GATEWATCHER

Livre blanc

Risques cyber IT/OT :
L'ère de l'anticipation

From detection
*to decision_*

Sommaire_

1 Contexte et nouveaux enjeux de la convergence IT/OT_

2 Cas d'usage_

3 Voir, comprendre, anticiper : Une nouvelle approche de la cybersécurité OT_

01 CONTEXTE ET NOUVEAUX ENJEUX DE LA CONVERGENCE IT/OT_

Convergence IT-OT

Votre plus grande force, votre pire vulnérabilité

Depuis plus d'une décennie, la transformation numérique redessine l'efficacité opérationnelle. L'intégration des technologies de l'information (IT) au cœur des systèmes opérationnels (OT), lignes de production, réseaux énergétiques ou plateaux techniques hospitaliers, est devenue un levier majeur de performance.

Maintenance prédictive plus fine, gestion des stocks en temps réel, personnalisation accrue des soins : **la convergence IT/OT génère des gains tangibles dans tous les secteurs**. Elle permet d'accroître la productivité, d'améliorer le pilotage des opérations et de réagir plus rapidement aux aléas.

Mais cette convergence brise un principe fondamental :
Celui de **l'isolement**. En connectant des actifs critiques, autrefois protégés par un cloisonnement physique (air gap), les organisations ont involontairement ouvert une véritable boîte de Pandore cyber.

> *Une cible stratégique au cœur des tensions mondiales*

Les risques encourus sont d'autant plus élevés que cette convergence intervient dans un contexte géopolitique de tensions accrues. Les infrastructures industrielles, énergétiques, de transport ou encore de santé sont désormais devenues des cibles prioritaires.

Les attaques ne visent plus seulement l'exfiltration de données, mais bien le sabotage pur et simple des opérations : paralyser un réseau de transport, altérer la distribution d'énergie, interrompre une chaîne de production, bloquer les systèmes d'urgence d'un hôpital... Quel que soit le mode opératoire; espionnage, sabotage, chantage, destruction; **frapper l'OT, c'est frapper au cœur de la souveraineté, perturber l'économie, affaiblir la concurrence, déstabiliser des activités essentielles, voire mettre en danger des populations.**

> *Industrialisation de la menace*

Et le risque est d'autant plus grand que les modes opératoires des cyberattaquants ont franchi un nouveau palier : portées par l'essor de l'intelligence artificielle, **les attaques s'automatisent, se spécialisent et gagnent en vitesse**. Des capacités autrefois réservées à des acteurs étatiques deviennent progressivement accessibles à un nombre croissant d'attaquants.

Face à cette menace à « haute fréquence », **les solutions de sécurité traditionnelles**, déjà souvent aveugles sur les protocoles industriels, **sont dépassées**.

> *Reprendre le contrôle : une condition de survie opérationnelle*

Dans ce contexte, reprendre le contrôle n'est plus une option, mais une nécessité absolue. Sans une maîtrise fine des environnements OT, les organisations s'exposent à une perte brutale de leur capacité à produire, à distribuer, à opérer des services critiques ou à soigner.

Il ne s'agit plus seulement de protéger des systèmes séparés, mais de gérer l'ensemble du réseau IT/OT. Avoir une vision complète de ce qui s'y passe est désormais essentiel pour repérer les premiers signes d'attaque, détecter les menaces furtives et reprendre le dessus face aux cybercriminels.

Car dans un environnement IT/OT interconnecté, quand le numérique flanche, c'est toute votre activité opérationnelle qui s'arrête.

Le nombre d'incidents cyber ayant entraîné une interruption physique de l'activité a été multiplié par trois entre 2021 et 2025.

Source : Gartner

74% des entreprises industrielles admettent n'avoir qu'une visibilité limitée, voire nulle, sur les activités au sein de leur réseau OT.

Source : Rapport SANS Institute sur la sécurité ICS/OT

Le saviez-vous ?

+ de 60 % des incidents affectant des environnements industriels trouvent leur origine dans les systèmes IT ou dans la chaîne d'approvisionnement (prestataires, partenaires).

Les attaquants privilégient ces points d'entrée indirects, souvent moins protégés, pour atteindre leurs cibles finales.

Sources : IBM X-Force / Dragos

Scénarios de rebond :

Quand l'IT ouvre *la porte à l'ennemi*

Contrairement aux idées reçues, les environnements OT sont rarement la porte d'entrée des attaques. Ils en sont la cible finale. Dans son dernier panorama de la cybermenace, l'ANSSI le confirme : **les attaquants privilégient des scénarios de rebond, en s'implantant d'abord dans le SI avant de progresser vers les environnements industriels**. Les points d'entrée ne manquent pas : postes utilisateurs, accès distants, comptes compromis, connexions de prestataires lors d'opérations de maintenance.

Or, parce qu'ils sont ouverts pour faire tourner l'activité au quotidien, ces accès échappent souvent aux contrôles appliqués au reste du SI. Une fois dans la place, les attaquants explorent les interconnexions et repèrent aisément les passerelles vers l'OT. **La compromission d'un seul compte administratif suffit alors, en quelques étapes, à faire basculer toute une chaîne de production.**

OT vs IT : *Deux logiques* en collision

Les environnements OT ont été conçus pour fonctionner à huis clos. Leur priorité : la continuité de production et/ou de service. Peu exposés, rarement modifiés, ils reposaient sur des architectures fermées où l'isolement constituait une protection implicite.

À l'inverse, les systèmes IT ont été pensés pour échanger : ouverts, interconnectés, en évolution permanente pour répondre aux besoins des utilisateurs et de l'activité.

Leur convergence a fait entrer ces deux logiques en collision. **En créant des ponts numériques entre ces environnements, les entreprises ont supprimé la frontière physique qui protégeait les systèmes industriels.** Ce qui relevait de deux mondes distincts devient un espace commun, où les contraintes d'ouverture de l'IT s'appliquent désormais à des systèmes qui n'ont pas été conçus pour y faire face.

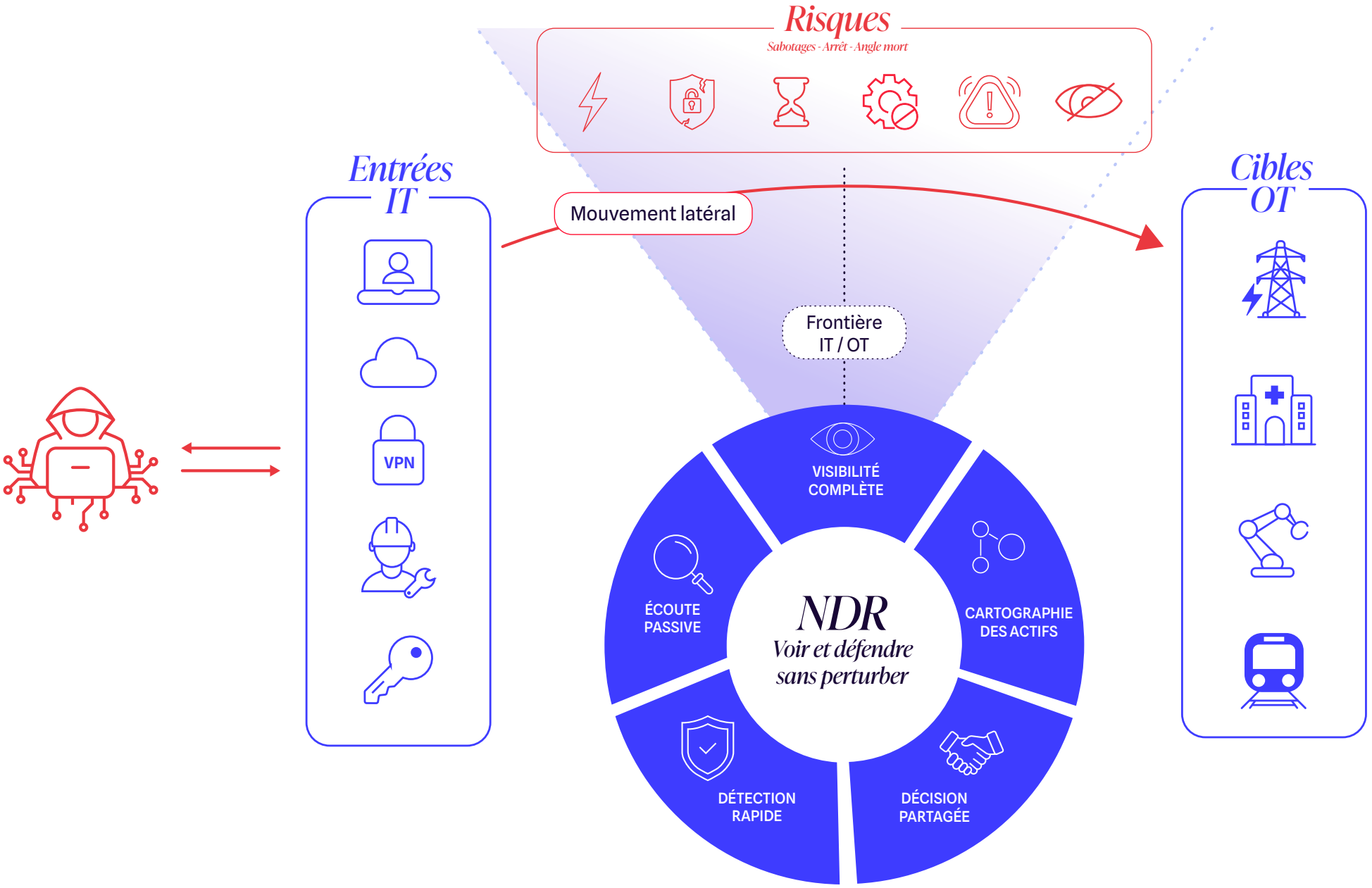
Le saviez-vous ?

