HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

Cybersécurité des systèmes industriels

Construire une résilience européenne avec des solutions de confiance

Edition 2026

SOMMAIRE

INTRODUCTION

PARTIE 1
ÉTAT DE LA MENACE ET ENJEUX

PARTIE 2
CARTOGRAPHIES DES ACTEURS DE CONFIANCE

PARTIE 3
TEMOIGNAGES ET CAS D'USAGES

Retours d'expérience et exemples de cas clients

LE MOT DU PRÉSIDENT

Jean-Noël DE GALZAIN
Président Hexatrust
Founder & CEO WALLIX Group

En 2025, la plus importante cyberattaque de l'année est celle subie par Jaguar Land Rover (JLR), une entreprise centenaire, qui provoque un électrochoc. Arrêt total des usines pendant plusieurs semaines, chute brutale des ventes mondiales, impact auprès de 6000 fournisseurs et une menace de faillite pour plusieurs sous-traitants de la chaîne d'approvisionnement qui ne peuvent plus être payés. On parle de 3 milliards d'€ de pertes cumulées et d'un sauvetage opéré par le gouvernement britannique. Quel dirigeant d'entreprise, quel élu, quel responsable d'organisation peut aujourd'hui ignorer le risque cyber, considéré comme la première menace qui pèse sur les entreprises selon l'étude annuelle publiée par PWC et réalisée auprès des chefs d'entreprise du monde entier ?

Avec l'adoption de l'IA, la transformation des organisations s'accélère ainsi que les besoins en ressources énergétiques. L'interconnexion des usines, des plateformes d'objets connectés, des véhicules autonomes, les bâtiments, les maisons, les hôpitaux : le numérique est partout. Au-delà des organisations, ce sont plus généralement les systèmes et les réseaux industriels qui nécessitent d'être interconnectés aux applications et aux algorithmes, avec des accès distants sécurisés, pour améliorer la productivité, optimiser leur efficacité énergétique ou encore leur usage grâce au numérique.

La protection des actifs industriels et leur accès à distance devient une priorité dont une partie de la réponse se trouve dans l'application de la directive européenne NIS2. Le projet de loi résilience prévoit ainsi le renforcement de la cybersécurité des systèmes industriels (OT/SCADA) en imposant aux entreprises des secteurs critiques une gestion stricte des risques, l'obligation de notifier les incidents de sécurité et une responsabilité accrue des dirigeants.

Dans ce contexte, Hexatrust a réuni l'expertise et le savoir-faire de ses membres pour apporter des réponses crédibles aux enjeux de sécurité numérique dans l'OT sécurité, avec une approche souveraine impliquant la maîtrise des dépendances technologiques. Nos membres éditeurs et intégrateurs couvrent aujourd'hui l'ensemble de la chaîne de valeur, de l'identification des risques à la gouvernance en phase opérationnelle, pour accompagner la mise en conformité NIS2 des organisations. De nombreux cas d'usage illustrent également ce livre blanc écrit à plusieurs mains pour accompagner les industriels dans leur stratégie.

Plus que jamais face au risque cyber, l'union fait la force !

ÉDITO

Olivier MOREL
Trésorier Hexatrust
Pilote du groupe de travail Cyber OT
Directeur Général SNOWPACK

La cybersécurité des environnements industriels est désormais au cœur des préoccupations des organisations exploitant des infrastructures critiques. L'accélération de la transformation numérique, la convergence entre les systèmes d'information et les technologies opérationnelles, ainsi que l'évolution des menaces imposent aujourd'hui d'intégrer la cybersécurité comme un levier de performance, de résilience et d'indépendance.

Ces dernières années, de nombreux travaux de grande qualité ont été publiés pour accompagner cette évolution. Qu'il s'agisse des recommandations de l'ANSSI, des référentiels internationaux ou des initiatives portées par les acteurs de la filière, les concepts, les architectures de référence et les bonnes pratiques sont désormais largement documentés.

L'ambition de cet ouvrage est différente. Notre objectif n'est pas de réécrire ce qui existe déjà, mais d'apporter une réponse concrète à une question essentielle : quelles sont aujourd'hui les solutions disponibles pour mettre en œuvre ces recommandations ?

Au sein d'Hexatrust, de nombreux membres développent des technologies répondant aux besoins spécifiques de la cybersécurité industrielle. Ensemble, ils démontrent qu'il existe une offre française et européenne mature, éprouvée sur le terrain et capable de répondre aux exigences des environnements industriels les plus critiques. Les solutions existent, sont déployées à grande échelle et constituent aujourd'hui une alternative crédible aux offres extra-européennes.

Cette complémentarité est devenue indispensable. Les attaques récentes montrent que les compromissions exploitent rarement une vulnérabilité unique : elles combinent plusieurs vecteurs, plusieurs étapes et plusieurs objectifs, jusqu'à produire des conséquences bien réelles sur les processus industriels. Face à cette complexité, aucune solution ne peut, à elle seule, répondre à l'ensemble des enjeux. La force d'Hexatrust réside précisément dans sa capacité à fédérer un collectif d'expertises complémentaires autour d'une ambition commune : construire une réponse souveraine, cohérente et opérationnelle au service des industriels. Les cartographies proposées dans ce livre blanc ainsi que les retours d'expérience de nos membres illustrent cette approche collective et mettent en lumière la richesse de l'écosystème français et européen.

Parce qu'en matière de cybersécurité industrielle, la résilience se construit autant par la qualité des technologies que par la capacité des acteurs à travailler ensemble, nous avons la conviction que ce livre blanc contribuera à faire connaître les solutions qui existent déjà et à renforcer la confiance dans une filière souveraine, innovante et résolument tournée vers l'action.

PAROLE D'EXPERTE

Hélène BERNADINI
Fondatrice HackteOT

Le code et l'acier : la fin des mondes étanches

Pendant des décennies, nous avons travaillé à l'abri d'une frontière invisible. D'un côté, l'informatique de gestion (IT) et ses serveurs qu'on étanchéifie pour protéger des secrets. De l'autre, l'usine, la chaîne logistique, le terrain : là où le code rencontre l'acier, les vannes, les moteurs et les automates. Ce second monde, l'OT, n'avait cure des cybermenaces. On n'y protégeait pas des données virtuelles, on y garantissait la disponibilité de l'outil de travail, la cadence de production et l'intégrité physique des opérateurs.

Mais cette étanchéité est morte. Aujourd'hui, les frontières s'effacent. Nos équipements critiques parlent en permanence à travers des réseaux interconnectés. Cette convergence offre une agilité sans précédent, mais elle a ouvert une boîte de Pandore. Les organisations cybercriminelles l'ont compris : paralyser l'informatique d'une entreprise est lucratif ; confisquer ses clés physiques et prendre son usine en otage est imparable. Un rançongiciel en milieu industriel, ce n'est pas un écran bleu ou une perte de fichiers Excel. C'est une ligne de production qui s'arrête net, une dérive silencieuse des seuils de sécurité sur une cuve, ou un système de ventilation coupé en zone stérile. Le risque cyber est devenu un risque vital, environnemental, mais aussi de souveraineté économique.

Sur le terrain, au sein de la communauté HacktheOT, la réalité que nous observons est prosaïque. Près de 80 % des intrusions passent par des accès de maintenance non sécurisés ou des clés USB sauvages. C'est ce routeur 4G branché à la hâte ou cette console d'automate laissée ouverte. Face à cela, la réponse ne peut plus être artisanale ou isolée. Elle impose d'instaurer un dialogue permanent entre le terrain, qui connaît les machines, et les équipes cyber. La cybersécurité est le nouvel EPI, l'équipement de protection individuelle de l'industrie moderne.

Pour équiper nos ateliers, les armes existent. Les solutions souveraines européennes en matière de cyber OT ne sont plus de lointaines promesses : elles sont concrètes, scalables et largement déployées sur le terrain. Sécuriser nos environnements exige de nourrir ce dialogue pour faire converger l'expertise de nos automaticiens et de nos champions technologiques. C'est tout le sens de l'écosystème réuni ici par Hexatrust : parce que « l'union fait la force », nous ne gagnerons qu'en collectif. Les cartographies fonctionnelles et les cas d'usage opérationnels qui suivent en sont la preuve par l'action. Face aux chocs de demain, unissons nos forces pour que nos industries continuent de croître en toute sécurité.

