CUSTOMER STORY

SÉCURISER LES RÉSEAUX D'UN ACTEUR DE L'ÉNERGIE_

“

La souveraineté de nos données était non négociable, et cette plateforme NDR y répond parfaitement. Nous surveillons désormais nos réseaux industriels 24/7 sans impacter l'opérationnel, et détectons la moindre anomalie bien avant qu'elle ne devienne une menace.

Directeur Cybersécurité
d'un opérateur régional du secteur de l'énergie

#NDR #ÉNERGIE #OT
#PROTOCOLEINDUSTRIEL #SOUVERAINETÉ

> *Le défi quotidien consiste donc à protéger des systèmes hétérogènes, souvent anciens et critiques, avec des ressources humaines limitées, tout en garantissant la continuité de service et la conformité aux normes de notre secteur.*

01 POUVEZ-VOUS NOUS PRÉSENTER VOTRE ORGANISATION ET LES ENJEUX CYBER SPÉCIFIQUES À VOTRE SECTEUR ?

Nous sommes un acteur à l'échelle nationale de l'énergie, présent de la production à la distribution d'électricité mais aussi de gaz, avec des infrastructures critiques réparties sur tout le territoire. À ce titre, nous faisons face à des enjeux cybersécurité très élevés. **D'une part, la digitalisation croissante** (smart grids, IoT industriel, télégestion à distance des sites) expose de nouveaux points d'entrée aux attaquants. **D'autre part, nos réseaux industriels** (SCADA, automatismes de centrales, capteurs et protocoles OT) sont des cibles de choix pour des acteurs malveillants sophistiqués, notamment des APT soutenus par des États ou des cybercriminels cherchant à causer des perturbations majeures. **Une cyberattaque réussie** pourrait non seulement **interrompre la fourniture d'énergie,** avec des conséquences économiques et sociétales plus ou moins graves, mais aussi **endommager des équipements coûteux** ou **mettre en danger la sécurité des personnes,** notamment sur des sites industriels sensibles (centrales thermiques ou nucléaires, postes haute tension en maintenance, ou encore systèmes de signalisation ferroviaire alimentés en direct).

Enfin, nous sommes **soumis à des réglementations strictes** (LPM, depuis peu directives de type NIS 2) **qui nous imposent un niveau de protection et de contrôle très élevé.** Le défi quotidien consiste donc à protéger des systèmes hétérogènes, souvent anciens et critiques, avec des ressources humaines limitées, tout en garantissant la continuité de service et la conformité aux normes de notre secteur.

*Enjeux cybersécurité_*

Protéger
des infrastructures critiques (réseaux électriques, systèmes industriels) contre des cybermenaces avancées (APT, ransomwares ciblés, sabotage)

Maintenir
la disponibilité 24/7 des systèmes OT tout en renforçant leur sécurité, sans jamais interrompre l'activité

Satisfaire
des exigences réglementaires strictes (conformité ANSSI, NIS 2, etc.) et assurer la souveraineté des données sensibles

Détecter
immédiatement des attaques sophistiquées sur des réseaux segmentés et des protocoles spécifiques, souvent invisibles aux outils classiques

Surveiller
un périmètre hybride IT/OT étendu avec des ressources humaines limitées, en évitant la surcharge et la fatigue des analystes SOC

