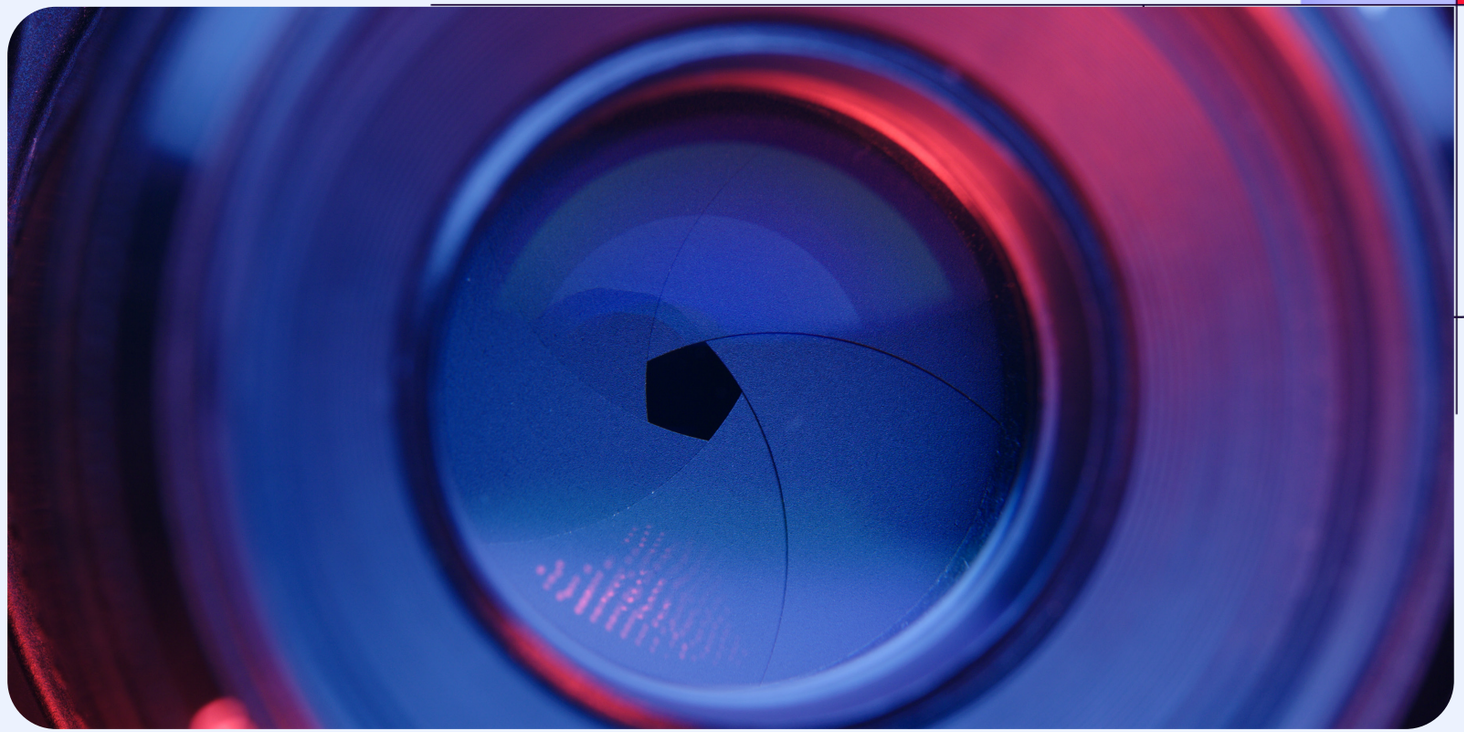
CUSTOMER STORY

LYNRED



“

En moins de deux jours, les machines étaient installées et les flux visibles. Le NDR, aligné avec notre PSSI, nous a offert une visibilité complète. Cette approche nous a permis de détecter des éléments pertinents dès la première semaine.

Bertrand FRÉMONT
RSSI LYNRED

#NDR #DEFENSE #AEROSPATIAL #INDUSTRIE

Bertrand FRÉMONT_
RSSI LYNRED

À propos

LYNRED et sa filiale américaine LYNRED USA sont des leaders mondiaux dans la conception et la fabrication de technologies infrarouges de haute qualité pour les secteurs de l'aérospatial, de la défense et des marchés commerciaux. Leur vaste portefeuille de détecteurs infrarouges couvre l'ensemble du spectre électromagnétique, du proche à l'infrarouge lointain. Les produits du Groupe sont au cœur de nombreux programmes et applications militaires. Leurs détecteurs infrarouges sont des composants clés pour de nombreuses grandes marques dans les équipements d'imagerie thermique utilisés dans les domaines commercial, civil et militaire, vendus en Europe, en Asie et en Amérique du Nord. L'organisation est le principal fabricant européen de détecteurs infrarouges déployés dans l'espace.