PAROLE D'EXPERT

Frédéric GUYOMARD
EDF R&D – Chef de projet Cybersécurité des Systèmes Industriels
Animateur de la commission technique CSI de l'EXERA

La Cybersécurité industrielle en 2026

Les technologies opérationnelles sont au cœur du fonctionnement des installations industrielles qui, parfois critiques, constituent des systèmes fortement interconnectés et interdépendants, sur les plans physique et numérique. Ces infrastructures s'appuient sur des systèmes cyber-physiques (CPS) — notamment les systèmes de contrôle industriel connus sous le terme générique de SCADA — dont le rôle est de surveiller, contrôler et agir à temps sur des processus de production ou de service. De plus en plus numérisés, ces CPS intègrent des fonctions et composants de sécurité numérique, en réponse aux exigences croissantes de sûreté de fonctionnement et aux risques inhérents à la numérisation générale des environnements industriels.

Les conséquences d'une cyberattaque peuvent varier largement en nature et en gravité. Elles peuvent aller d'une simple dégradation des performances (temps de réponse, stabilité des systèmes) à une atteinte à l'intégrité des données ou des applications (modification, altération, corruption) ou encore au vol d'information sensible, voire l'arrêt partiel ou total de fonctions critiques. Les impacts peuvent être opérationnels, financiers, ou patrimoniaux (physiques ou intellectuels). Dans les cas les plus graves, la compromission de systèmes critiques peut engendrer des conséquences humaines ou environnementales significatives.

Face à ces menaces, la défense en profondeur s'impose comme cadre de référence partagé par l'ensemble des acteurs de la cybersécurité. Elle repose sur trois piliers : l'identification des criticités, l'intégration de mesures de protection/sécurité dès la conception (secure by design) et la capacité à détecter les comportements anormaux afin de prévenir et réagir aux incidents.

Des exemples récents illustrent avec acuité l'exposition du secteur électrique : les cyberattaques contre le réseau ukrainien en 2015, 2016 et 2022, ainsi que les attaques plus récentes visant des installations du réseau polonais, rappellent que les systèmes industriels moins résilients sont des cibles de choix, avec des conséquences potentiellement graves sur la continuité de service et la sécurité des populations.

L'EXERA agit, au sein de sa commission technique CSI, pour échanger, appréhender et analyser ces problématiques afin d'y apporter des solutions. Son approche est d'adopter le point de vue des opérateurs de terrain, à tous les niveaux.

PAROLE D'EXPERT

Loïs Samain
Administrateur du CESIN
Responsable de la Stratégie Cybersécurité
Groupe RATP

Relever ensemble le défi de la cybersécurité industrielle par la convergence et l'adaptation

La transformation numérique n'épargne aucun secteur et le monde industriel y trouve un formidable levier de performance. Cependant, cette digitalisation accélérée s'accompagne d'une réalité incontournable : l'augmentation drastique de notre surface d'exposition aux risques cyber. Les frontières autrefois étanches entre l'environnement opérationnel et le monde extérieur se structurent de passerelles numériques, transformant des infrastructures critiques en cibles potentielles.

Face à cette menace, copier-coller les recettes de la cybersécurité classique est une impasse. Le monde industriel possède ses propres spécificités : la primauté de la sûreté des biens et des personnes (safety), une exigence absolue de disponibilité, une attention forte à l'intégrité des processus selon les secteurs, des cycles de vie longs et des protocoles locaux spécifiques. Pour naviguer dans cet écosystème, nous devons accompagner la convergence de trois mondes distincts : l'IT (les systèmes d'information traditionnels), l'OT (les technologies opérationnelles) et, à la jointure des deux, l'« IT for OT ».

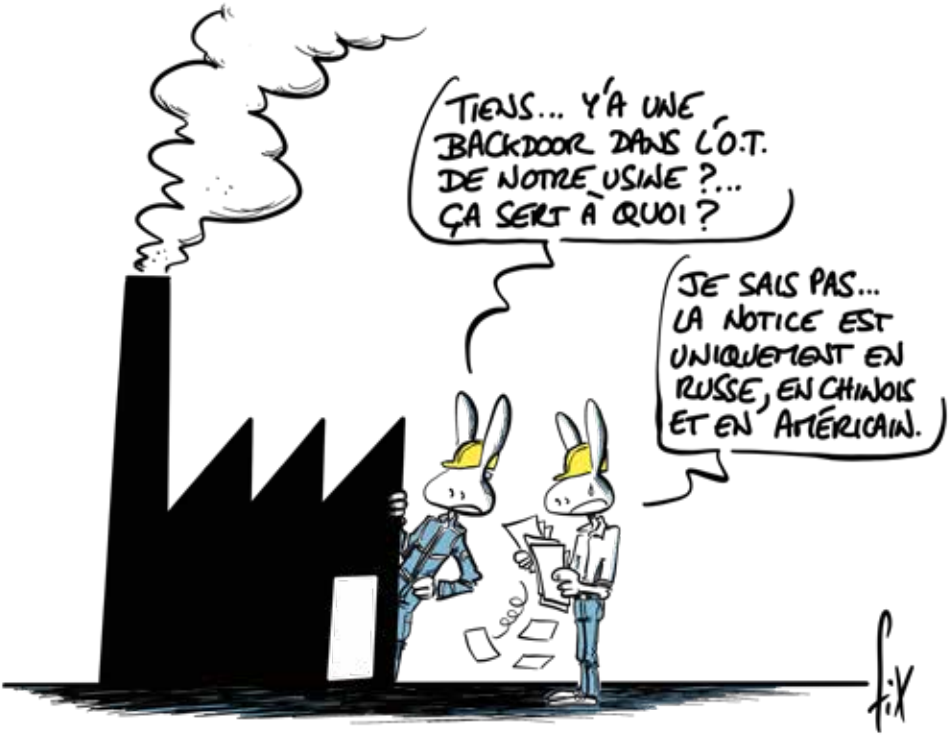
Au sein du CESIN, qui rassemble plus de 1 200 responsables de la cybersécurité, nous constatons quotidiennement cette mutation. C'est pourquoi notre communauté dédiée à l'OT, de plus en plus nombreuse, se réunit régulièrement pour partager entre pairs, échanger sur les bonnes pratiques et coconstruire des approches pragmatiques face à ces enjeux complexes.

Car la réponse à ce défi n'est pas uniquement l'affaire de produits. Une protection efficace repose avant tout sur une stratégie claire, une gouvernance solide, une adaptation profonde des processus et une évolution de l'organisation. C'est en transformant nos méthodes de travail que nous donnerons leur pleine mesure aux outils de défense.

C'est là que réside toute la valeur de ce livrable. Pour les responsables cybersécurité et responsables industriels, maintenir une visibilité claire sur l'exhaustivité des solutions du marché est un exercice complexe, l'écosystème OT étant parfois moins connu. Cette publication d'Hexatrust est donc particulièrement salutaire : elle dresse un inventaire précieux des solutions françaises et européennes existantes, renforçant notre souveraineté technologique.

Enfin, la réussite repose sur un dialogue renouvelé. Clients et fournisseurs européens doivent travailler main dans la main pour coconstruire les solutions les plus adaptées aux besoins opérationnels du terrain. Cette collaboration étroite est une dynamique profondément « gagnant-gagnant » : elle permet d'élever notre niveau de protection tout en renforçant l'écosystème technologique européen. C'est à cette seule condition que nous bâtirons une Europe plus forte, plus résiliente, et capable de sécuriser durablement ses infrastructures industrielles et critiques.

Changer de regard sur la menace



PARTIE I

ÉTAT DE LA MENACE ET ENJEUX

Une menace en profonde mutation

La menace évolue

Pendant longtemps, les systèmes industriels ont été considérés comme relativement préservés des cyberattaques. Conçus pour fonctionner dans des environnements fermés, reposant sur des équipements spécialisés et des protocoles propriétaires, ils bénéficiaient d'un cloisonnement naturel vis-à-vis des systèmes d'information traditionnels. Cette situation a profondément évolué au cours des dernières années.

La transformation numérique des sites industriels, l'interconnexion croissante entre les environnements IT et OT, le développement de la maintenance à distance, l'essor de l'Internet industriel des objets (IIoT) ou encore la généralisation des échanges avec les partenaires et les fournisseurs ont considérablement accru leur surface d'exposition.