02 QUELLES SONT VOS PRINCIPALES CONTRAINTES TECHNIQUES ET OPÉRATIONNELLES EN MATIÈRE DE CYBERSÉCURITÉ ?

Nos contraintes tiennent à la nature même de notre métier et de nos outils. D'abord, **la disponibilité** de nos systèmes industriels est une priorité absolue : **aucune solution de sécurité ne doit perturber le fonctionnement de nos automates, ni engendrer de latence sur le réseau de commande.** Nous devons donc privilégier des technologies passives et non intrusives. C'est pour cela que nous utilisons des TAP réseaux pour dupliquer le trafic vers les sondes NDR sans jamais interrompre la production. Ensuite, nous opérons **des sites répartis géographiquement, avec parfois des liaisons réseau limitées ou isolées.** Il a donc fallu un système capable de fonctionner de manière **autonome en local,** sans dépendance à un cloud public. **La souveraineté** et la **confidentialité** de nos données opérationnelles sont en effet un impératif : les données sensibles (par exemple les schémas de nos réseaux électriques ou des infos sur nos clients industriels) ne peuvent pas être exposées hors de nos infrastructures. Par ailleurs, **nos environnements IT/OT sont très hétérogènes,** mêlant des protocoles modernes et d'autres très spécifiques au monde industriel (Modbus, OPC-UA, S7COM, IEC-104, etc.).

La solution doit donc 'comprendre' ces protocoles OT et s'adapter à des équipements parfois anciens ou non standards. Enfin, comme beaucoup d'équipes sécurité, **nous devons faire plus avec moins** : le secteur de l'énergie fait face à une pénurie de talents cyber spécialisés en OT, et nous n'avons pas un SOC de cent analystes. **Chaque alerte non pertinente, chaque faux positif peut nous faire perdre un temps précieux. Il nous fallait donc un outil qui filtre et priorise intelligemment les alertes, s'intègre à nos processus existants (ITSM, workflows SOC) et automatise autant que possible les tâches sans valeur ajoutée.** L'objectif final : renforcer significativement la sécurité sans alourdir la charge opérationnelle, ni nécessiter une armée d'experts difficile à mobiliser.

03 POURQUOI AVOIR CHOISI DE DÉPLOYER UNE PLATEFORME NDR ?

Il est vite apparu que **sécuriser uniquement nos postes de travail et serveurs (via des EPP, EDR ou IDS/IPS) ne suffisait pas,** surtout dans un environnement industriel. Une grande partie des attaques avancées transitent ou se manifestent d'abord sur le réseau. Or, sur les automates industriels et autres équipements OT, on ne peut pas toujours installer d'agent de sécurité, et les journaux d'événements sont parfois inexistants. Nous avions besoin d'une visibilité globale, couvrant à la fois le réseau IT et les réseaux OT, pour détecter les menaces avant qu'elles n'impactent nos systèmes. **Le NDR s'est imposé car il analyse en continu le trafic sur l'ensemble de nos segments (du siège jusqu'aux usines et aux postes de transformation) et peut identifier des comportements suspects dès les premiers signaux faibles.**

Par exemple, une machine compromise qui cherche à se déplacer latéralement ou un logiciel malveillant inconnu qui communique vers l'extérieur peuvent être repérés grâce aux schémas de trafic inhabituels, même si les attaques utilisent du chiffrement ou des techniques furtives.

En résumé, le NDR comble le « trou noir » qui subsistait entre l'IT et l'OT : il surveille ce que nous ne voyions pas auparavant. Cette approche nous permet d'anticiper les attaques plutôt que de simplement réagir après coup. En intégrant la solution NDR à notre écosystème cyber existant (SIEM, EDR,etc.), **nous construisons progressivement une stratégie XDR unifiée**, fondée sur des solutions best of breed. Cette approche nous permet de détecter les menaces plus en amont et de les traiter avec une efficacité accrue, en tirant le meilleur de chaque technologie spécialisée.

SECTEUR D'ACTIVITÉ
Opérateur régional du secteur de l'énergie

COLLABORATEURS
~2 000
employés

NOMBRE DE SITES SUPERVISÉS
Une trentaine de sites critiques incluant centrales de production, postes sources, centres de contrôle régionaux, sièges administratifs et installations sensibles.

PARC INFORMATIQUE ET INDUSTRIEL
Environ 4 000 postes de travail et serveurs répartis sur l'ensemble du territoire, plusieurs centaines d'équipements OT (automates, capteurs, systèmes SCADA, relais haute tension, systèmes de télégestion), réseaux hybrides IT/OT intégrant des protocoles industriels variés (Modbus, IEC-104, OPC-UA, S7COM, etc.), infrastructure réseau segmentée, connectée à des environnements distants parfois isolés.