*Enjeux cybersécurité_*

Détecter et sécuriser
les réseaux industriels et de défense critiques contre des cybermenaces avancées

Gérer
des ressources en cybersécurité limitées tout en garantissant une protection complète

Intégrer
les solutions EDR et NDR pour une détection et une réponse unifiée aux menaces

S'adapter
aux menaces cyber en constante évolution avec une stratégie de sécurité évolutive et résiliente

Unifier
la cybersécurité dans un environnement fragmenté pour une protection sans faille

01 POUVEZ-VOUS NOUS EXPLIQUER LE CONTEXTE DE CYBERSÉCURITÉ DANS LEQUEL VOUS ÉVOLUEZ ?

LYNRED est détenue à parts égales par Safran et Thales, mais nous avons été totalement indépendants dans le choix des solutions techniques de cybersécurité pour ce projet.

Notre entreprise **emploie plus de 1 000 personnes et fonctionne en continu, 24h/24 et 7j/7**. Compte tenu de notre taille et de la nature critique de notre secteur, nous devons **optimiser nos ressources et éviter de multiplier les solutions différentes pour chaque problème spécifique.**

De plus, **LYNRED est répartie sur deux sites principaux**, à Grenoble et en région parisienne, ce qui complexifie davantage la gestion de notre infrastructure. C'est pourquoi nous avons opté pour une approche unifiée, plus adaptée à nos besoins et à la structure de notre infrastructure.

> *Il était donc crucial d'ajouter une couche de visibilité sur le réseau pour surveiller les activités qui échappent au périmètre de l'EDR, en particulier sur les systèmes industriels (SI).*

02

QUELLE FORME PREND LE RISQUE CYBER ET QUELLES MÉTHODES TRADITIONNELLES UTILISEZ-VOUS POUR Y PALLIER ?

Le principal risque auquel nous faisons face aujourd'hui concerne les **attaques de type cryptographique**, que nous avons identifiées comme étant la menace majeure. En parallèle de ce constat, nous avons initié un chantier global pour réduire ces risques, touchant à la fois l'architecture de nos systèmes, notre organisation et les outils que nous employons. Comme beaucoup d'entreprises industrielles, nous renforçons notre posture de sécurité. **Nous abandonnons progressivement les antivirus traditionnels, devenus insuffisants face aux nouvelles menaces, pour adopter des solutions plus robustes et adaptées à l'évolution des cyberattaques.**

03

QUELLES SOLUTIONS AVEZ-VOUS RETENUES ET QUEL EST L'ÉTAT DE LEUR DÉPLOIEMENT ?

Nous avons pris la décision d'aborder nos trois projets — architecture, organisation et outillage — de manière intégrée. L'idée est de **combiner plusieurs solutions complémentaires** : EDR pour la protection individuelle, NDR pour une protection à grande échelle, un SOC managé pour une surveillance continue 24h/24 et 7j/7 et un recours au CSIRT en cas d'urgence ou de plan de reprise d'activité (PRA).

Notre choix s'est fait en prenant en compte plusieurs facteurs :

> **La confiance dans la technologie,** avec la question clé de savoir si la solution répondra réellement à nos besoins spécifiques.

> **Notre capacité à la gérer en interne,** ou bien si cela devra finalement se transformer en service managé.

> **L'aspect financier,** même si en l'occurrence, le budget alloué était relativement équivalent pour les différentes options.

Nous avons ainsi opté pour l'EDR Sentinel One, le NDR Gatewatcher, et la gestion du SOC managé avec Synetis.

04

POURQUOI AVEZ-VOUS CHOISI D'INVESTIR DANS UNE SOLUTION NDR ?

Bien que l'EDR soit une solution efficace, un environnement industriel, comme celui de LYNRED, impose des contraintes qui ne permettent pas toujours son déploiement, notamment sur certains systèmes spécifiques. Il était donc crucial d'ajouter une couche de visibilité sur le réseau pour surveiller les activités qui échappent au périmètre de l'EDR, en particulier sur les systèmes industriels (SI).