Un automate industriel est conçu pour fonctionner 20 à 30 ans, là où un serveur IT est renouvelé tous les 3 à 5 ans en moyenne.

Cette distorsion crée des failles structurelles : une part importante des environnements industriels repose encore sur des systèmes ou protocoles « legacy » difficilement sécurisables.

Sources : ANSSI

Schéma d'une attaque sur un périmètre convergé IT/OT



Le défi du Legacy
Sécuriser sans interrompre la production

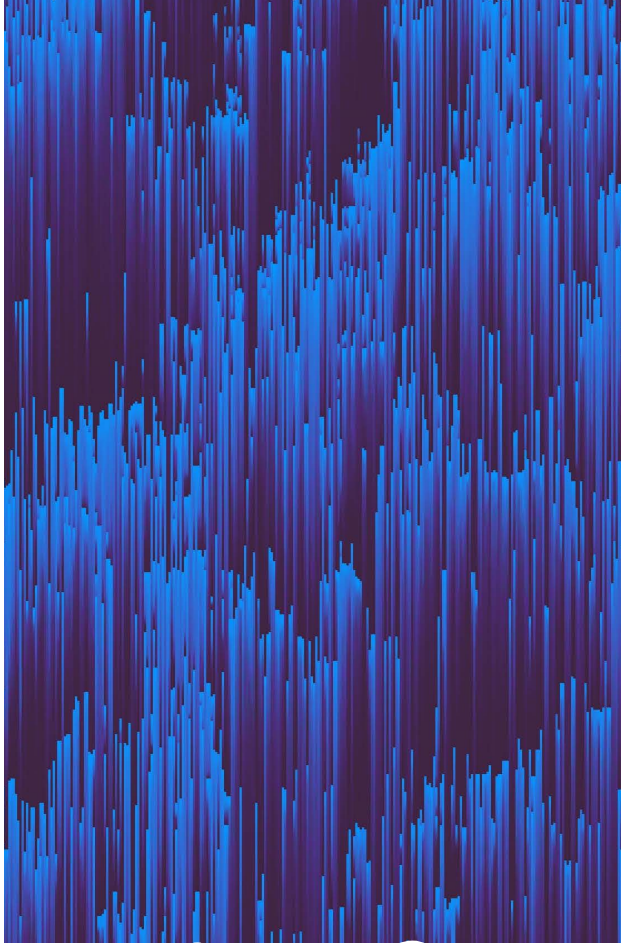
La stabilité de l'OT est sa plus grande force opérationnelle, mais elle devient également son principal défi cyber. **Conçus pour fonctionner pendant vingt à trente ans, les environnements industriels évoluent à un rythme radicalement différent de celui des systèmes IT.** Les mises à jour y sont rares, les fenêtres de maintenance limitées et chaque modification doit être soigneusement évaluée afin d'éviter tout impact sur la production. Dans un contexte de convergence IT/OT, ce rythme lent se retrouve confronté à des menaces capables d'évoluer, de se propager et d'agir en quelques minutes seulement.

Cette différence de temporalité crée une tension structurelle : **comment protéger des équipements critiques qu'il est parfois impossible de patcher, de redémarrer ou même de scanner sans risque pour l'activité ?** Dans l'industrie, l'énergie, les transports ou la santé, arrêter un système pour le sécuriser n'est souvent pas envisageable. La cybersécurité doit donc s'adapter aux contraintes opérationnelles et non l'inverse.

C'est précisément dans ce contexte que **l'approche NDR (Network Detection and Response) prend tout son sens.** Contrairement aux solutions de sécurité qui interagissent directement avec les équipements et dont l'analyse génère du trafic, **le NDR repose sur une écoute totalement passive du réseau.** Grâce à des mécanismes de duplication des flux (TAP réseau, ports miroir/SPAN ou infrastructures de visibilité dédiées), une copie des communications est envoyée vers la plateforme d'analyse. Les équipements industriels continuent ainsi à fonctionner normalement tandis que le NDR observe, décode et analyse les échanges en temps réel **sans jamais injecter le moindre paquet sur le réseau de production.**

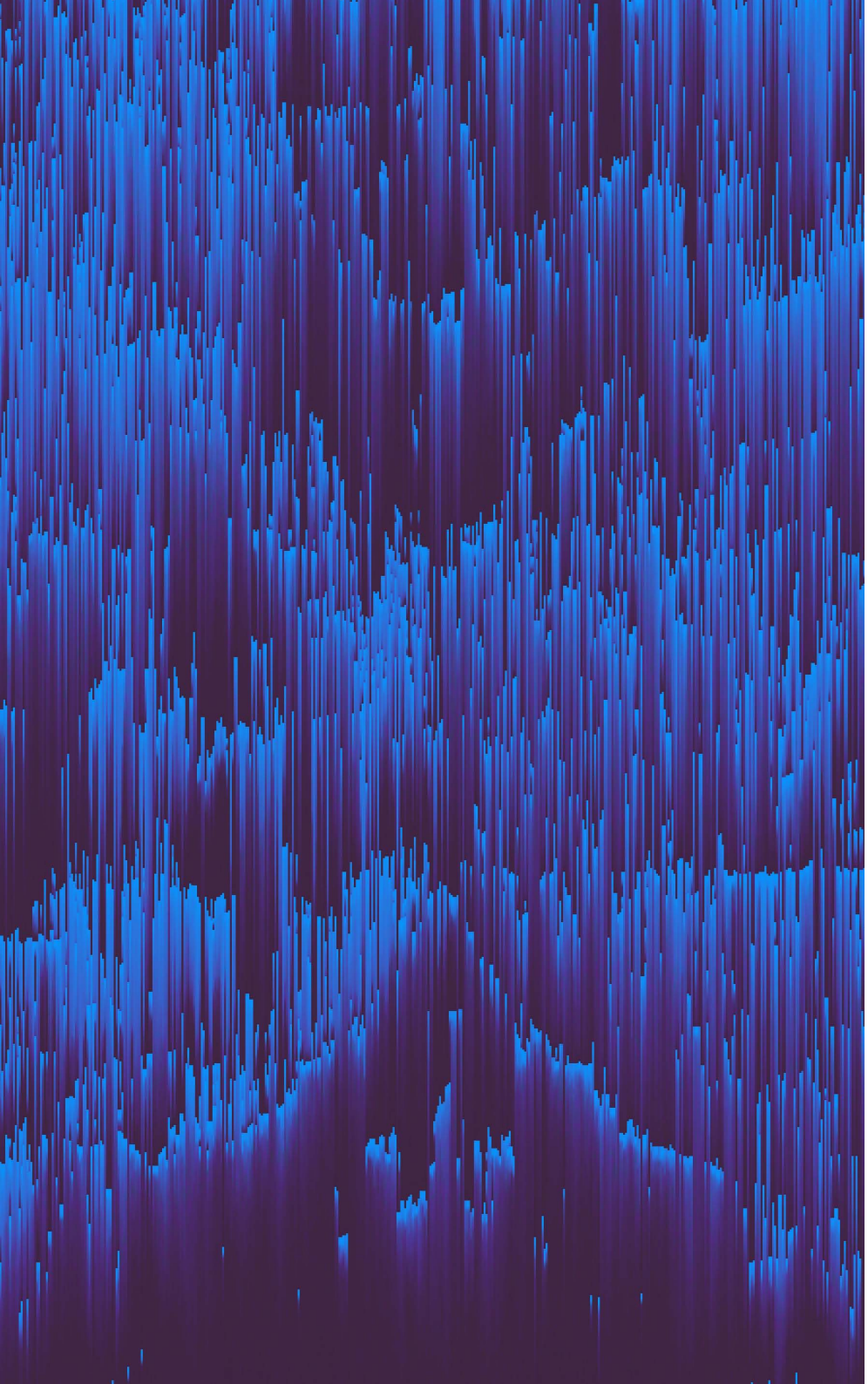
Cette approche permet d'obtenir une visibilité exhaustive sur les actifs, les protocoles industriels et les communications IT/OT sans créer de risque opérationnel. Elle est particulièrement adaptée aux environnements avec une forte presence d'équipement «legacy» où la moindre perturbation peut entraîner un arrêt de service ou affecter un processus critique.