04

COMMENT S'EST DÉROULÉ LE DÉPLOIEMENT DE LA PLATEFORME NDR, ET COMMENT S'INTÈGRE-T-ELLE DANS VOTRE ENVIRONNEMENT ?

Le déploiement s'est fait de manière **progressive** et **maîtrisée.** Nous avons commencé par équiper un périmètre pilot - une de nos centrales de production électrique - afin de valider l'efficacité et l'innocuité de la solution en conditions réelles. Concrètement, des sondes ont été installées sur les segments réseau stratégiques (IT et OT), alimentées via des TAP qui recopient passivement le trafic en temps réel. **L'installation matérielle s'est faite sans interruption de service : en quelques heures, les capteurs étaient en place et commençaient à analyser les flux.** La plateforme NDR de Gatewatcher a la particularité de pouvoir être déployée on-premise de bout en bout, ce qui correspondait parfaitement à nos exigences de souveraineté. Nous hébergeons l'orchestrateur et la console de gestion centralisée dans notre datacenter principal, ce qui nous assure que toutes les données restent sous notre contrôle. Une fois le pilote concluant (avec déjà des détections intéressantes dès les premiers jours), nous avons étendu le NDR à l'ensemble de nos sites critiques : postes source, centres de contrôle régionaux, sièges et quelques installations sensibles. L'**intégration** avec notre écosystème s'est révélée fluide.

Par exemple, le NDR envoie ses alertes agrégées vers notre SIEM existant, et s'interface via API avec certains outils maison de supervision. Nous avons également enrichi les informations sur les postes/utilisateurs liés aux alertes grâce à l'annuaire Active Directory, ce qui facilite la contextualisation. **Aujourd'hui, la console Cockpit™ nous permet de tout piloter de manière unifiée : on y voit en temps réel l'état de chaque sonde, les incidents en cours, et on peut zoomer sur n'importe quel site ou segment réseau depuis un seul écran.** C'est un vrai plus pour nos opérations, surtout avec une équipe distribuée entre IT et OT : chacun accède aux données dont il a besoin via un outil commun, sans cloisonnement.

“C'est un vrai plus pour nos opérations, surtout avec une équipe distribuée entre IT et OT : chacun accède aux données dont il a besoin via un outil commun, sans cloisonnement.

05

QUELLES FONCTIONNALITÉS DE LA PLATEFORME UTILISEZ-VOUS LE PLUS ET POURQUOI ?

Nous exploitons pleinement les différentes composantes de la plateforme NDR. Les moteurs de détection basés sur une approche multi-vectorielle, sont bien sûr au cœur du dispositif : **ils analysent l'ensemble des flux (jusqu'aux protocoles industriels ésotériques) et déclenchent des alertes dès qu'un comportement sort de la normale ou correspond à une technique d'attaque connue.** Ce qui nous a impressionnés, c'est sa capacité à détecter y compris des anomalies sur des communications chiffrées ou des attaques « fileless » difficiles à repérer autrement, y compris via nos solutions existantes. En ce qui concerne l'analyse fine du trafic, nous dépendons essentiellement de DEEP VISIBILITY. Il nous donne **une visibilité totale sur qui communique avec qui, sur quel protocole, à quel moment.** Par exemple, lors d'investigations, nos analystes peuvent remonter dans l'historique des métadonnées réseau et **cartographier** en un clic toutes les métriques clés d'un équipement OT (activité des hôtes, la latence, les protocoles TCP/UDP) sur les 30 derniers jours, très utile pour comprendre la portée d'un incident ou déceler des mouvements latents.