L'EDR est déployé là où nous avons la maîtrise complète du système, notamment sur les serveurs et les postes de travail, mais dans les environnements OT, où nous n'avons pas ce contrôle, le NDR devient indispensable. **Le NDR nous permet de capter l'ensemble des flux réseau**, quelle que soit la nature des équipements concernés, complétant ainsi la couverture offerte par l'EDR. Ensemble, ces deux solutions assurent une **protection globale, adaptée à la diversité de nos systèmes.**

Découvrez toutes nos alliances technologiques

SIÈGE SOCIAL
Veurey-Voroize, France

SECTEUR D'ACTIVITÉ
Fabrication de semi-conducteurs

> 1,000
collaborateurs

MARCHÉS SERVIS
défense, spatial, sécurité & surveillance, industrie, grand public, bâtiment intelligent et automobile

05

SUITE À VOTRE CHOIX D'UNE SOLUTION NDR, POURQUOI AVEZ-VOUS OPTÉ POUR GATEWATCHER ?

Dans le cadre de notre appel d'offres, nous avons mené une analyse approfondie des différentes solutions disponibles sur le marché. Nous avons participé à des ateliers et des démonstrations avec plusieurs acteurs, y compris des concurrents internationaux. À l'issue de ce processus, nous avons choisi la solution la plus performante selon nous et qui répondait à nos besoins de détection et de sécurité.
Nous avions par ailleurs **plusieurs objectifs en matière de détection** : surveiller les flux Nord/Sud, l'exfiltration de données entre Internet et les DMZ par exemple ; ainsi que la collecte des flux Est/Ouest, en particulier sur nos réseaux industriels.
Ce qui nous a convaincus chez Gatewatcher, c'est la **modularité de la solution** : elle peut être déployée en mode on-premise, en SaaS, ou un mélange des deux, selon les besoins. Cette flexibilité est essentielle, surtout dans un contexte où nos infrastructures sont réparties entre Grenoble et Paris. Gatewatcher permet justement de combiner des sondes physiques et des machines virtuelles dans une infrastructure virtualisée. Un autre aspect essentiel pour nous était **l'interopérabilité**. Nous souhaitions des solutions parfaitement intégrées à notre écosystème existant, capables de communiquer entre elles, plutôt que des systèmes isolés. De plus, la solution est exhaustive et assez facile à prendre en main.
Le fait que Gatewatcher soit une solution française conforme aux exigences de l'ANSSI et souveraine représentait un atout important, en particulier dans notre secteur, mais ce n'était pas le seul critère sur lequel nous avons fondé notre décision, comme en témoigne notre choix de Sentinel One pour l'EDR.

06

POUVEZ-VOUS NOUS PARLER DU DÉPLOIEMENT DE LA SOLUTION ET DES PRINCIPAUX DÉFIS RENCONTRÉS ?

Le déploiement, bien que rapide une fois les emplacements et interconnexions définis, nécessite une attention particulière car «le diable est dans les détails.» Chaque flux réseau doit être soigneusement pris en compte, ce qui implique une collaboration étroite avec l'équipe réseau et Gatewatcher. Ce n'est pas un projet que l'on peut mener seul.
Une fois cette phase préparatoire achevée, tout est allé très vite: en moins de deux jours, les machines étaient installées et les flux visibles. **Le NDR, aligné avec notre PSSI, nous a offert une visibilité complète. Cette approche nous a permis de détecter des éléments pertinents dès la première semaine.**

Comparativement, le déploiement de l'EDR s'est révélé plus complexe et chronophage, notamment à cause de la gestion des faux positifs. Comme l'EDR s'imbrique directement avec chaque machine, il est nécessaire de traiter des centaines de faux positifs lors du déploiement sur chaque poste, ce qui ralentit considérablement le processus.

Exemples concrets d'utilisation _

>Tentative de phishing déjouée grâce à l'analyse des requêtes DNS :

Nous avons rapidement pu déjouer une tentative de phishing **en identifiant un domaine malveillant grâce à une simple requête DNS.** Gatewatcher a détecté cette activité suspecte en analysant les requêtes vers des serveurs potentiellement dangereux. Bien que le processus ait généré un nombre important d'alertes au départ, celles-ci se sont rapidement révélées cruciales pour renforcer notre sécurité. Grâce à cette analyse, nous avons pu bloquer la menace avant qu'elle n'atteigne la boîte mail de l'utilisateur concerné.

>Correction d'une vulnérabilité critique sur la téléphonie IP :

Nous avons identifié une tentative d'exploitation d'une vulnérabilité sur notre plateforme de téléphonie IP, grâce à la visibilité apportée par le NDR sur les flux Nord/Sud. En analysant les données entrantes et sortantes de notre site, le **NDR a détecté qu'une des plateformes n'était pas à jour avec un correctif de sécurité.** Cette détection nous a permis d'agir rapidement en corrigeant la faille, puis en prenant des mesures proactives, telles que le blacklistage des sources malveillantes qui cherchaient à exploiter cette vulnérabilité.