Déployable aussi bien sur site que dans des architectures hybrides ou cloud, le NDR s'intègre aux infrastructures existantes sans modifier leur fonctionnement. Il offre ainsi une capacité de détection avancée, compatible avec les exigences de disponibilité des environnements critiques et avec les cadres réglementaires tels que NIS 2 ou la norme IEC 62443.



Le saviez-vous ?

Selon Gartner, **+ de 75 %** des environnements OT contiennent des équipements qui ne peuvent pas être mis à jour sans interruption de production.
Résultat : de nombreuses vulnérabilités connues restent exploitables pendant plusieurs années.



On ne protège pas *ce que l'on ne voit pas...*

Dans de nombreux environnements industriels, l'enjeu ne se limite plus à détecter une intrusion, mais à comprendre la réalité profonde des échanges réseau. **Les flux OT reposent sur des protocoles métiers spécifiques, souvent opaques pour les outils de sécurité IT traditionnels** : ils peinent à les décoder. Les interactions entre équipements restent souvent mal documentées, et certaines communications échappent complètement à la supervision.

Résultat : une partie significative de l'activité réseau reste dans l'ombre, masquant des signaux faibles ou des menaces furtives.

Dans un environnement interconnecté, l'absence de visibilité ne constitue pas seulement un manque d'information : elle devient un risque majeur pour la continuité d'activité.

Le saviez-vous ?

Dans les environnements industriels, jusqu'à **90 %** des actifs ne sont pas correctement inventoriés ou supervisés en temps réel.
Sans visibilité complète, il devient impossible d'identifier précisément les flux ou les comportements anormaux.

Sources : Gartner / Nozomi Networks

Sortir de la paralysie décisionnelle : Le défi de la *convergence humaine*

Les systèmes IT et OT convergent en terme de capacité a communiquer entre eux mais ils restent distincts techniquement, les organisations, elles, restent trop souvent prisonnières de leurs silos historiques. D'un côté, les équipes IT, gardiennes de la sécurité, cultivent l'agilité : mises à jour constantes, correctifs immédiats et primauté de la confidentialité.

De l'autre, les équipes OT, garantes de la continuité de production, vivent au rythme de la disponibilité absolue. Pour un responsable d'usine, un système qui fonctionne est un système auquel on ne touche pas.

Cette divergence crée une tension naturelle : **là où l'expert cyber voit une vulnérabilité critique à patcher d'urgence, l'opérationnel voit un risque d'arrêt de production.**

Ce choc des perceptions constitue un point de fragilité majeur. En cas d'incident, les lignes de décision se brouillent : qui est légitime pour agir, à quel moment, et selon quels critères ? Tandis que les équipes IT cherchent à contenir la menace, les équipes OT s'attachent à préserver la continuité.

Cette divergence de perception est d'autant plus problématique que les experts IT maîtrisent rarement les spécificités des environnements industriels et inversement. Ce manque de transversalité dans les compétences **limite la capacité à appréhender une situation dans sa globalité et à prendre les bonnes décisions au bon moment.**

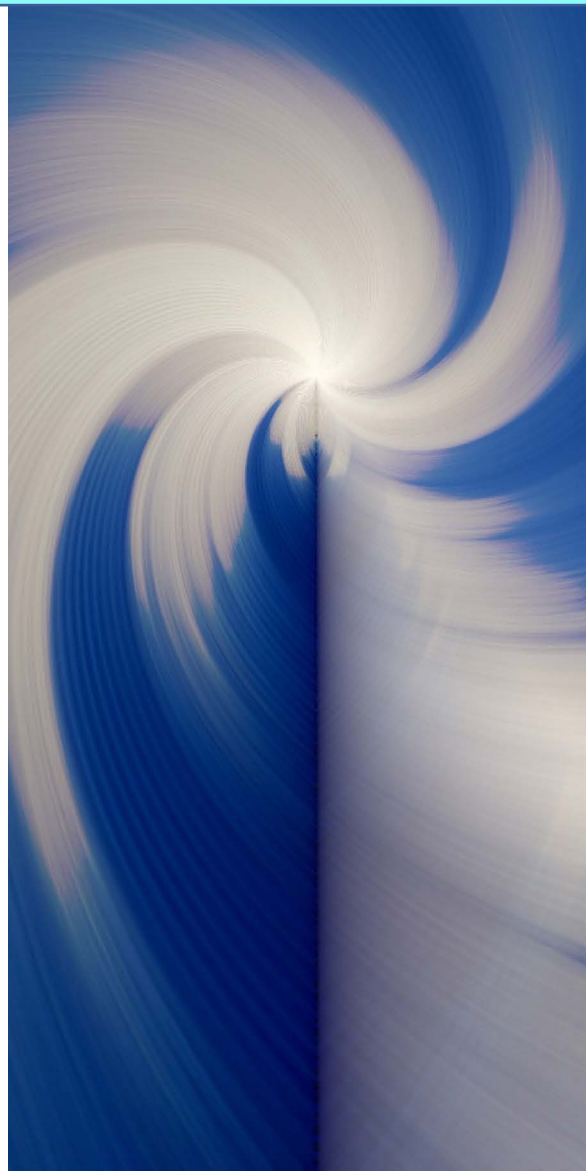
Dit autrement, le succès de la convergence suppose aussi une transformation organisationnelle profonde avec des équipes, des processus et des responsabilités alignés autour d'un risque désormais commun. Sans cette convergence humaine, les meilleures solutions techniques se heurteront toujours au mur de la paralysie décisionnelle.

Sécuriser l'OT, c'est briser les silos, y compris humains, pour faire de la cybersécurité un levier de résilience au service de la production, et non une contrainte imposée par l'informatique.

Le saviez-vous ?

+ de 60 % des organisations industrielles, les responsabilités IT et OT restent cloisonnées, avec des chaînes de décision distinctes.

Sources : Deloitte / IBM Security



02 CAS D'USAGES_

ÉNERGIE : LA RÉSILIENCE SOUS TENSION NUMÉRIQUE_

L'énergie à l'heure des *réseaux intelligents*

Dans le secteur de l'énergie, la convergence IT/OT n'est plus une simple option d'optimisation technique, elle est le moteur même de la transition énergétique. L'émergence des **Smart Grids**, l'intégration massive des énergies renouvelables distribuées et le pilotage à distance des postes sources ont transformé l'infrastructure en un organisme de données vivant. Cette mutation répond à une exigence métier forte : équilibrer en temps réel la production et la consommation sur des réseaux de plus en plus complexes. Mais cette hyper-connectivité brise l'isolement historique des systèmes industriels et crée une surface d'attaque sans précédent.

Désormais, les protocoles spécifiques au secteur, tels que l'IEC 61850 pour l'automatisation des postes électriques, l'IEC 104 ou le DNP3 pour la téléconduite, circulent sur des réseaux interconnectés avec le SI de gestion.

Le risque majeur a changé de nature : **une faille initiée sur un poste administratif ou un accès de maintenance distant peut se propager jusqu'aux automates de protection (IED)**. Pour les acteurs de l'énergie, l'enjeu est de protéger des actifs critiques dont la défaillance ne se traduit pas seulement par une perte de données, mais par une rupture de charge nationale, une déstabilisation de la fréquence du réseau ou des dommages physiques irréversibles sur des transformateurs haute tension, piliers de la souveraineté énergétique.

Scénarios d'attaques récurrents

Sabotage furtif via un relais de protection

Un attaquant compromet une session de maintenance pour modifier les seuils de déclenchement d'un relais.

Impact : L'équipement reste opérationnel en apparence, mais devient incapable de protéger le réseau lors d'une surtension réelle, provoquant un effet cascade potentiellement dévastateur.

Aveuglement du Dispatching (SCADA Hijacking)

Injection de fausses trames de mesures dans le système de supervision pour simuler une charge normale.

Impact : L'opérateur, trompé par une réalité falsifiée, ne détecte pas une surcharge critique, menant à une instabilité de fréquence et un délestage non maîtrisé.

Ransomware ciblé sur les serveurs de téléconduite

Chiffrement des serveurs gérant l'interface homme-machine (IHM) du centre de contrôle.

Impact : Perte totale de capacité de pilotage à distance des installations distribuées, forçant un passage en mode dégradé manuel coûteux et risqué.

