de développement de nos véhicules blindés – où les vulnérabilités exploitées peuvent se situer. Nous devons savoir comment faire pour corriger, pour détecter et nous protéger de ce que l'on ne connaît pas encore. Et la question essentielle pour nous est aussi de savoir à quel niveau se situe le risque pour mettre en place les mesures adaptées en tenant compte des contraintes opérationnelles.

Les attaques, les menaces évoluent – si nous n'évoluons pas, la sécurité face à la menace diminue. Il nous faut maintenir un niveau d'agilité technologique.

03

QUELLE FORME PREND LE RISQUE CYBER ?

Le risque concerne tout l'écosystème en amont et le numérique embarqué. Il se traduit concrètement par des menaces sur la **disponibilité** (qui est critique en opération), par des menaces en **intégrité** (indispensable entre autres pour la précision des capacités de feu) et par un enjeu de **confidentialité**, notamment des communications de commandement. Le numérique est donc déterminant pour maintenir la performance des véhicules et les activités de KNDS France. Par ailleurs, il existe aujourd'hui pour notre secteur une menace importante, encore ignorée, à savoir l'espionnage ainsi que le piégeage. Il nous faut donc imaginer et prévenir la volonté de cyber attaquants de s'intégrer dans le réseau local à des fins d'atteinte à la confidentialité des données, des contrats et de notre savoir-faire.

04

COMMENT LA TECHNOLOGIE DE GATEWATCHER A-T-ELLE RÉPONDU À CE DÉFI SPÉCIFIQUE DE DIVERSITÉ ?

Au vu des changements très rapides dans le domaine de la cybersécurité, aussi bien du point de vue des attaques que des solutions de défense, nous avons aujourd'hui plus que jamais besoin **d'agilité et de modularité.** Aussi, une solution monolithique ne fonctionne pas. C'est la raison pour laquelle nous privilégions une solution à base de «briques», à l'image de l'approche OpenXDR par exemple, qui correspond à un éventail interopérable de technologies de cybersécurité. Au sein de KNDS France, nous avons donc déployé : la technologie EDR pour maîtriser les postes, la sandbox pour contrôler les entrants et la technologie NDR de Gatewatcher pour surveiller le trafic Est-Ouest (interne) et Nord-Sud (de l'extérieur vers l'intérieur du réseau informatique). La solution NDR de Gatewatcher dispose de nombreux avantages, notamment pour les secteurs comme le nôtre qui présentent certaines contraintes, et pour les entreprises qui cherchent **à optimiser leur stratégie de détection sans impacter leur production.** La technologie NDR proposée peut en effet être utilisée «on premise», pour les entités sensibles et soumises à réglementations, ou dans le cloud.

SIÈGE SOCIAL
Versailles

SECTEUR D'ACTIVITÉ
Défense aéroterrestre

4 500
collaborateurs

12
implantations en Europe

250
références produits

+100
armées utilisatrices de matériels

LE NDR AU SEIN D'UNE DEMARCHE XDR_

05

POURRIEZ-VOUS NOUS DONNER UNE VUE D'ENSEMBLE DU PROJET?

Notre stratégie de cybersécurité a pu être mise en place grâce à trois étapes clés : **la connaissance des enjeux de notre territoire** via les règlementations, **le modèle de déploiement de la solution,** dans le cloud ou non, et les besoins métiers ; **la connaissance des menaces** et enfin, la connaissance des moyens pour se défendre.

Nous avons ensuite 'construit le besoin' et adopté une démarche incrémentale : avant de dresser le cahier des charges, nous avons fait tester les solutions sur des périmètres bien maîtrisés par les utilisateurs finaux [les équipes] et évalué la relation avec les futurs partenaires, pour nous permettre de choisir le meilleur assemblage et la solution qui nous convienne le mieux. Nous avons intégré la DSI dans ce processus pour évoquer les questions d'intégration; nous nous sommes également assuré de l'interopérabilité de la solution NDR avec les technologies existantes: solutions périmétriques, sandbox, EDR.

06

QUELS ONT ÉTÉ LES CRITÈRES DE SÉLECTION ET LES ÉLÉMENTS DÉCLENCHEURS DE VOTRE PROJET?

L'élément principal et déclencheur de ce projet a été et reste définitivement **la menace cyber quotidienne**. Nous avons besoin d'outiller nos équipes, de leur donner des capacités de détection et de réaction, nous avons besoin de maîtriser en interne la sécurité opérationnelle. C'est en cela que le NDR est apparu comme une des solutions indispensables pour répondre à ces enjeux-là.

La conformité réglementaire a été également un élément pris en compte et enfin, **la souveraineté du produit.** Cette dernière induit que nous réinvestissions en France et implique des liens de proximité avec l'éditeur choisi – un aspect bénéfique car nous voulons éviter les éventuels 'gaps culturels'. Pour y arriver, nous avons notamment, au sein de KNDS France, renforcé la gouvernance numérique et cyber en rapprochant le DSI et le RSSI.

07

EN QUOI EST-CE UN SOCLE POUR LA SUITE?

Le XDR est une démarche, un fonctionnement, qui correspond au besoin d'être modulaire et de maintenir un niveau d'agilité face à l'évolution de la menace. Dès lors que nous avons atteint ce nouveau niveau de maturité, nous rentrons dans un cercle vertueux d'amélioration continue, la maîtrise de chaque brique permet de challenger les autres lors d'une détection.

Au-delà de ces aspects, nous nous efforçons aussi d'automatiser au mieux tout ce que nous pouvons, car l'humain est faillible. Lorsque ce n'est pas faisable, nous nous employons à implémenter l'outillage afin d'aider l'expert dans sa capacité de réaction.

> Nous avons besoin d'outiller nos équipes, de leur donner des capacités de détection et de réaction, nous avons besoin de maîtriser en interne la sécurité opérationnelle. C'est en cela que le NDR est apparu comme une des solutions indispensables pour répondre à ces enjeux-là.

*Bénéfices_*

La technologie Gatewatcher permet une :

Haute visibilité
sur les vulnérabilités et les menaces encore inconnues, dissimulées au cœur du réseau

Optimisation
de la stratégie de détection sans impact sur la production

Flexibilité
de la solution: utilisation de la technologie NDR “on premise”, ou dans le cloud, selon le degré de sensibilité des entités à protéger.

4 conseils du RSSI:

> **Maîtrise - Connaître son territoire:** l’IT bien sûr mais aussi les contraintes réglementaires, les besoins métiers, le degré d’exposition de votre organisation.

> **Capacités - Développer des capacités humaines et technologiques :** organiser des équipes de sachants utilisateurs finaux afin de consolider de la compétence en interne et se reposer dessus pour construire le socle technologique (et pour ce faire je recommande de tester les solutions et la relation partenaires).

> **Communauté -** Ne pas s’isoler, échanger avec des pairs, travailler avec des partenaires, s’informer sur les approches et bonnes pratiques possibles auprès de sa communauté cyber.

> **Pragmatisme -** Adopter une démarche incrémentale et empirique, en y allant pas à pas et en mettant les briques les unes après les autres, pour apprendre à s’en servir et les interconnecter.

LA SOLUTION GATEWATCHER

La plateforme NDR de Gatewatcher offre une cartographie et une analyse comportementale des cybermenaces pour obtenir une détection augmentée sur les attaques ciblées, y compris en cas de flux chiffrés. Elle associe machine learning, analyses statique et dynamique.