Les systèmes industriels sont désormais pleinement intégrés aux chaînes de valeur numériques et, à ce titre, exposés aux mêmes menaces que les systèmes d'information classiques, avec des conséquences potentiellement beaucoup plus importantes.

> Les analyses publiées par les autorités publiques, les organismes spécialisés et les principaux acteurs du secteur convergent vers un même constat : les infrastructures industrielles constituent désormais des cibles privilégiées.

Cette évolution s'inscrit dans un contexte marqué par la multiplication des tensions géopolitiques, la professionnalisation des groupes cybercriminels et l'industrialisation des modes opératoires. Les campagnes d'attaques sont plus nombreuses, mieux préparées et s'appuient sur des chaînes de compromission toujours plus sophistiquées.

L'intelligence artificielle contribue par ailleurs à accélérer cette industrialisation des attaques, en facilitant certaines phases de reconnaissance, d'ingénierie sociale ou d'automatisation. Si elle ne constitue pas, à elle seule, une rupture des modes opératoires observés dans les environnements OT, elle participe à l'abaissement du niveau d'expertise nécessaire et à l'augmentation du rythme des campagnes malveillantes.

Au-delà de l'augmentation du nombre d'incidents, c'est la nature même des attaques qui évolue. Alors que les premières campagnes visaient principalement le vol d'informations ou l'interruption de systèmes informatiques, les attaques les plus récentes cherchent désormais à produire des effets concrets sur les processus industriels : arrêt d'une chaîne de production, indisponibilité d'un service essentiel, perturbation d'un réseau d'énergie, d'un oléoduc ou d'une installation de traitement des eaux. **Les conséquences ne sont plus seulement numériques ; elles deviennent opérationnelles, économiques, voire physiques.**

Les attaques évoluent

Parallèlement, les attaquants ont profondément fait évoluer leurs modes opératoires. Les campagnes les plus récentes montrent qu'il est rarement nécessaire de compromettre directement un automate programmable ou un système de supervision pour perturber un processus industriel. Les accès distants et les systèmes insuffisamment maintenus ou exposés sur Internet, les postes d'administration, les annuaires d'entreprise, les équipements de maintenance, les fournisseurs ou encore la chaîne d'approvisionnement constituent désormais des points d'entrée privilégiés. Une fois le système d'information compromis, les attaquants cherchent à progresser latéralement (lateral movement) jusqu'aux environnements industriels afin d'obtenir l'effet recherché.

Cette évolution remet en question certaines idées reçues. L'isolement physique des réseaux industriels ne constitue plus, à lui seul, une protection suffisante. De même, la sécurité des environnements OT ne peut plus être pensée indépendamment de celle des systèmes d'information. **La convergence IT/OT, devenue indispensable pour améliorer la performance, la supervision ou la maintenance des installations, impose désormais une approche globale de la cybersécurité.**

Comme le souligne l'ANSSI dans son Panorama de la cybermenace 2025, les attaques les plus préoccupantes sont aujourd'hui celles qui combinent plusieurs techniques de compromission afin d'atteindre des infrastructures critiques ou des processus industriels. **Cette hybridation des attaques constitue l'une des principales évolutions observées au cours des deux dernières années et impose aux organisations de renforcer simultanément leur capacité de prévention, de détection et de réaction.**

Face à cette évolution, la question n'est plus de savoir si les environnements industriels seront ciblés, mais comment construire une stratégie de cybersécurité capable de prendre en compte la diversité des menaces, la complexité des architectures industrielles et les fortes exigences de disponibilité qui caractérisent les systèmes OT. Également, elle doit tenir compte de la réalité des environnements industriels, où coexistent fréquemment des équipements anciens, parfois non maintenus, avec des technologies beaucoup plus récentes. Cette hétérogénéité constitue aujourd'hui l'un des principaux défis de la cybersécurité OT.

> *« Alors que l'année 2025 s'est terminée de manière alarmante sur une série d'attaques informatiques contre les infrastructures polonaises, attaques coordonnées et à visée destructive, cet évènement dresse le spectre du scenario redouté, auquel la France se prépare. Un scenario central dans lequel nous ferions face à une augmentation massive d'ici 2030 des attaques dites « hybrides », dont les cyberattaques constituent un pan majeur, avec des effets concrets voire destructeurs sur nos infrastructures critiques. »*
>
> **Vincent Strubel, directeur général de l'ANSSI**
> Panorama de la cybermenace 2025

Les cybercriminels, eux aussi, savent s'adapter

Quand une cyberattaque produit des effets dans le monde réel

Les attaques visant les environnements industriels ont profondément évolué au cours des dernières années. Si les objectifs des attaquants demeurent variés – espionnage, extorsion, sabotage ou déstabilisation – leurs modes opératoires convergent désormais vers une même logique : **exploiter les interconnexions entre les systèmes d'information et les environnements industriels afin de produire un impact opérationnel.**

Contrairement à une idée largement répandue, **les cyberattaques contre les systèmes industriels ne ciblent pas systématiquement les automates programmables, les systèmes SCADA ou les équipements de terrain.** Les exemples récents montrent au contraire que les compromissions débutent très souvent dans les environnements informatiques traditionnels : poste utilisateur, accès VPN, serveur exposé sur Internet, compte à privilèges compromis, fournisseur de maintenance ou encore chaîne d'approvisionnement logicielle.

Une fois cette première étape franchie, les attaquants cherchent à progresser latéralement au sein du système d'information jusqu'à atteindre les réseaux industriels ou les systèmes permettant leur administration. Cette approche, plus discrète et souvent plus efficace, leur permet d'exploiter les relations de confiance existant entre les environnements IT et OT pour atteindre leur objectif final.

Cette évolution est d'autant plus préoccupante que de nombreux environnements industriels restent contraints par un patrimoine technologique parfois ancien. Les cycles de vie des équipements industriels, souvent supérieurs à quinze ou vingt ans, rendent les mises à jour complexes, voire impossibles, tandis que certains systèmes d'exploitation ou logiciels ne sont plus maintenus par leurs éditeurs. À ces contraintes s'ajoutent des exigences de disponibilité qui limitent les fenêtres d'intervention et retardent parfois l'application des correctifs de sécurité.

Parallèlement, les besoins croissants d'interconnexion, de télémaintenance, de supervision centralisée ou d'accès distants ont conduit de nombreuses organisations à exposer, parfois involontairement, certains services industriels sur Internet. Plusieurs études récentes montrent que **cette surexposition constitue désormais l'un des principaux facteurs de risque des environnements OT,** offrant aux attaquants des points d'entrée accessibles sans même compromettre le réseau interne de l'organisation.

Les incidents les plus récents confirment ces évolutions

Fin 2025 et début 2026, plusieurs attaques ont illustré la capacité des cybercriminels et des groupes liés à des intérêts étatiques à provoquer des perturbations sur des infrastructures critiques européennes. Les attaques ayant visé le réseau de pipelines roumain, certaines infrastructures électriques polonaises, des opérateurs du secteur de l'eau au Danemark ou encore plusieurs grands groupes industriels européens démontrent que les objectifs dépassent désormais le simple chiffrement de données ou le vol d'informations. **L'objectif est désormais de produire un effet concret dans le monde réel : interrompre une production, perturber un réseau d'énergie, empêcher l'accès à une ressource essentielle ou dégrader un service critique.** Les systèmes industriels deviennent ainsi des leviers de pression économique, stratégique ou politique, dans un contexte marqué par une instabilité géopolitique croissante.