Reprendre la maîtrise d'un réseau sans frontières

> Décoder l'intention derrière la commande industrielle_

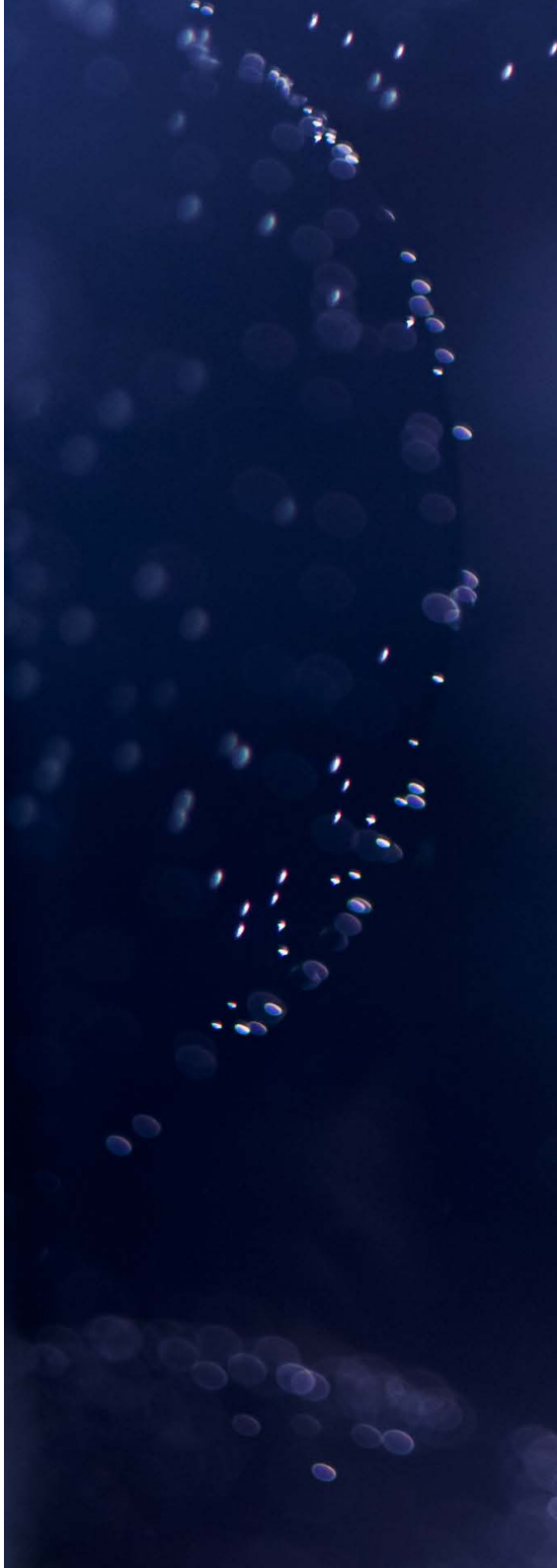
La détection d'intrusion ne suffit plus : il faut analyser la sémantique des échanges au cœur des protocoles métier pour distinguer l'opération de maintenance légitime d'une tentative de sabotage furtive et repérer/bloquer une commande atypique avant qu'elle n'altère la stabilité du réseau électrique.

> Unifier la visibilité sur une infrastructure éclatée_

Le secteur s'appuie sur des actifs très dispersés, souvent administrés à distance par des tiers. Reprendre la main suppose de cartographier en continu les flux entre le SI, les systèmes de téléconduite et les équipements de terrain (IED), afin de repérer tout mouvement latéral suspect et d'éviter qu'un segment vieillissant ne déclenche un effet domino. Décoder l'intention derrière la commande industrielle.

> L'écoute passive comme garantie de stabilité_

Quand l'équilibre production-consommation se joue à la seconde, l'outil de sécurité ne doit surtout pas devenir lui-même un facteur de risque. Une approche NDR par écoute passive surveille en continu sans toucher aux flux de protection critiques : elle capte les signaux faibles, soulage les équipes de conduite et renforce, au passage, la souveraineté énergétique.



Énergie

L'ancrage sectoriel de Gatewatcher

Références clients_

Suez, Veolia, RTE, Dunkerque LNG Groupe Fluxis, Eau de Paris, Eau du Grand Lyon, Eau de Strasbourg et Eau de Bordeaux.

Protocoles industriels couverts_

IEC 104, DNP3, Modbus, S7, OPC UA, MQTT, ENIP/CIP (BACnet uniquement pour la GTB/efficacité énergétique des bâtiments).
> Exclus : DICOM et HL7 (santé), Pcom (automate générique).

Équipements / fabricants OT_

Siemens (Siemens Energy), Hitachi Energy (ex-ABB Power Grids), ABB, Schneider Electric, GE Vernova, Schweitzer Engineering Laboratories (SEL), Eaton, Emerson, Honeywell, Rockwell Automation (Allen-Bradley), SMA, Huawei, SolarEdge, Fronius..

SANTÉ :
PROTEGER LE SOIN
À L'ÈRE DE L'HOPITAL NUMÉRIQUE_

Des établissements de santé hyperconnectés

L'établissement de santé moderne est devenu un écosystème hyperconnecté où la frontière entre le système d'information hospitalier (SIH) et le plateau technique s'efface. Scanners, IRM, pompes à perfusion connectées, automates de laboratoire et robots chirurgicaux : ces dispositifs biomédicaux (IoMT) communiquent désormais en continu via les protocoles DICOM ou HL7. **Si cette convergence fluidifie le parcours de soins et accélère le diagnostic, elle transforme chaque équipement médical en une porte d'entrée potentielle pour une cyberattaque.** Dans un hôpital, la menace ne vise pas seulement la confidentialité du dossier patient, elle menace directement l'intégrité de l'acte médical.

Le secteur de la santé est aujourd'hui la cible prioritaire des cyberattaquants pratiquant la « double extorsion ». Le chantage ne porte plus uniquement sur la donnée, mais sur la survie opérationnelle de l'établissement et donc sa capacité à soigner. Un bloc opératoire paralysé ou une imagerie médicale indisponible représentent une perte immédiate et critique pour le patient. **La complexité est d'autant plus grande que ces parcs sont hétérogènes, mêlant des applications cloud dernier cri à des équipements médicaux critiques dotés de systèmes d'exploitation obsolètes qu'on ne peut ni patcher ni isoler sans briser la chaîne de soin.** Dès lors, le succès de cette transformation ne dépend plus de la performance des outils, mais de la capacité de l'organisation à maîtriser les flux nés de cette convergence, pour garantir que l'ouverture des réseaux ne devienne jamais le point de rupture de la prise en charge.

Scénarios d'attaques récurrents

Paralysie du bloc opératoire par mouvement latéral

Un ransomware s'introduit par le SI administratif (via un mail de phishing) et profite de la convergence pour progresser vers la console - le serveur - le systeme. Une passerelle peut servir à la progression du malware mais ne fait pas de supervision des signes vitaux.

Impact : Déconnexion brutale de la surveillance patient en plein acte opératoire, forçant une bascule en mode urgence sans retour vidéo/données.

Altération de l'intégrité diagnostique (Data Tampering)

Un attaquant modifie les métadonnées d'un examen d'imagerie médicale circulant entre le réseau OT (scanner) et le réseau IT (serveur d'archivage PACS).

Impact : Erreur de diagnostic basée sur une image falsifiée ou attribuée au mauvais patient, sans que le personnel soignant ne détecte l'anomalie réseau.

Détournement des équipements techniques (GTB)

Une intrusion sur le réseau de gestion technique du bâtiment (climatisation, pression d'air) via une passerelle Web mal sécurisée.

Impact : Rupture des conditions de stérilité dans les chambres blanches ou les blocs opératoires, rendant le plateau technique inutilisable malgré un SI parfaitement fonctionnel.

Sécuriser le soin sans l'entraver

> Garantir la continuité de soins dans un réseau ouvert_

Dans le secteur de la santé, la cybersécurité n'est plus une discipline de support, mais une composante directe de la sécurité patient. L'arrêt n'est jamais une option. La gestion de la convergence doit donc se traduire par une capacité de détection « silencieuse » et ultra-précise.

> Alerter sur les dérives avant la paralysie du soin_

Des signaux faibles sur le réseau peuvent annoncer une menace passant de l'IT à l'OT biomédical. Détecter une communication inhabituelle ou un flux anormal est essentiel. L'analyse des protocoles spécialisés permet d'intercepter une tentative d'attaque avant que l'équipement ne dérive ou soit endommagé.

> Réduire l'angle mort du parc biomédical_

L'hôpital doit gérer un parc médical mêlant équipements récents et anciens non mis à jour. Une cartographie dynamique permet d'identifier et de surveiller chaque objet connecté. Cette visibilité globale protège contre les failles des dispositifs « Legacy » impossibles à isoler ou corriger.

> Une supervision transparente pour les équipes médicales_

Toute mesure de sécurité qui alourdirait l'accès aux données ou ralentirait un diagnostic met directement en péril la réactivité des équipes soignantes. La réponse à la convergence doit donc être totalement non intrusive.

> *« La détection précoce de comportements inhabituels nous permet aujourd'hui d'anticiper certaines dérives avant qu'elles n'impactent les services de soin. »*
>
> Franck Moussé, RSSI - GHT du Cher

Santé

L'ancrage sectoriel de Gatewatcher

Références clients_

GHT Réunion, CH St Lô, Ch Polynésie française, CHU Nice, GHT Cher, CH Douai, GHT Vaucluse, EFS et Santé Publique France.

Protocoles industriels couverts_

DICOM, HL7 (cœur métier), BACnet et Modbus (GTB, HVAC critique, gaz médicaux), MQTT (dispositifs médicaux connectés / IoMT).
> Exclus : DNP3, IEC 104, S7, ENIP/CIP, Pcom (non spécifiques santé).