La dimension **Threat Intelligence intégrée à la plateforme est un vrai atout :** elle enrichit nos alertes NDR. Côté exploitation quotidienne, l'interface COCKPIT est très appréciée de l'équipe SOC. **Elle consolide les alertes en incidents, calcule un score de risque pour chaque incident, et offre des vues personnalisées.** Par exemple, notre équipe IT peut filtrer sur les incidents affectant le SI bureautique, tandis que l'équipe OT surveille les alertes concernant les automatismes, tout en travaillant sur la même plateforme collaborative. Enfin, en parallèle, nous commençons depuis peu à tirer parti de l'orchestration avec REFLEX. Certaines actions de réponse simples sont d'ores et déjà automatisées via des playbooks :

par exemple,

isoler automatiquement un poste infecté du réseau dès que le NDR détecte une compromission critique, ou pousser une règle de blocage sur nos firewalls en cas de détection d'une IP malveillante. Cette automatisation est encore partielle (nous l'activons sur des cas bien définis), mais elle augure d'un gain de temps énorme sur la remédiation des menaces récurrentes.

06

POURQUOI AVOIR CHOISI GATEWATCHER POUR RÉPONDRE À CES ENJEUX ?

Après une phase d'étude de marché et de tests, Gatewatcher s'est distingué sur plusieurs points critiques pour nous. D'abord, c'est un acteur français, offrant une solution souveraine sans dépendance à des infrastructures hors de notre contrôle. Pour un opérateur sensible comme nous, c'était un gage de confiance supplémentaire, d'autant que la solution a été conçue dès le départ en accord avec les bonnes pratiques de l'ANSSI, ce qui **facilite notre mise en conformité.** Ensuite, la technologie NDR de Gatewatcher a prouvé sa pertinence technique lors du pilote : la combinaison de l'intelligence artificielle, d'analyses statiques et dynamiques, et du feed de Threat Intelligence natif a permis de détecter des menaces que d'autres outils n'avaient pas remontées. Nous avons particulièrement apprécié l**a vision à 360°** que propose la plateforme: elle couvre l'intégralité du réseau, du cloud à l'usine, ce qui n'était pas le cas de certaines solutions concurrentes plus focalisées sur l'IT traditionnel. Un autre facteur de choix a été **la flexibilité d'intégration.** Gatewatcher s'interface aisément avec nos systèmes existants, via des API ouvertes et des connecteurs standard. **Plutôt que de nous imposer une « boîte noire » rigide, ils nous ont fourni une brique qu'on a pu intégrer dans notre architecture globale sans tout repenser.** Par ailleurs, la plateforme est évolutive : elle regroupe non seulement le NDR, mais aussi des modules CTI et peut interagir avec toutes nos solutions existantes.

En choisissant Gatewatcher, on a le sentiment d'investir dans un partenariat long terme plus qu'un simple produit : les équipes de Gatewatcher nous ont accompagnés de près lors du déploiement, et continuent de le faire, en comprenant bien nos enjeux métiers (notamment la composante OT). Cette proximité et cette expertise secteur ont clairement pesé dans la balance. Enfin, il faut le souligner, Gatewatcher est déjà présent chez d'autres acteurs critiques en France et en Europe – savoir que la solution fait ses preuves dans des environnements comparables au nôtre (énergie, défense, transport…) a fini de nous convaincre que c'était le bon choix pour répondre à nos défis.

07

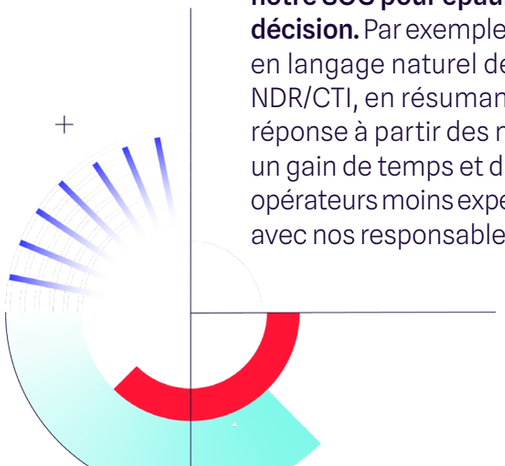
QUELS BÉNÉFICES CONCRETS AVEZ-VOUS CONSTATÉS DEPUIS LA MISE EN PLACE DU NDR ?