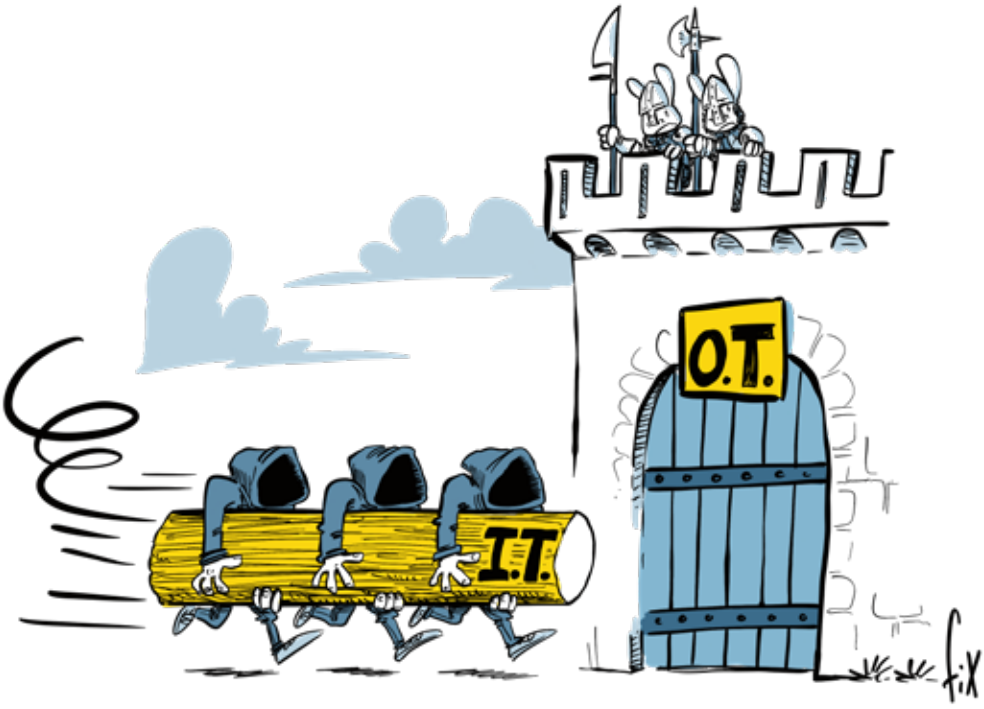
Au-delà de leurs spécificités techniques, ces incidents illustrent plusieurs tendances de fond. Les campagnes sont de plus en plus hybrides, combinant cybercriminalité, espionnage et opérations d'influence. Elles exploitent simultanément plusieurs vecteurs de compromission et ciblent aussi bien les personnes que les processus et les technologies. Les groupes les plus sophistiqués privilégient des stratégies de long terme, fondées sur une connaissance approfondie des architectures industrielles et des contraintes opérationnelles de leurs victimes.

Cette évolution remet également en question la frontière entre l'IT et l'OT. Si les réseaux industriels restent soumis à de fortes exigences de disponibilité et de sûreté de fonctionnement, ils ne peuvent plus être considérés comme des environnements isolés. Les échanges de données, la supervision centralisée, la télémaintenance ou les besoins de pilotage à distance créent autant de points de passage qui doivent être maîtrisés.

> **Le constat est désormais largement partagé : la cybersécurité industrielle ne peut plus reposer sur une mesure de protection unique ni sur la seule sécurisation d'un périmètre technique.**

Les architectures modernes imposent une approche globale, combinant gouvernance, mesures organisationnelles et technologies complémentaires. Cette vision systémique, fondée sur la défense en profondeur, constitue aujourd'hui le socle des principaux référentiels internationaux et des stratégies de résilience les plus matures.

Les attaques industrielles modernes ciblent moins les automates… que tout ce qui permet d'y accéder !



Structurer la réponse

Face à des menaces toujours plus hybrides et à des architectures industrielles toujours plus interconnectées, la cybersécurité ne peut plus être envisagée comme une succession de mesures techniques indépendantes. **Elle relève désormais d'une démarche globale, conciliant disponibilité des systèmes industriels, sûreté de fonctionnement et sécurité numérique.**

Cette évolution a conduit les industriels à s'appuyer sur des référentiels reconnus, capables de structurer une stratégie de cybersécurité cohérente dans la durée. Au premier rang de ces référentiels, la série de normes **IEC 62443** s'est progressivement imposée comme la référence internationale en matière de cybersécurité des systèmes d'automatisation et de contrôle industriels **(IACS)**. Sans prescrire une architecture unique ni recommander des technologies particulières, elle propose un cadre méthodologique permettant d'intégrer la cybersécurité tout au long du cycle de vie des installations.

> **L'un des principes fondateurs de cette approche repose sur la défense en profondeur (*Defense in Depth*). Il ne s'agit plus de protéger uniquement le périmètre du réseau industriel, mais de mettre en œuvre plusieurs niveaux de protection complémentaires afin de limiter les possibilités de compromission, de ralentir la progression d'un attaquant et de renforcer les capacités de détection et de réaction en cas d'incident.**

Cette logique s'appuie notamment sur une segmentation adaptée des architectures industrielles, la maîtrise des flux entre les différentes zones fonctionnelles, le contrôle des accès, le maintien en condition de sécurité des équipements, la supervision des activités et la capacité à détecter rapidement tout comportement anormal.

Le *Purdue Model*, **présenté dans la partie suivante de ce document, constitue à cet égard un modèle largement utilisé pour représenter ces différents niveaux d'architecture et organiser les mesures de sécurité associées.**

Au-delà des aspects techniques, les organisations doivent également intégrer la cybersécurité dans leur gouvernance. Gestion des risques, politique de sécurité, maîtrise des accès distants, gestion des vulnérabilités, réponse aux incidents, maintien en condition de sécurité ou sensibilisation des équipes constituent désormais des composantes essentielles d'une stratégie de protection durable.

Cette approche trouve aujourd'hui un écho particulier dans les évolutions réglementaires européennes. Avec la directive **NIS2**, de nombreuses organisations exploitant des services essentiels ou importants sont désormais tenues de démontrer leur capacité à maîtriser leurs risques cyber et à mettre en œuvre des mesures de sécurité proportionnées. Si NIS2 fixe des objectifs de résilience, les référentiels tels que l'IEC 62443 apportent quant à eux un cadre opérationnel permettant de décliner ces exigences dans les environnements industriels.

Cette complémentarité entre gouvernance, architecture, technologies et maintien en condition de sécurité rappelle qu'il n'existe pas de solution universelle capable, à elle seule, de protéger un système industriel. La résilience repose au contraire sur l'association de compétences, de processus et de technologies complémentaires, mises en œuvre de manière cohérente en fonction des risques, des contraintes opérationnelles et du niveau de maturité de chaque organisation.

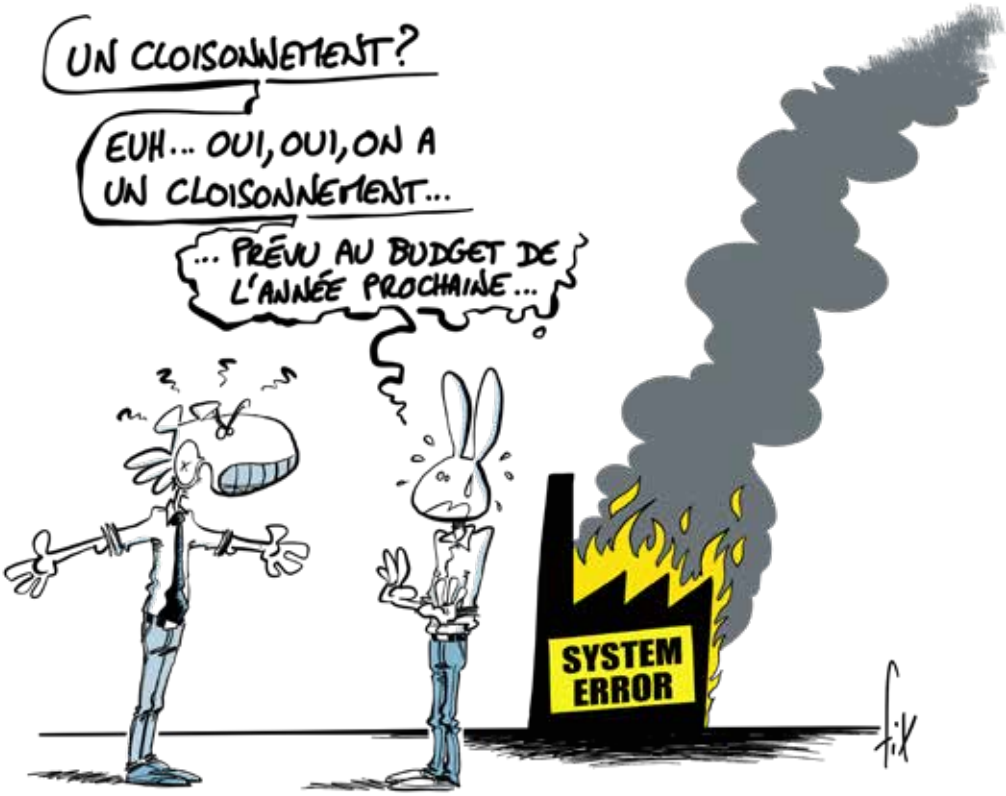
C'est dans cette logique que s'inscrivent les cartographies présentées dans les pages suivantes. Elles ne proposent pas une architecture de référence unique, mais offrent plusieurs grilles de lecture permettant de comprendre comment les expertises réunies au sein d'Hexatrust contribuent, de manière complémentaire, à renforcer la résilience des environnements industriels.