Équipements / fabricants OT_

GE HealthCare, Siemens Healthineers, Philips, Canon Medical, Fujifilm Healthcare, Dräger, Medtronic ; pour HL7/SI hospitalier : Epic, Oracle Health (ex-Cerner) ; pour la GTB hospitalière : Siemens, Schneider Electric, Johnson Controls, Honeywell.

« Avec quatre CHU et un très grand nombre d'actifs à superviser, nous avions besoin d'une visibilité globale sur nos environnements IT, OT et biomédicaux. Le NDR de Gatewatcher nous apporte cette vision à 360° et facilite la collaboration entre les équipes cyber et les équipes métiers. Résultat : une meilleure maîtrise de notre surface d'attaque et une capacité de réaction renforcée en cas d'incident. »

Stéphane Duchesne, Directeur des risques - GHT de La Réunion

« Sur certains équipements biomédicaux, on n'a pas toujours la main. Ce sont des solutions packagées : il faut donc trouver des moyens de les sécuriser malgré tout. »

Franck Baibourdian, RSSI - CH Avignon & GHT Vaucluse

INDUSTRIE : SÉCURISER L'USINE 4.0 SANS INTERROMPRE LA LIGNE_

L'industrie connectée face au risque de propagation numérique

Dans la fabrication industrielle, la convergence IT/OT est devenue le pilier central de l'usine du futur. L'intégration de l'Internet des Objets Industriels (IIoT), de l'intelligence artificielle et de la robotique collaborative permet d'atteindre des niveaux de productivité et de flexibilité inédits. Cependant, cette agilité repose sur une interconnexion totale et permanente : **les capteurs de bord de ligne, les automates programmables (API) et les systèmes de gestion de la production (MES) sont désormais directement reliés aux réseaux d'entreprise et aux plateformes cloud de maintenance prédictive.**

Cette transformation alimente l'essor de l'usine 4.0. Maintenance prédictive, robotique collaborative, pilotage énergétique des sites, contrôle qualité automatisé ou jumeaux numériques : **toute l'intelligence industrielle repose désormais sur la circulation continue des données entre les systèmes IT et les équipements OT.** Mais cette hyperconnexion crée aussi une nouvelle dépendance critique : lorsqu'un flux numérique est altéré, c'est l'outil de production physique qui déraille.

Le risque ne se limite plus à l'arrêt d'un poste informatique. **Une compromission peut désormais affecter directement les cadences de fabrication, les paramètres de production, les recettes industrielles ou les systèmes de contrôle commande.** Dans des environnements où les chaînes fonctionnent en flux tendu et où chaque minute d'arrêt représente des pertes considérables, la menace cyber devient un enjeu direct de continuité opérationnelle et de compétitivité.

Cette exposition est aggravée par l'hétérogénéité des technologies. Les usines font cohabiter des équipements récents, connectés au cloud ou supervisés à distance, et des machines en service depuis des décennies, des systèmes fermés, conçus pour durer, désormais confrontés à des menaces qui évoluent à la vitesse de l'IA.

Scénarios d'attaques récurrents_

Sabotage de la qualité (Data Tampering)

Un attaquant infiltre le réseau OT et modifie les paramètres de température ou de pression d'une cuve via le protocole Modbus.

Impact : la production semble normale, mais le produit fini est défectueux ou non conforme, entraînant des rebuts massifs, des rappels de produits et un risque juridique majeur.

Ransomware industriel

Chiffrement des serveurs MES ou des stations d'ingénierie qui pilotent les automates de la ligne de production.

Impact : paralysie totale de l'usine. Contrairement à l'IT, la restauration ici est complexe car elle peut nécessiter un recalibrage physique de chaque machine.

Espionnage de la propriété intellectuelle

Captation des fichiers de configuration des robots ou des procédés de fabrication transmises via le réseau vers les automates.

Impact : fuite critique de secrets de fabrication critiques vers la concurrence, affaiblissant durablement l'avantage concurrentiel de l'entreprise.

Reprendre la maîtrise de l'atelier connecté

> Détecter les dérives opérationnelles avant la panne_

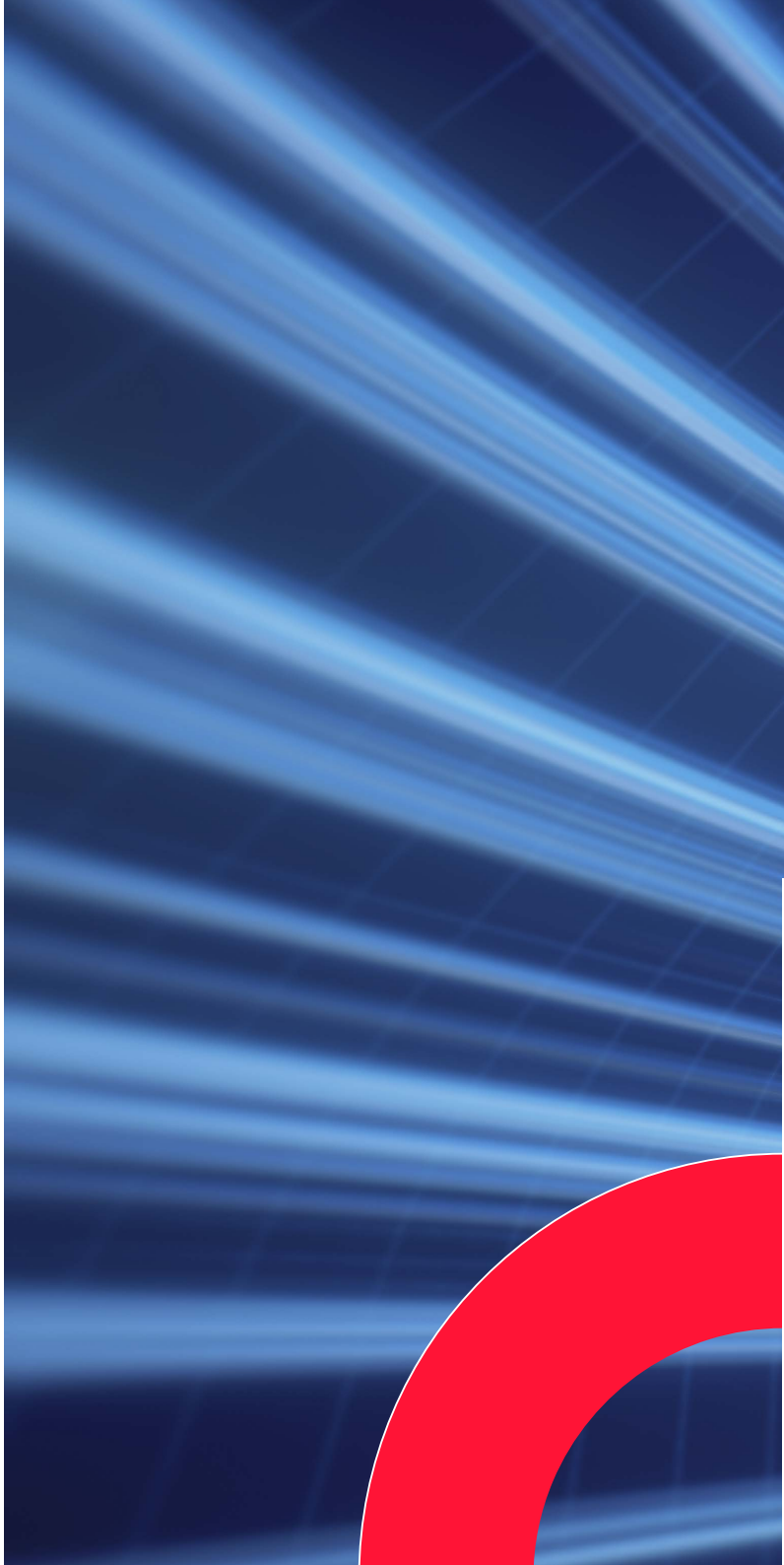
Dans une usine automatisée, les anomalies peuvent être subtiles, comme un changement de paramètre ou un échange inhabituel entre équipements. Ces signaux faibles précèdent parfois des incidents graves. L'analyse des protocoles industriels permet de les détecter avant qu'ils n'impactent la production.

> Retrouver une visibilité globale sur des ateliers fragmentés_

L'industrie d'aujourd'hui est composée de technologies récentes et d'équipements anciens parfois non évolutifs. En analysant les flux, il devient possible de détecter les dépendances cachées, de protéger ces anciens équipements et d'anticiper les risques de propagation d'incidents à travers l'ensemble de la chaîne de production.

> Éviter qu'un incident IT ne devienne une crise industrielle_

Avec la convergence IT/OT, des incidents locaux peuvent impacter l'ensemble du site industriel. Pour éviter qu'une faille dans le SI ou la maintenance touche la production physique, il faut surveiller et contenir les mouvements latéraux avant qu'ils ne traversent les passerelles IT/OT.