Ils sont nombreux. Le premier bénéfice, immédiat, c'est la **visibilité.** Dès les premiers jours, nous avons découvert des éléments qui nous échappaient auparavant : des équipements oubliés communiquant sur le réseau, des flux insoupçonnés entre certaines sous-stations et des serveurs, ou encore des erreurs de configuration qui, sans être malveillantes, représentaient un risque pour la sécurité. Pouvoir 'faire la carte' de tout notre trafic, notamment en OT, nous a permis de remédier à ces angles morts très vite. Sur le plan de la détection des menaces, la plateforme a prouvé son efficacité à plusieurs reprises. Par exemple, peu de temps après le déploiement global, une alerte NDR a mis en lumière un échange inhabituel entre un poste bureautique et un automate industriel de régulation. Ce comportement anormal a été instantanément classé à haut risque par l'outil. En investiguant, nous avons identifié un malware inconnu qui tentait de pénétrer le réseau OT. Sans le NDR, cette activité furtive serait passée inaperçue. De manière générale, notre **temps de réaction** s'est considérablement amélioré : **on est capables de passer du premier signal faible au traitement d'une machine en l'espace de quelques minutes, là où auparavant il nous fallait des heures ou des jours pour remonter la piste d'une intrusion.** Un autre gain notable concerne la charge du SOC. La **priorisation intelligente des alertes par le NDR a réduit le bruit de fond** : nos analystes ne sont plus noyés sous des centaines d'alertes sans gravité. Le nombre de faux positifs a baissé drastiquement (nous l'estimons à plus de 30 % de réduction sur certaines catégories d'alertes). Concrètement, cela signifie que l'équipe se concentre sur les vraies menaces, et cela se ressent en termes de fatigue opérationnelle : moins d'alertes redondantes à traiter, c'est plus de temps pour l'investigation approfondie et la chasse proactive. Enfin, le NDR nous a aidés à **mieux communiquer sur la cybersécurité en interne.** Les tableaux de bord et rapports générés ont servi à démontrer aux dirigeants et aux équipes métiers la réalité des menaces et l'efficacité des mesures prises. Cette transparence a renforcé la confiance globale dans notre démarche cyber, ce qui est un bénéfice plus intangible mais précieux : aujourd'hui, la cybersécurité est perçue comme un atout pour la pérennité de nos opérations, et non plus comme un centre de coût opaque.

08

QUELLES SONT LES PROCHAINES ÉTAPES POUR CONTINUER À RENFORCER VOTRE CYBERSÉCURITÉ ?

Nous souhaitons capitaliser sur l'élan donné par le NDR et aller encore plus loin dans la **réactivité** et la **proactivité.** La prochaine grande étape, déjà en cours, c'est l'extension de l'automatisation de certains pans de nos activités via Reflex™. Nous travaillons à enrichir nos playbooks de réponse automatique afin de gérer instantanément les menaces courantes : par exemple, isoler un segment OT si un comportement critique y est détecté, ou déclencher des analyses forensiques immédiates dès qu'une alerte se confirme. L'idée est d'accélérer encore le MTTR pour frôler le temps réel sur les actions de remédiation, tout en laissant aux analystes le contrôle final sur les décisions stratégiques. En parallèle, nous suivons de près les avancées en matière d'IA appliquée à la cybersécurité. **GAIA,** l'assistant cybersécurité piloté par IA générative, nous intéresse particulièrement. À terme, nous envisageons d'**intégrer GAIA à notre SOC pour épauler nos équipes dans l'analyse et la prise de décision.** Par exemple, GAIA pourrait aider un analyste en formulant en langage naturel des recherches complexes dans les données NDR/CTI, en résumant un incident ou en suggérant des pistes de réponse à partir des millions d'IoC connus. Cela pourrait apporter un gain de temps et d'efficacité non négligeable, surtout pour nos opérateurs moins expérimentés, et faciliter le partage d'information avec nos responsables métier sous une forme compréhensible.