À RETENIR !

Quatre principes clés d'une cybersécurité industrielle résiliente…

- Évaluer les risques propres aux environnements OT.
- Structurer la sécurité selon une approche de défense en profondeur.
- S'appuyer sur des référentiels reconnus (IEC 62443, NIS2…).
- Combiner des expertises et des technologies complémentaires plutôt que rechercher une solution unique.

La cybersécurité doit être pensée avant...



PARTIE II

CARTOGRAPHIES DES ACTEURS DE CONFIANCE

Trois lectures complémentaires d'un même écosystème

La cybersécurité des systèmes industriels ne peut être appréhendée sous un seul angle. Les solutions répondent à des besoins multiples, interviennent à différentes étapes d'un projet et s'intègrent à des niveaux variés de l'architecture industrielle. Une représentation unique ne permettrait donc pas de refléter la richesse et la complémentarité des expertises réunies au sein d'Hexatrust.

C'est pourquoi nous avons choisi de proposer trois cartographies complémentaires, offrant chacune une lecture différente de cet écosystème.

- La première adopte une **approche fonctionnelle.** Elle regroupe les membres d'Hexatrust selon leurs principaux domaines d'expertise afin d'offrir une vision globale des grandes familles de solutions disponibles pour protéger les environnements industriels.

- La deuxième privilégie une **lecture opérationnelle.** Elle s'intéresse non plus aux technologies elles-mêmes, mais aux principaux besoins auxquels sont confrontés les exploitants : inventorier leurs actifs, superviser les infrastructures, sécuriser les accès distants, segmenter les réseaux, ou encore accompagner la transformation des systèmes industriels.

- Enfin, la troisième cartographie propose **une vision technique,** en positionnant les différentes offres au regard du *Purdue Model for ICS Security*, modèle d'architecture de référence largement utilisé pour représenter l'organisation des systèmes industriels et les différents niveaux qui les composent.

Ces trois représentations sont complémentaires. Elles ne visent ni à établir une classification exhaustive, ni à enfermer les solutions dans une catégorie unique. Au contraire, de nombreuses technologies couvrent plusieurs fonctions ou répondent à plusieurs usages, tandis que les sociétés de services et d'intégration accompagnent les projets de manière transverse, de la définition des besoins jusqu'au maintien en conditions opérationnelles et de sécurité.

L'objectif de ces cartographies est avant tout de faciliter la lecture de l'écosystème Hexatrust et d'aider les organisations à identifier les expertises susceptibles de répondre à leurs enjeux, en fonction de leur propre contexte technique, opérationnel ou organisationnel.

Cartographier pour mieux sécuriser

Vision fonctionnelle de l'écosystème Hexatrust

Accès distants sécurisés & cloisonnement logique

SNOWPACK : réduction de la surface d'attaque externe, invisibilité réseau

WALLIX : PAM, bastion, traçabilité des sessions

snowpack wallix

Services & accompagnement

Audit, conseil, formation et sensibilisation, mise en conformité, intégration, services managés, soc...

• ADAMANTE CYBER • ALGOSECURE • AXIANS • BLUESECURE • COGICEO • EVICYS • EXCELSIOR SAFETY • FENRISK

ADAMANTE algosecure KEEP IT SAFE AND SECURE axians bluesecure

COGICEO EVICYS eXcelsior Safety fenrisk

Supervision & détection (visibilité réseau, NDR, gestion vulnérabilités)

AIOTRUST : détection d'attaques sur infrastructures de production

CYBERWATCH : gestion des vulnérabilités, inventaire et conformité

CYBI : détection des vulnérabilités critiques et priorisation des remédiations

GATEWATCHER : NDR, détection comportementale, CTI et réponse

SECLAB : cartographie non-intrusive, détection des changements et anomalies

Isolation, périmètre réseau & durcissement matériel

CYBERIUM : segmentation réseau OT et hardware security

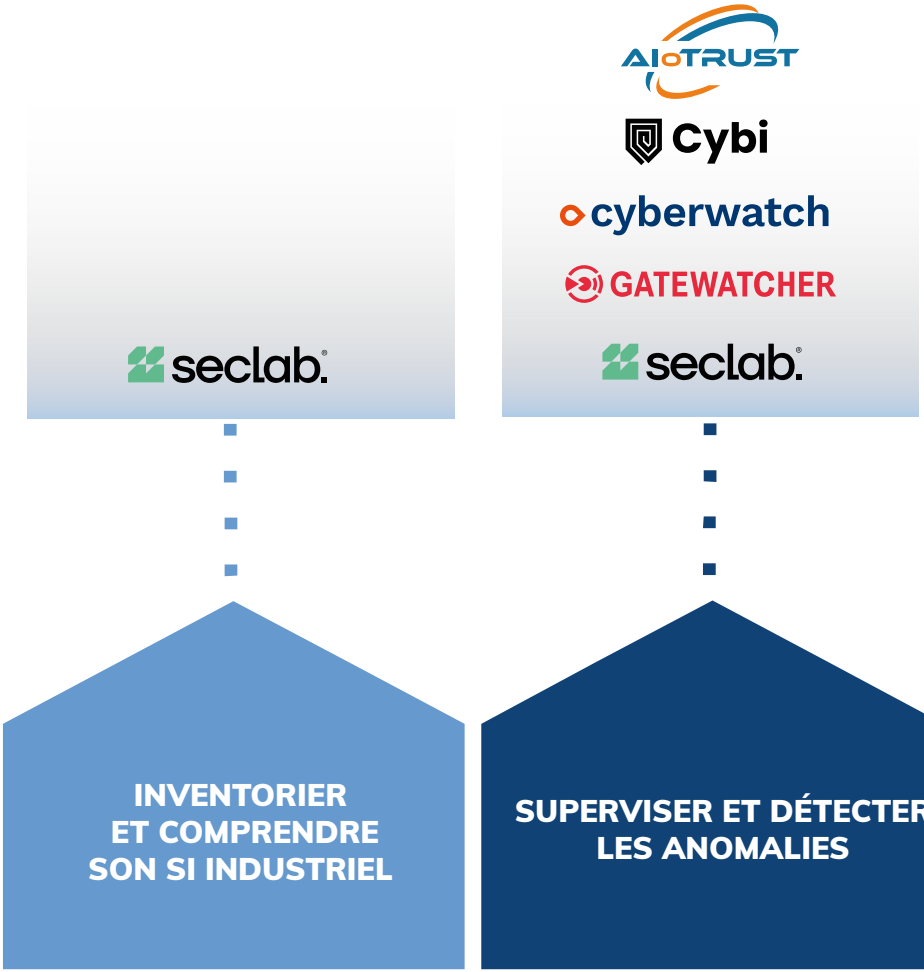
P4S : contrôleurs réseau matériels, chiffrement, FW hardware et protection DDoS

PROVENRUN : HSM souverain, cloud-native et post-quantique

SECLAB : isolation électronique, segmentation réseau et protection USB

TYREX : stations et bornes de décontamination, analyse des médias amovibles

Vision opérationnelle de l'écosystème Hexatrust



Cyberium

PROVENRUN

P4S

seclab.

TYREX

snowpack

wallix

DURCIR ET SEGMENTER LES COMMUNICATIONS OT/IT

SÉCURISER LES ACCÈS DISTANTS

ESTRER LA TRANSFORMATION

axians

bluesecure

eXcelsior Safety

fenrisk

Le *Purdue Model* : une lecture de référence des architectures industrielles

Les systèmes industriels modernes reposent sur une grande diversité d'équipements, de réseaux et d'applications qui interagissent pour piloter les procédés de production. Automates, capteurs, systèmes de supervision, postes d'ingénierie, serveurs applicatifs ou encore systèmes d'information de l'entreprise n'ont ni les mêmes fonctions, ni les mêmes contraintes opérationnelles ou de sécurité.