Manufacturing

L'ancrage sectoriel de Gatewatcher

Références clients_

Safran, Arthus Bertrand, Groupe Burger&Cie, France Metal, Sanofi et Paris La Défense.

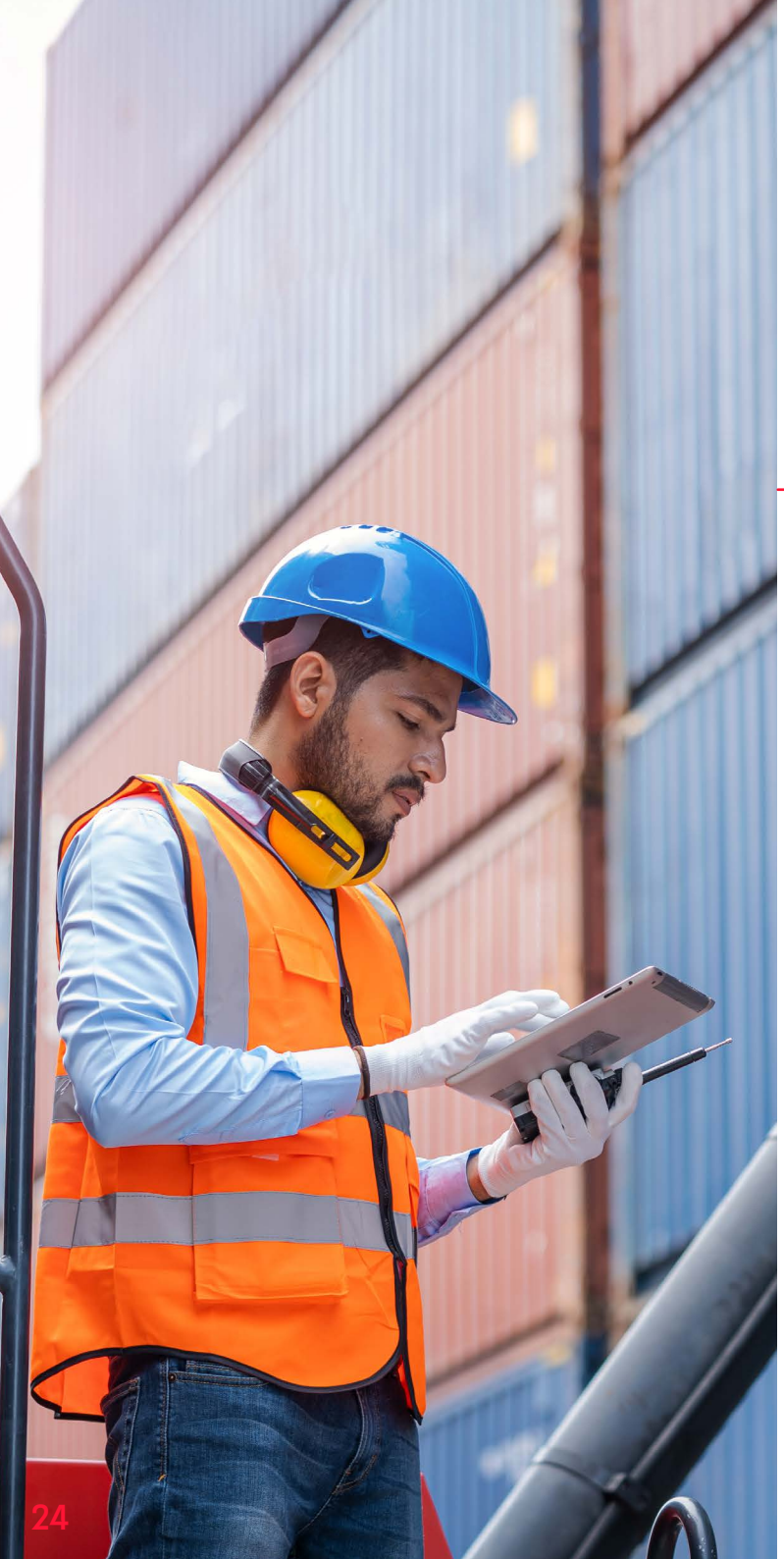
Protocoles industriels couverts_

Modbus, S7, ENIP/CIP, OPC UA, MQTT, Pcom.
> Exclus : DICOM et HL7 (santé), DNP3 et IEC 104 (SCADA énergie/utilities), BACnet (bâtiment uniquement).

Équipements / fabricants OT_

Siemens, Rockwell Automation (Allen-Bradley), Schneider Electric (Modicon), Mitsubishi Electric, Omron, Beckhoff, B&R (ABB), ABB, Bosch Rexroth, Phoenix Contact, Unitronics (Pcom), Fanuc, KUKA, Yokogawa, Emerson.

> *« Les infrastructures aéroportuaires modernes reposent sur l'interconnexion de nombreux systèmes IT et OT : SCADA, contrôle d'accès, vidéosurveillance, gestion des vols, équipements de traitement des bagages ou encore réseaux opérationnels. Gatewatcher nous apporte la visibilité nécessaire pour comprendre ces interactions, détecter les menaces en amont et renforcer la résilience de nos opérations face à un paysage de risques en constante évolution. »*
>
> Jean-Yves Poichotte, Head of Cybersecurity - Sanofi



TRANSPORTS & LOGISTIQUE : SÉCURISER LA MOBILITÉ ET LA CHAINE DE FLUX_

La mobilité au défi de la porosité des réseaux

Dans les transports et la logistique, la convergence IT/OT est devenue le moteur invisible de la fluidité opérationnelle. Centres de tri automatisés, signalisation ferroviaire, systèmes portuaires, hubs logistiques, supervision routière, gestion du trafic ou automatisation des terminaux : l'ensemble de la chaîne repose désormais sur des échanges numériques continus entre infrastructures physiques et systèmes d'information.

Cette transformation répond à une pression opérationnelle majeure : **accélérer les flux, synchroniser les opérations en temps réel et absorber des volumes toujours plus importants sans rupture de service**. La logistique moderne fonctionne désormais comme un système nerveux interconnecté où chaque donnée influence immédiatement un mouvement physique : aiguillage d'un colis, positionnement d'un train, ouverture d'un portique ou pilotage d'un convoyeur automatisé. Mais cette fluidité repose sur une forte dépendance aux réseaux industriels et aux interconnexions IT/OT.

Les infrastructures de transport ne sont plus des systèmes isolés : elles communiquent avec des plateformes cloud, des prestataires externes, des outils de maintenance distante ou des systèmes centraux de pilotage. Quand l'IT et l'OT fusionnent, la surface d'attaque s'étend des postes administratifs jusqu'aux automates de tri et aux systèmes de sécurité des infrastructures (tunnels, gares, terminaux). Le risque majeur n'est plus seulement le vol de données, mais le sabotage du mouvement lui-même. **Une intrusion qui débute par une simple compromission d'accès peut, par mouvement latéral, paralyser les systèmes de guidage ou de signalisation.**

Dans un monde où le transport est le socle de l'économie, chaque heure de paralysie ne se chiffre pas seulement en pénalités financières, mais en une désorganisation systémique de la chaîne d'approvisionnement, mettant en péril la continuité des échanges et la sécurité des usagers.

Scénarios d'attaques récurrents

Détournement de flux logistique (Routing Manipulation)

Un attaquant infiltre le réseau OT d'un centre de tri et modifie les instructions d'aiguillage via le protocole S7 (Siemens).

Impact : les marchandises sont mal orientées ou bloquées, provoquant une rupture de la chaîne d'approvisionnement et des pertes sèches pour les clients finaux.

Blocage des infrastructures portuaires ou ferroviaires

Un ransomware se propage depuis le SI de gestion vers les serveurs de supervision des grues automatisées ou de la signalisation.

Impact : paralysie totale d'un hub de transport. Contrairement à l'IT, le redémarrage nécessite une vérification physique de chaque automate pour garantir la sécurité avant la reprise.

Sabotage des systèmes de sûreté (GTB/GTC)

Une intrusion sur le réseau gérant les ventilations de tunnels ou la détection incendie via une passerelle de maintenance mal sécurisée.

Impact : Fermeture forcée de l'infrastructure pour raisons de sécurité, même si les systèmes de transport eux-mêmes sont fonctionnels, entraînant un chaos logistique régional.