*Bénéfices de la plateforme NDR_*

Détecter les menaces en temps réel
sur l'ensemble du réseau, avant qu'elles n'impactent les systèmes

Surveiller tout le trafic (IT et OT)
pour une visibilité complète et une cartographie dynamique des communications

Enrichir automatiquement
le contexte des alertes grâce à l'IA et à la CTI (indicateurs de menace mis à jour en continu)

Prioriser les incidents critiques
et filtrer les faux positifs pour concentrer les analystes sur ce qui compte vraiment

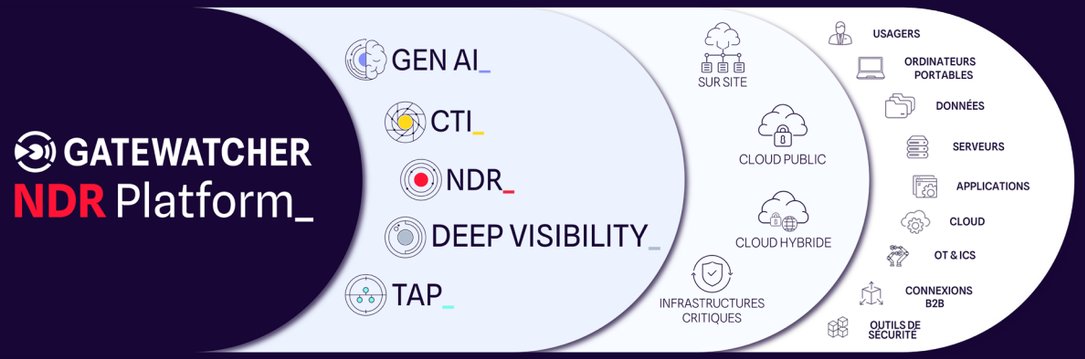
Automatiser la réponse
aux attaques (isolement d'hôtes, blocage d'IP, etc.) afin d'accélérer la remédiation et réduire le temps de réponse

Intégrer la solution
de façon transparente à l'écosystème existant (SIEM, EDR, pare-feu, SOC...) pour une protection unifiée et efficace

*À propos_*

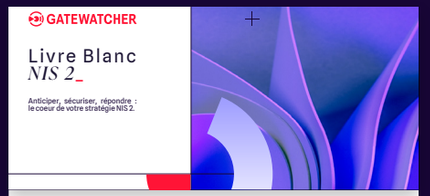
Leader de la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux des entreprises et des institutions publiques, y compris les plus critiques. La plateforme NDR Gatewatcher (Network Detection and Response), combine intelligence artificielle, techniques d'analyse dynamiques et comportementales et Cyber Threat Intelligence (CTI) contextualisée. Elle offre ainsi une visibilité unifiée et complète, une détection et une cartographie des systèmes en temps réel et une réponse globale, automatisée et priorisée face aux attaques. Déployée sur infrastructures cloud, on-premise ou sensibles, et compatible avec les environnements IT, OT et IoT, elle sécurise l'ensemble des actifs critiques et simplifie les opérations grâce à son assistant IA intégré. Gatewatcher allie puissance technologique et sérénité opérationnelle, afin d'aligner la cybersécurité sur vos objectifs business.

Contactez-nous

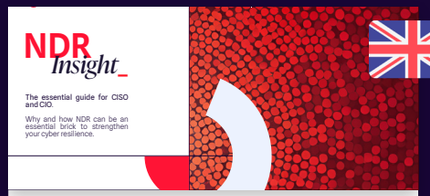


Envie d'en *savoir plus ?_*

[REPLAY]
Gatewatcher & MCS : Simplicité de bout en bout, du déploiement à la prise en main



[LIVRE BLANC]
Livre Blanc NIS 2 – anticiper, sécuriser, répondre : le cœur de votre stratégie NIS 2



[GUIDE]
Guide NDR: l'essentiel pour les DSI, RSSI et C-suite