Afin de représenter cette organisation complexe, le *Purdue Enterprise Reference Architecture* (PERA), plus communément appelé *Purdue Model*, s'est progressivement imposé comme l'un des modèles de référence les plus utilisés dans le monde industriel. Développé à l'origine pour décrire l'architecture des systèmes d'automatisation, il est aujourd'hui largement repris dans les démarches de cybersécurité industrielle, notamment comme support de réflexion pour la segmentation des réseaux, l'analyse des flux et la mise en œuvre d'une défense en profondeur.

Le principe est simple : représenter l'architecture industrielle sous la forme de plusieurs niveaux hiérarchiques, chacun correspondant à de grandes fonctions au sein du système de production.

Les niveaux les plus bas regroupent les équipements directement connectés au procédé industriel : capteurs, actionneurs, moteurs ou automates. En remontant progressivement dans l'architecture, on retrouve les systèmes de supervision, les postes d'exploitation, les serveurs industriels, puis les applications de gestion de la production. Enfin, les niveaux supérieurs correspondent au système d'information de l'entreprise, où coexistent les applications métiers, les outils décisionnels ou encore les services informatiques traditionnels.

Entre les environnements industriels (OT) et le système d'information (IT), une zone intermédiaire, souvent appelée Industrial DMZ (niveau 3.5), joue un rôle essentiel. Véritable zone tampon, elle permet de contrôler les échanges entre ces deux mondes, de limiter les mouvements latéraux et de renforcer la sécurité des accès tout en préservant les contraintes opérationnelles des installations.

Bien que les architectures industrielles évoluent aujourd'hui vers des environnements plus distribués, intégrant le cloud, l'IIoT ou encore les accès distants sécurisés, **le Purdue Model demeure un langage commun largement partagé par les industriels, les intégrateurs et les acteurs de la cybersécurité.**

Positionner les solutions pour mieux comprendre leur complémentarité

Le *Purdue Model* constitue un support particulièrement pertinent pour représenter la place des différentes solutions de cybersécurité au sein d'une architecture industrielle. **C'est pourquoi nous avons choisi de positionner les offres des membres d'Hexatrust selon les principaux niveaux du modèle.**

Cette représentation n'a pas vocation à définir une architecture cible ni à recommander une solution plutôt qu'une autre. Son objectif est avant tout pédagogique : aider le lecteur à visualiser où interviennent les différentes technologies et comment elles contribuent, chacune à leur niveau, à la sécurisation des systèmes industriels.

Certaines solutions protègent directement les équipements de terrain ou les réseaux industriels ; d'autres sécurisent les accès distants, assurent la supervision des communications, renforcent les mécanismes d'authentification, protègent les échanges entre les différents niveaux de l'architecture ou accompagnent les équipes dans le maintien en condition de sécurité. De la même manière, les sociétés de conseil, d'intégration et de services interviennent de façon transverse sur l'ensemble de ces environnements.

Cette cartographie illustre également un principe fondamental de la cybersécurité industrielle : la sécurité ne repose jamais sur un composant unique, mais sur la combinaison de plusieurs mesures complémentaires mises en œuvre à différents niveaux de l'architecture. Cette approche, souvent qualifiée de défense en profondeur, vise à limiter les possibilités de compromission tout en renforçant la capacité des organisations à détecter, contenir et répondre aux incidents.

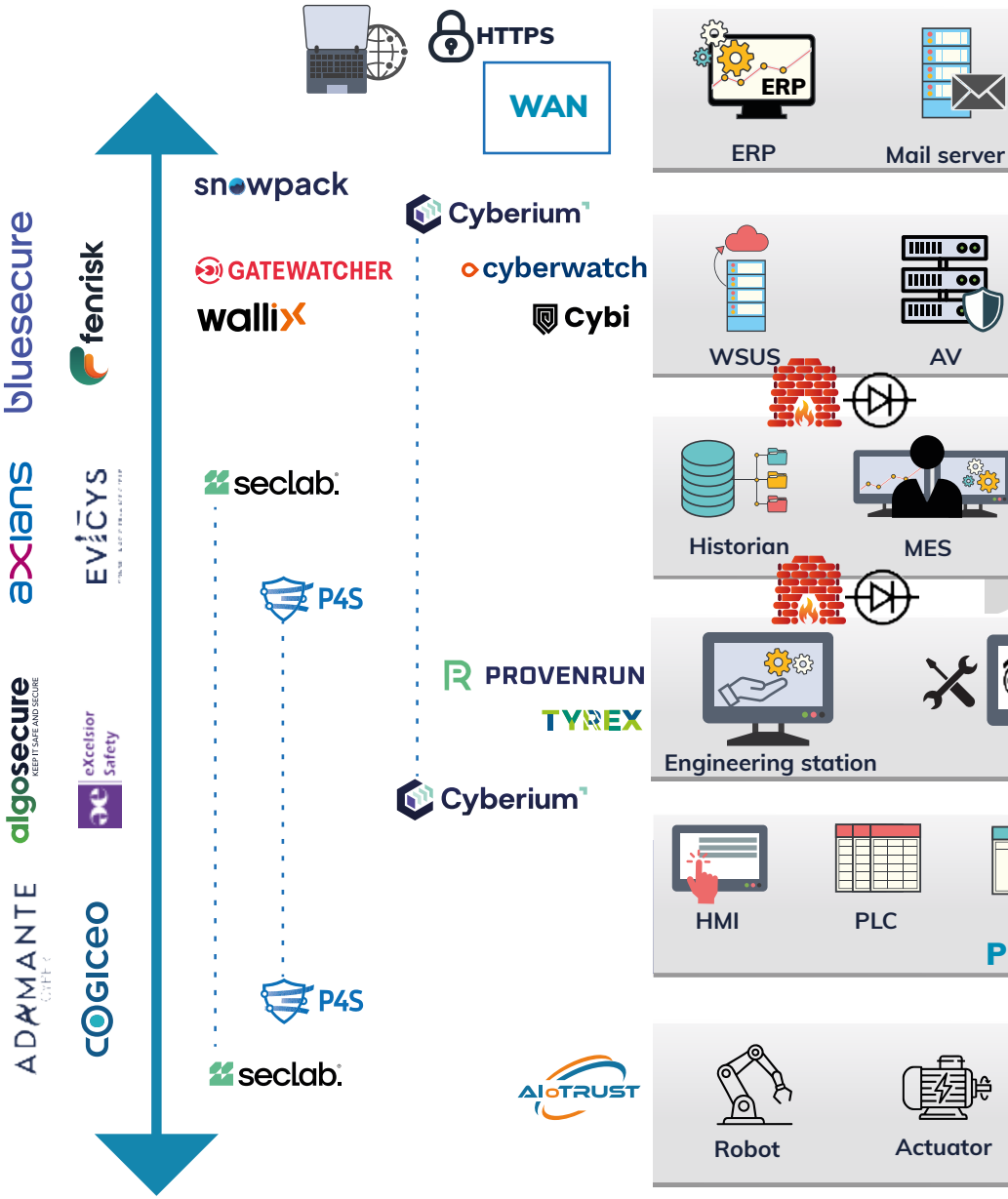
Les positionnements proposés doivent donc être considérés comme des repères de lecture. Certaines offres couvrent naturellement plusieurs niveaux du Purdue Model ou plusieurs fonctions de sécurité, tandis que les besoins des industriels varient selon leur secteur d'activité, leur niveau de maturité et les contraintes propres à leurs installations.