Sécuriser des flux qui ne tolèrent aucune interruption

> Détecter l'intention malveillante dans le signal métier_

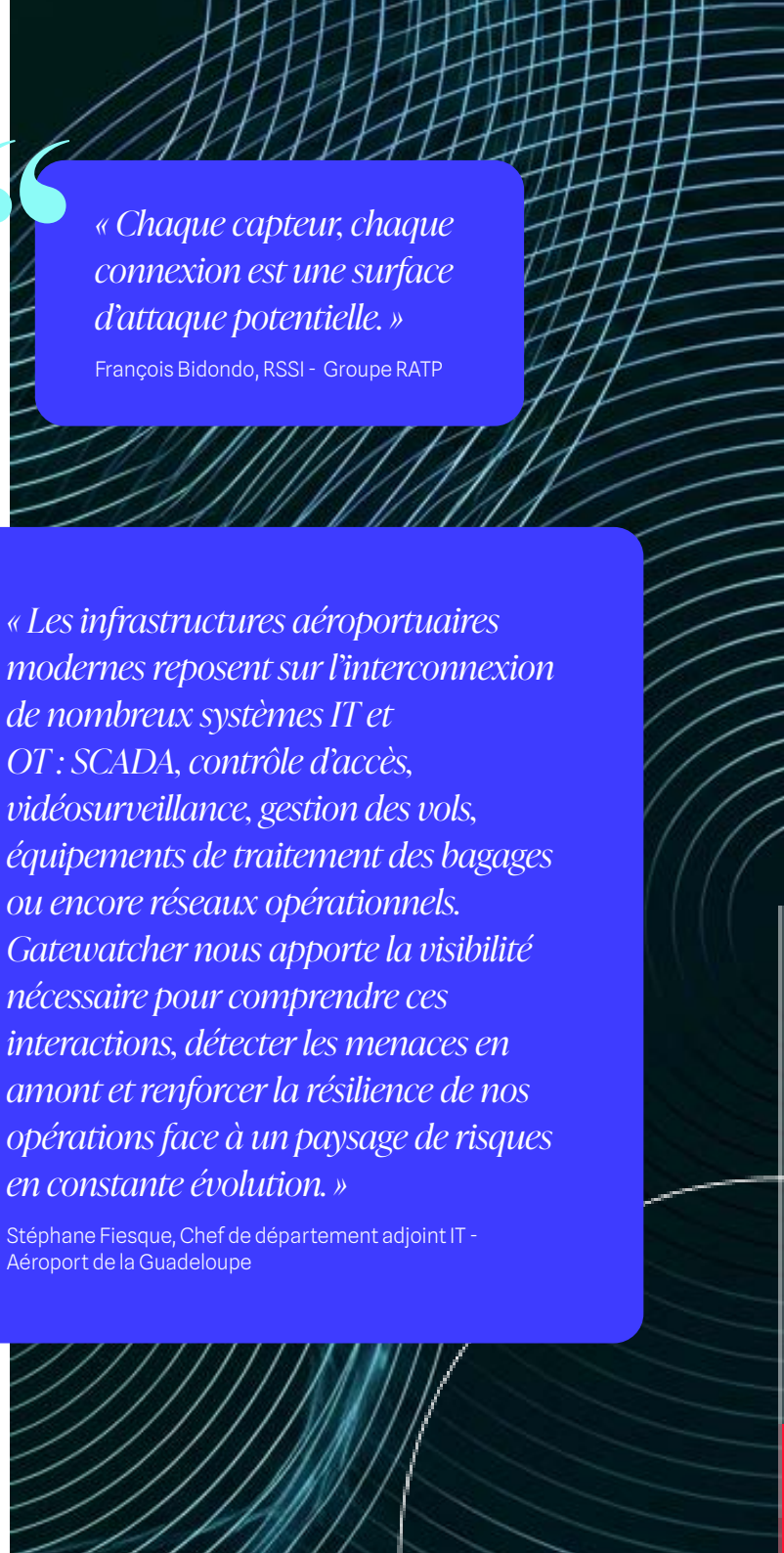
Dans une usine automatisée, les anomalies peuvent être subtiles, comme un changement de paramètre ou un échange inhabituel entre équipements. Ces signaux faibles précèdent parfois des incidents graves. L'analyse des protocoles industriels permet de les détecter avant qu'ils n'impactent la production.

> Sécuriser les accès tiers et la maintenance distante_

L'industrie d'aujourd'hui est composée de technologies récentes et d'équipements anciens parfois non évolutifs. En analysant les flux, il devient possible de détecter les dépendances cachées, de protéger ces anciens équipements et d'anticiper les risques de propagation d'incidents à travers l'ensemble de la chaîne de production.

> Préserver la fluidité sans introduire de latence_

Avec la convergence IT/OT, des incidents locaux peuvent impacter l'ensemble du site industriel. Pour éviter qu'une faille dans le SI ou la maintenance touche la production physique, il faut surveiller et contenir les mouvements latéraux avant qu'ils ne traversent les passerelles IT/OT.



> *« Chaque capteur, chaque connexion est une surface d'attaque potentielle. »*
>
> François Bidondo, RSSI - Groupe RATP

> *« Les infrastructures aéroportuaires modernes reposent sur l'interconnexion de nombreux systèmes IT et OT : SCADA, contrôle d'accès, vidéosurveillance, gestion des vols, équipements de traitement des bagages ou encore réseaux opérationnels. Gatewatcher nous apporte la visibilité nécessaire pour comprendre ces interactions, détecter les menaces en amont et renforcer la résilience de nos opérations face à un paysage de risques en constante évolution. »*
>
> Stéphane Fiesque, Chef de département adjoint IT - Aéroport de la Guadeloupe

L'ancrage sectoriel de Gatewatcher

Références clients_

SNCF, RATP, SAMSIC, Air France, Aéroport de la Guadeloupe, Aéroport de Lyon, IDF Mobilités, APRR et Eurotunnel.

Protocoles industriels couverts_

Modbus, IEC 104, DNP3, S7, OPC UA, MQTT, ENIP/CIP (et BACnet pour les bâtiments de gares/aéroports).

Équipements / fabricants OT_

Siemens Mobility, ABB, Schneider Electric, Alstom, Yunex Traffic, SWARCO, Kapsch TrafficCom, Wabtec, Rockwell Automation (Allen-Bradley), Honeywell, Johnson Controls.

> *« La gestion d'une crise cyber ne se résume pas à détecter une menace ; elle exige de comprendre en quelques heures quels actifs sont concernés et quelles seront les conséquences opérationnelles des décisions prises. La cartographie dynamique de Gatewatcher nous apporte cette visibilité en temps réel sur nos 600 000 actifs et leurs dépendances, permettant aux équipes de prendre des décisions plus rapides, plus éclairées et mieux adaptées aux enjeux des systèmes critiques ferroviaires. »*
>
> José Araujo, Directeur de la cybersécurité - SNCF

> *« Le métro, le bus, le tramway ne sont plus seulement des objets physiques, mais aussi des objets connectés qui doivent être protégés comme tels. »*
>
> François Bidondo, RSSI - Groupe RATP

03 VOIR, COMPRENDRE, ANTICIPER : UNE NOUVELLE APPROCHE DE LA CYBERSECURITE OT_

Proactivité, la nouvelle ligne de défense

La convergence IT/OT a profondément changé la nature du risque dans tous les secteurs d'activité. Les menaces ne ciblent plus des systèmes isolés, mais des environnements hybrides, distribués et interconnectés où une compromission peut désormais produire des conséquences physiques immédiates. Réseaux énergétiques, hôpitaux, chaînes de production, plateformes logistiques, infrastructures de transport ou industries sensibles : partout, le numérique pilote désormais des opérations essentielles au fonctionnement des organisations.

Dans ce contexte, **les approches fondées uniquement sur la protection périmétrique ou le traitement des incidents après coup montrent leurs limites.** L'enjeu n'est plus simplement de bloquer une attaque, mais de **comprendre suffisamment tôt ce qui se passe réellement dans les flux entre systèmes IT et OT afin de détecter une dérive avant qu'elle n'affecte les opérations**. Car lorsqu'un incident devient visible sur la production, la distribution d'énergie, la logistique ou les soins, il est souvent déjà trop tard pour agir.

Cette capacité d'anticipation repose sur un **prérequis fondamental : la visibilité sur les actifs**, les communications, les dépendances et les comportements anormaux au sein d'environnements où coexistent systèmes récents, équipements legacy, accès distants et protocoles spécialisés. Dans ces architectures convergées complexes, le réseau constitue un point d'observation privilégié, capable de révéler l'activité réelle des systèmes et les interactions entre les mondes IT et OT.