07

POURQUOI AVEZ-VOUS CHOISI DE COLLABORER AVEC UN MSSP POUR EXPLOITER VOTRE NDR ?

Étant une entreprise de taille intermédiaire avec une équipe dédiée à la cybersécurité, il était essentiel pour nous d'exploiter pleinement notre solution NDR. **Il n'y a rien de pire que de déployer une solution sans en tirer tous les bénéfices.** Afin d'optimiser les coûts et l'efficacité d'une surveillance 24h/24 et 7j/7, nous avons choisi d'externaliser cette partie avec l'appui de Synetis, tout en gardant le contrôle sur les consoles. Cela dit, notre décision de faire appel à un MSSP répond à nos besoins spécifiques. **La solution Gatewatcher est suffisamment intuitive et facile à prendre en main pour être exploitée en interne par des entreprises qui disposent des ressources nécessaires.**

L'un des enjeux principaux pour nous était **de pouvoir réagir rapidement,** même si une menace, telle qu'une exfiltration de données, survenait un vendredi soir. Il ne suffit pas de s'appuyer uniquement sur le NDR ; il faut être capable de déclencher les alertes adéquates, d'agir sur le système d'information, et de contacter le CSIRT si nécessaire. Nos équipes internes ne disposant pas des compétences requises pour une telle réactivité, nous avons opté pour cette solution hybride, tout en conservant la possibilité de mener nos propres analyses.

08

VOUS AVEZ DÉPLOYÉ UN NDR ET UN EDR SIMULTANÉMENT, POURQUOI NE PAS AVOIR ENVISAGÉ DE VOUS TOURNER VERS DES OFFRES XDR ?

L'approche XDR est parfois utilisée à des fins marketing. Nous ne voyons pas d'intérêt à opter pour une solution unique censée tout faire, car en général, **ce type de solution n'excelle jamais dans tous les domaines.** Notre objectif est tout de même de rationaliser les outils que nous utilisons. Si nous nous retrouvons avec une console différente pour chaque problématique, cela ne sera pas optimal, ni pour nous, ni pour les services managés avec lesquels nous collaborons.

Selon moi, **ce sont encore des solutions distinctes aujourd'hui.** Le NDR et l'EDR visent à protéger l'entreprise, mais ils ne s'appliquent pas aux mêmes types d'assets et n'agissent pas au même niveau. Il n'est donc pas nécessaire, à ce stade, de chercher à fusionner toutes ces technologies dans une seule solution.

Bénéfices clés_

Détecter
les menaces avancées sur les environnements IT et OT

Surveiller
le trafic réseau pour identifier les risques cachés

Accélérer
la réponse aux menaces et leur mitigation

Renforcer
la résilience cybersécurité dans les environnements industriels

Intégrer
de manière transparente avec les solutions EDR et les SOC

> *« Un point fort de la solution a été sa réactivité et sa quasi instantanéité: « en seulement 3 heures, grâce à notre service managé, nous avons pu identifier l'attaque, bloquer les sources et lancer les mises à jour nécessaires. »*

*À propos de Gatewatcher_*

Leader dans la détection des cybermenaces,Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques à travers le monde. Ses solutions de Network Detection and Response (NDR) et de Cyber Threat Intelligence (CTI) détectent les intrusions et répondent rapidement à toutes les techniques d'attaque. Grâce à l'association de l'IA à des techniques d'analyse dynamiques, Gatewatcher offre une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on-premise.

Contactez-nous

Plateforme NDR_
GATEWATCHER

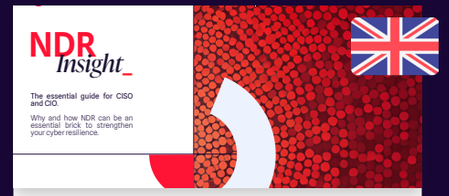
GEN AI_
CTI_
NDR_
DEEP VISIBILITY_
TAP_

La plateforme NDR de Gatewatcher offre une cartographie des cybermenaces et une analyse comportementale afin d'assurer la détection des attaques ciblées, même en cas de flux de données chiffrées. Elle combine notamment du machine learning avec des analyses statiques et dynamiques.

Envie d'en *savoir plus ?_*

[TÉMOIGNAGE CLIENT KNDS]
Découvrez notre customer story avec KNDS, entreprise européenne de l'industrie de la défense.

[CAS D'USAGE]
Renforcer mon EDR



[GUIDE NDR]
Guide NDR : L'essentiel pour les RSSI, DSI et dirigeants