REPÈRES

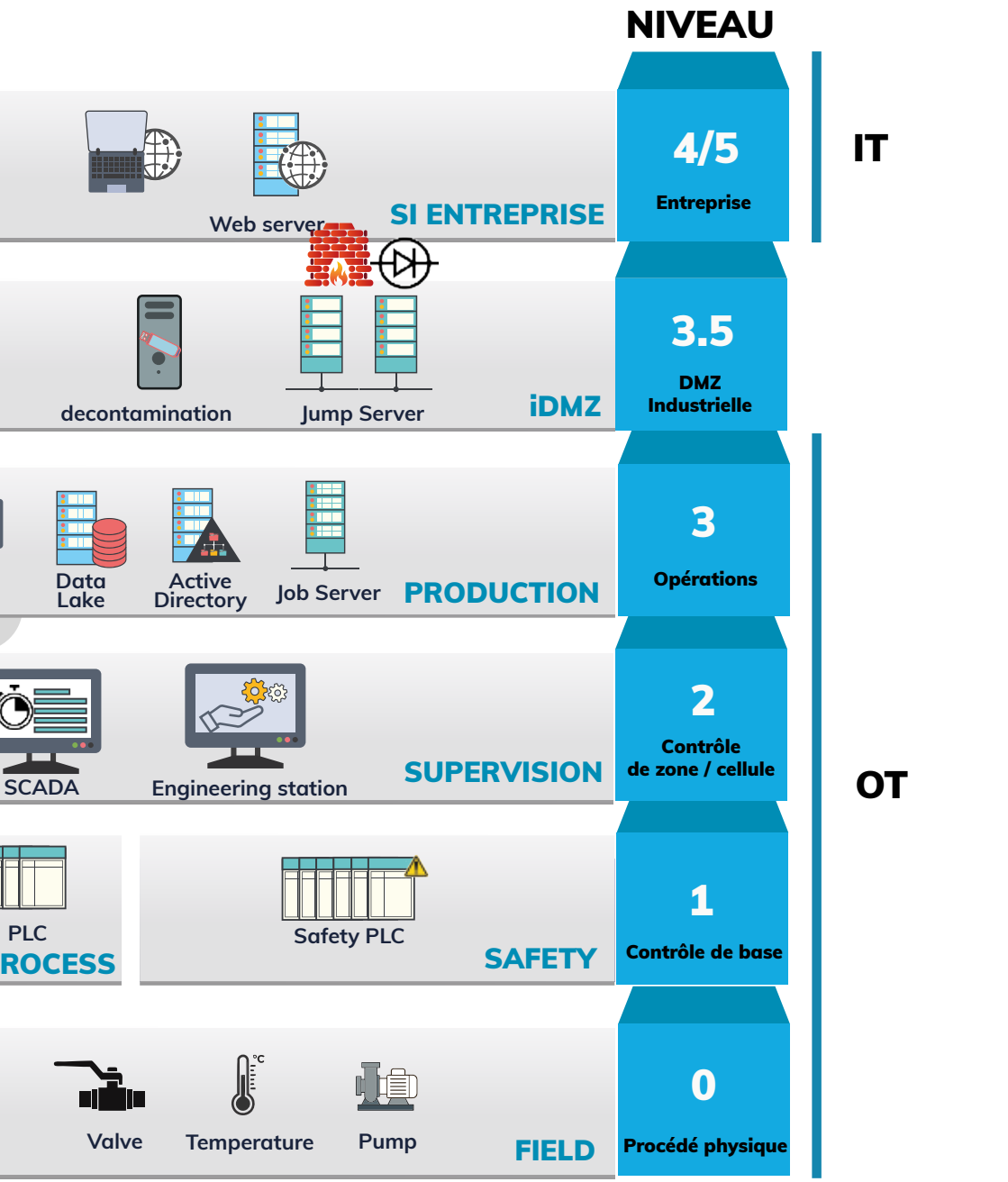
Les niveaux du Purdue Model

Niveau 0 : procédé physique (capteurs, actionneurs, équipements).
Niveau 1 : contrôle de base (API/PLC, automatismes).
Niveau 2 : supervision et conduite (IHM, SCADA).
Niveau 3 : gestion des opérations industrielles (MES, historisation, ingénierie).
Niveau 3.5 : DMZ industrielle, zone d'échange sécurisée entre OT et IT.
Niveaux 4/5 : système d'information de l'entreprise (ERP, métiers, bureautique).

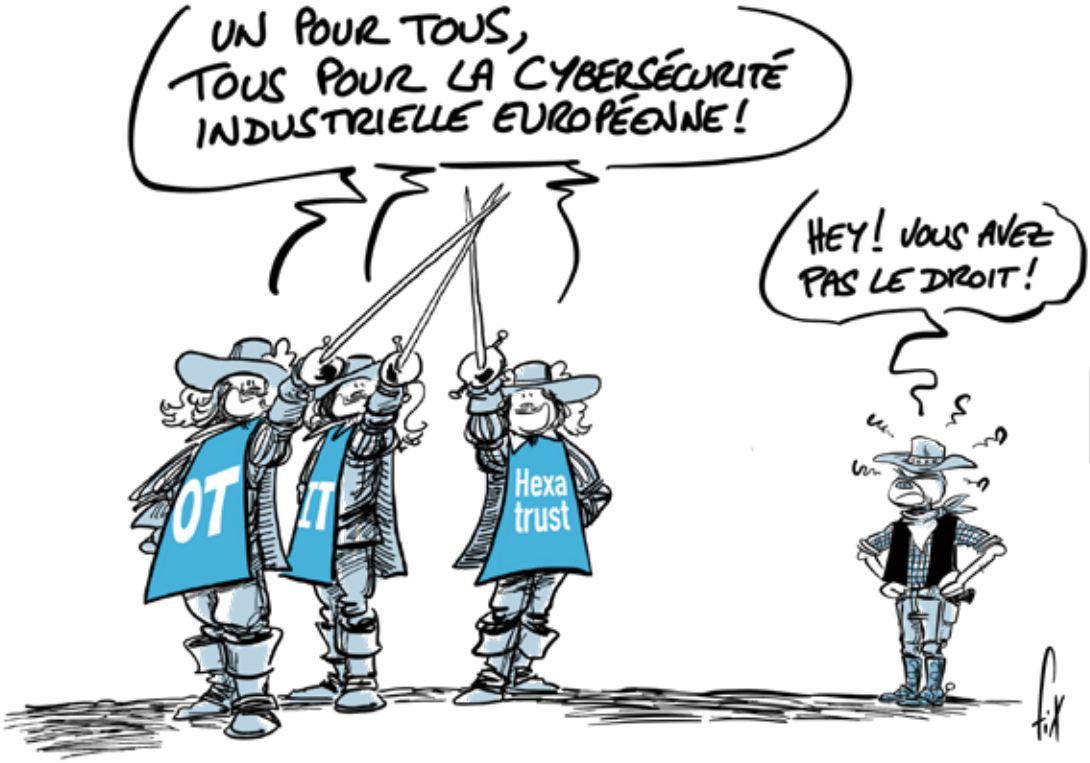
Vision technique de l'écosystème Hexatrust selon



le *Purdue Model for ICS Security*



L'union fait la force !



PARTIE III

TÉMOIGNAGES ET CAS D'USAGES

ADAMANTE CYBER

Adamante cyber est une société française spécialisée en cybersécurité des systèmes industriels. Nous accompagnons les industriels et opérateurs critiques dans l'audit, la sécurisation et la validation de leurs environnements OT, avec une expertise forte en simulation industrielle réaliste, détection des menaces et validation opérationnelle des capacités SOC OT.

Validation des capacités de détection SOC OT par simulation industrielle réaliste appliquée aux infrastructures critiques dans le secteur de l'énergie.

Besoin

Le client, acteur majeur du secteur énergétique, souhaitait évaluer la capacité de son SOC OT à détecter des comportements malveillants réalistes dans un environnement industriel représentatif, sans risque pour la production.

L'objectif était également de valider les règles de détection, les mécanismes de supervision et les processus de traitement des alertes.

Solution

Adamante cyber a conçu un environnement de simulation industrielle reproduisant plusieurs infrastructures énergétiques interconnectées, intégrant équipements OT, supervision SCADA et protocoles industriels.

Cet environnement a été connecté aux outils de supervision du SOC OT d'ENGIE afin d'exécuter plusieurs scénarios d'attaque réalistes et déterministes, et valider les capacités de détection, corrélation et traitement des incidents cyber sur des cas d'usage représentatifs.

Bénéfices

Cette approche a permis au client de tester ses capacités SOC OT dans un environnement réaliste sans impact sur les systèmes de production. Les scénarios simulés ont permis de confirmer certaines capacités de détection, identifier des axes d'amélioration sur les règles de corrélation et valider les chaînes de supervision et de traitement des alertes. Le projet a également renforcé la collaboration entre équipes cybersécurité et opérationnelles autour de cas d'usage industriels concrets, reproductibles et adaptables à différents contextes d'infrastructures critiques énergétiques, avant déploiement ou incident réel.