Mais la visibilité seule ne suffit plus. Pour comprendre une menace dans sa globalité, **les organisations doivent être capables de corréler les informations issues de multiples sources** : trafic réseau, événements de sécurité, inventaires d'actifs, renseignements sur les menaces (CTI), vulnérabilités connues, journaux systèmes ou encore données métiers. C'est la convergence de ces différents signaux qui permet de **transformer une simple alerte technique en une compréhension précise du risque opérationnel.**

L'enjeu devient alors double : détecter plus tôt, mais également décider plus vite. **Observer les flux, identifier les mouvements latéraux et repérer les signaux faibles n'a de valeur que si ces informations peuvent être contextualisées, priorisées et traduites en actions concrètes.** Face à des attaques capables de se propager en quelques minutes, **la rapidité de la décision devient aussi importante que la qualité de la détection.**

Dans les environnements convergés, passer d'une logique de réaction à une logique d'anticipation ne consiste plus seulement à voir davantage. Il s'agit de transformer la visibilité en compréhension, puis la compréhension en capacité d'action. **C'est cette chaîne — voir, comprendre, décider et agir — qui constitue aujourd'hui le véritable fondement de la résilience opérationnelle.**

Voir avant l'impact : le rôle stratégique du NDR_

Fondé sur une analyse comportementale du réseau, le NDR (Network Detection and Response) s'impose comme l'une des seules approches capables de fournir une **visibilité globale et continue sur l'ensemble des flux sans perturber les opérations.**

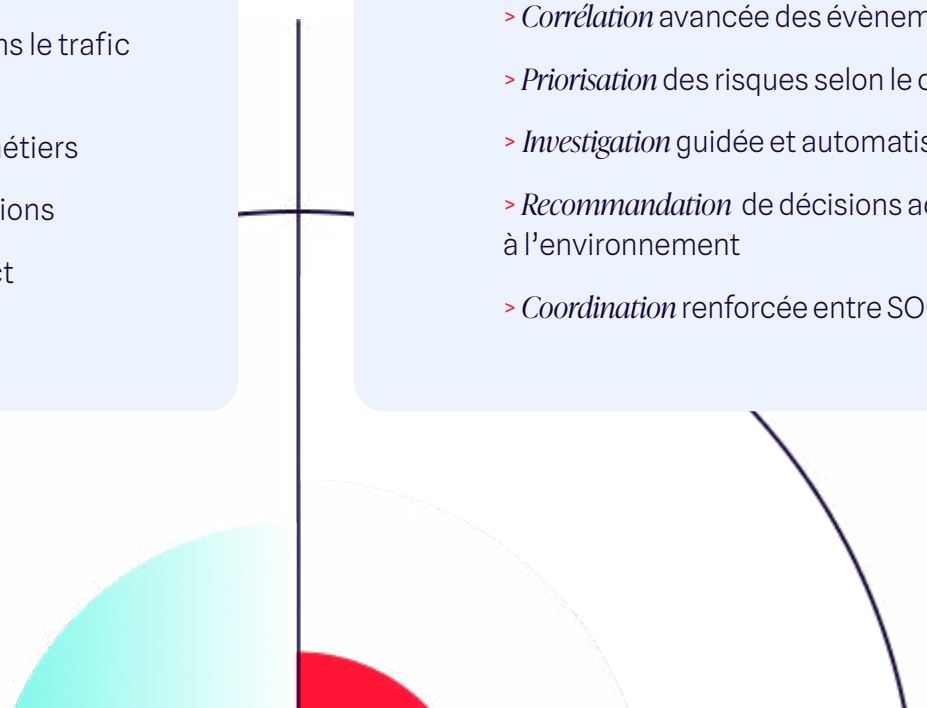
Il permet notamment de :

- *Obtenir* une vision unifiée des flux réels entre systèmes IT et équipements OT
- *Détecter* les mouvements latéraux avant qu'ils n'atteignent les environnements critiques
- *Identifier* les comportements anormaux dissimulés dans le trafic légitime
- *Comprendre* nativement les protocoles industriels et métiers
- *Superviser* les infrastructures sans perturber les opérations
- *Corréler* les signaux faibles entre IT et OT avant l'impact opérationnel

Decision Center : *transformer la visibilité en capacité d'action_*

Le NDR constitue le socle de la connaissance opérationnelle des environnements IT et OT. En offrant une visibilité exhaustive sur les actifs, les communications et les comportements du réseau, il permet de détecter les signaux faibles et les menaces émergentes. Le défi n'est alors plus d'accéder à l'information, mais de **l'interpréter dans son contexte opérationnel afin de prendre les bonnes décisions au bon moment.** Decision Center, la plateforme décisionnelle de Gatewatcher, apporte cette capacité en corrélant les événements, les risques, les dépendances et les impacts métiers pour guider l'action et accélérer la réponse.

- *Corrélation* avancée des évènements IT et OT
- *Priorisation* des risques selon le contexte du secteur
- *Investigation* guidée et automatisée
- *Recommandation* de décisions actionnables adaptées à l'environnement
- *Coordination* renforcée entre SOC, équipes OT et métiers



Au-delà de la compréhension, il accélère également la réponse en guidant les équipes dans la **qualification des incidents, la priorisation des actions et l'orchestration des mesures de remédiation** adaptées à leur environnement.

Selon le niveau d'autonomie défini par l'organisation, certaines **décisions peuvent être automatisées** afin de réduire les délais de réaction, tandis que les actions les plus sensibles restent soumises à validation humaine.

Cette approche permet d'accélérer le passage de la détection à l'action tout en garantissant une gouvernance complète, avec des décisions contextualisées, explicables et auditées.

*Le NDR détecte. Decision Center accélère et orchestre la réponse_*

Les 4 piliers d'une stratégie de cybersécurité IT/ OT efficace

> Reprendre le contrôle de l'écosystème IT/OT

Cartographiez en continu l'ensemble des actifs, communications et dépendances entre environnements IT et OT. Dans des architectures hybrides et hétérogènes, seule une visibilité exhaustive et non intrusive permet d'identifier les angles morts, les interconnexions critiques et les usages à risque sans perturber les opérations.

> Réduire le temps entre détection et décision

Automatisez l'investigation, la corrélation et la priorisation des alertes afin d'accélérer la prise de décision opérationnelle. Dans des environnements où les attaques se propagent en quelques minutes, la capacité à contextualiser rapidement une menace devient essentielle pour limiter l'impact sur l'activité.

VOIR TOUT EN CONTEXTE

Visibilité complète et compréhension réelle des actifs et des flux

DÉTECTER TÔT LES ANOMALIES

Détection comportementale et signaux faibles pour anticiper les menaces

DÉCIDER VITE ET BIEN

Automatisation et orchestration pour des décisions éclairées

AGIR ENSEMBLE

Collaboration IT/OT et métiers pour protéger ce qui compte vraiment : l'activité

> Passer d'une logique de réaction à une logique d'anticipation

Adoptez une détection comportementale capable d'analyser les protocoles industriels, d'identifier les signaux faibles et de repérer les mouvements latéraux avant qu'ils n'atteignent les systèmes critiques. Face à des menaces furtives et évolutives, l'anticipation devient un enjeu direct de continuité d'activité.

> Faire converger les équipes IT, OT et métiers

Construisez une gouvernance commune entre RSSI, équipes OT et directions opérationnelles. La cybersécurité IT/OT ne peut plus être traitée comme un sujet purement technique : elle doit être pilotée en fonction de ses conséquences potentielles sur la production, les soins, la logistique ou la continuité de service.

Des contraintes différentes, un même impératif de résilience

Les quatre verticaux présentés dans ce livre blanc illustrent certaines problématiques majeures de la convergence IT/OT. Mais ils ne représentent qu'un aperçu de la diversité des environnements concernés.

Aéronautique, défense, spatial, industries spécialisées, optronique, infrastructures sensibles… **chaque secteur possède ses propres contraintes opérationnelles**, protocoles métiers, exigences de disponibilité et enjeux de souveraineté.

Cette diversité impose une cybersécurité capable de s'adapter à des environnements hétérogènes, parfois très contraints, où coexistent systèmes legacy, infrastructures critiques et technologies de dernière génération.

À travers ses déploiements et partenariats, Gatewatcher a développé une approche fondée sur la **compréhension native des environnements métiers** : couverture étendue des protocoles OT, supervision passive adaptée aux infrastructures contraintes, capacité d'intégration avec les écosystèmes existants et contextualisation des risques selon les réalités opérationnelles de chaque organisation.

Les retours d'expérience de clients comme Look Up Space ou Lynred illustrent cette réalité : dans certains secteurs, la cybersécurité ne protège pas seulement des systèmes d'information, mais des capacités industrielles, technologiques et souveraines critiques.

Voir plus tôt, comprendre plus vite, décider rapidement : la convergence IT/OT impose une cybersécurité fondée sur l'anticipation.

Quand le numérique pilote les opérations critiques, la cybersécurité devient un enjeu direct de *continuité, de résilience opérationnelle et de souveraineté*_

À propos_

Leader dans le domaine de la détection des cybermenaces, Gatewatcher protège les réseaux des entreprises et du secteur public à travers le monde, y compris les plus critiques. La société offre une visibilité complète sur le réseau grâce à une plateforme NDR basée sur l'IA qui analyse l'activité dans les environnements cloud et sur site. Son « Decision Center » transforme les signaux de sécurité en décisions exploitables et conformes aux règles en unifiant les données provenant du réseau, des terminaux, du cloud et des sources d'identité, améliorant ainsi l'efficacité du SOC et les temps de réponse.

gatewatcher.com

Découvrir nos solutions.....

contact@gatewatcher.com
+33 (0)1 44 51 03 93
Campus Cyber • Puteaux, France

GATEWATCHER
GATEWATCHER Official
@GATEW4TCHER

gatewatcher.com

Ahead of *threats*_

Explore our solutions.....

contact@gatewatcher.com
+33 (0)1 44 51 03 93
Campus Cyber · Puteaux, France

GATEWATCHER
GATEWATCHER Official
@GATEW4TCHER