AIoTRUST

AIoTrust apporte une solution souveraine de cyber résilience dédiée aux infrastructures industrielles. L'approche est fondée sur l'analyse des signaux physiques de mesure et de commande des équipements. Elle permet de détecter en temps réel anomalies, falsifications et actions malveillantes, grâce à un traitement local, hors du réseau ICS.

Surveillance d'un sous-système industriel critique pour assurer la continuité des process sur tout un site de production.

Besoin

Un process critique demande qu'un fluide stocké dans un réservoir alimentaire soit toujours disponible pour le process. Bien que celui-ci dispose de capteurs de niveaux haut et bas, le client doit pouvoir réagir immédiatement si le dispositif de pompage ou de relevage s'active suite à une attaque visant à paralyser la production du site industriel.

Solution

Nous avons mis en place une solution permettant de monitorer les commandes des deux pompes et des différents capteurs de niveau, totalement indépendamment du système de contrôle installé. Des règles ont été mises en place pour alerter immédiatement l'exploitant si des commandes sont envoyées dans le but de paralyser la production, soit en vidant totalement la cuve, soit en la faisant déborder.

Bénéfices

AIoTRUST a apporté une solution simple de remontée d'alerte en cas d'anomalie sur un élément critique de production, sans impacter le process et le dispositif en place. En cas de compromission de l'automate ou de l'ICS, celui-ci peut paralyser la production, tout en renvoyant au SCADA ou au SIEM des données caractéristiques d'un fonctionnement normal. Notre système apporte un niveau de sécurité supplémentaire car il permet de détecter en temps réel toute anomalie en se basant sur des données non-falsifiables.

algosecure
KEEP IT SAFE AND SECURE

AlgoSecure est un cabinet français indépendant, qualifié PASSI et certifié ISO 27001, expert en cybersécurité. Il accompagne les industriels dans la sécurisation des environnements OT et IT/OT, l'évaluation des risques cyber et la définition de plans d'actions concrets pour renforcer la résilience et la continuité d'activité.

Audit d'un processus de maintenance d'automate industriel.

Besoin

Un industriel (secteur industrie lourde) a souhaité évaluer la sécurité de son processus de maintenance de ses automates.

L'objectif était de vérifier la maîtrise des accès, la segmentation entre les réseaux IT et OT et assainir les processus de maintenance d'un point de vue sécuritaire.

Solution

AlgoSecure a réalisé un audit complet des processus de maintenance OT, combinant évaluation technique, analyse documentaire et entretiens de l'architecture industrielle :

- Cartographie des actifs et des flux liés à la maintenance.
- Analyse des accès distants et des comptes à privilèges.
- Évaluation de la segmentation IT/OT.
- Revue des procédures de gestion des automates.
- Recommandation d'un plan d'actions.

Bénéfices

- Renforcement de la gouvernance des opérations de maintenance OT.
- Amélioration de la traçabilité des interventions sur les automates industriels.
- Réduction des risques liés aux accès non maîtrisés et aux connexions distantes.
- Réduction du risque d'incident cyber pouvant entraîner un arrêt de production, une altération des procédés industriels ou une perte de disponibilité des équipements critiques.

Axians, marque de Vinci Energies, accompagne les industriels agroalimentaires dans la convergence IT/OT, la cybersécurité et les services managés. Avec Actemium, spécialiste des environnements OT, Axians sécurise les sites de production critiques, multisites et internationaux, et leur performance opérationnelle.

Sécurisation cyber OT d'un groupe agroalimentaire multisite : GRC, cartographie, convergence IT/OT et support MSSP.

Besoin

Pour un groupe agroalimentaire multisite et multinational, disposer d'une vision complète de la posture cyber OT nécessite d'évaluer la gouvernance, les risques et la conformité, de cartographier les actifs et flux, puis de sécuriser la convergence IT/OT.
L'enjeu est aussi d'organiser un accompagnement MSSP au quotidien pour exploiter, superviser et maintenir durablement les dispositifs de sécurité.

Solution

Axians, avec Actemium pour l'expertise terrain OT, conduit une analyse GRC complète, déploie des solutions de cartographie des actifs et flux industriels, renforce la convergence IT/OT par la segmentation, les accès sécurisés et l'intégration des contrôles, puis assure via son dispositif MSSP la supervision, le traitement des alertes et le support opérationnel quotidien des équipes du client.

Bénéfices

Le client bénéficie d'une vision consolidée de sa posture cyber sur l'ensemble de ses sites, d'une meilleure maîtrise des risques, des dépendances et d'une convergence IT/OT plus sûre. La cartographie facilite la priorisation des actions, l'industrialisation des standards et le pilotage international. Le support MSSP renforce la détection, la réactivité, la continuité d'activité et l'accompagnement quotidien des équipes locales sur les sujets de cybersécurité.

bluesecure

BlueSecure est une plateforme française de sensibilisation à la cybersécurité. Hébergée en France, conforme au RGPD et certifiée Qualiopi, elle combine simulations de phishing multicanal, micro-learning gamifié et pilotage du risque humain. Elle aide à transformer les comportements des équipes, du bureau au terrain industriel.

Chez ENEDIS, la réalité virtuelle sensibilise les opérateurs aux risques cyber directement dans l'environnement industriel.

Besoin

Dans le cadre de son programme de sensibilisation, ENEDIS souhaitait toucher les opérateurs travaillant dans les postes source avec un format contextualisé et engageant.

L'enjeu : permettre à ses équipes de terrain de se projeter dans un environnement fidèle à leur quotidien, là où l'e-learning classique mobilise difficilement ces populations.

Solution

BlueSecure a conçu un environnement de réalité virtuelle entièrement modélisé en 3D, fidèle à un poste source. Le collaborateur doit y repérer six éléments porteurs d'un risque pour la sécurité de l'information.

À chaque indice trouvé, un mini-quiz s'affiche, suivi de la justification de la bonne réponse. Le dispositif est déployable sur site, par sessions de dix minutes.

Bénéfices

ENEDIS déploie ce dispositif directement sur les lieux de travail, pendant la pause déjeuner ou lors de sessions planifiées, pour atteindre des opérateurs difficiles à mobiliser par les formats classiques. Immergés dans un contexte familier intégrant des risques réels et proches de leur activité, les collaborateurs adhèrent plus facilement. Le format court, déployé sans déplacer les équipes, limite l'impact sur l'activité. Cette mise en situation favorise l'engagement et la mémorisation durable des bons réflexes et ancre une culture de sécurité partagée entre équipes IT et de terrain.

Depuis 2012, Cogiceo est une société indépendante d'audits de cybersécurité, spécialisée en tests d'intrusions, RedTeam et sécurité de l'Active Directory. Qualifiée PASSI niveau élevé sur l'ensemble des activités (organisationnel et physique, architecture, configuration, code source, tests d'intrusion), Cogiceo intervient très fréquemment en environnements industriels et périmètres OT.

Réalisation d'audits de cybersécurité des réseaux industriels de plusieurs usines situées en Europe de l'Est pour un équipementier automobile.

Besoin

Le client souhaitait vérifier le cloisonnement entre les réseaux IT, OT et Wi-Fi, contrôler l'accessibilité des équipements OT depuis les différents sites et réseaux et s'assurer que seuls les équipements identifiés et autorisés pouvaient communiquer sur le réseau industriel.

L'audit visait également à identifier les équipements OT vulnérables ou obsolètes.

Solution

Les auditeurs ont réalisé des tests de segmentation et de connectivité entre les réseaux IT, OT et Wi-Fi afin d'évaluer le cloisonnement et les chemins d'accès vers les équipements industriels. Ils ont cartographié l'ensemble des éléments accessibles depuis le réseau OT et réalisé un inventaire des actifs afin d'identifier les équipements présents, inconnus ou non autorisés, ainsi que les versions logicielles et systèmes détectés.

Bénéfices

Cet audit a permis au client d'obtenir une cartographie précise de l'exposition de ses infrastructures OT et des flux associés. Les analyses ont révélé plusieurs interconnexions entre les sites industriels, augmentant les surfaces d'exposition potentielles. Des pare-feux protégeant certaines lignes de production présentaient des défauts de configuration majeurs. L'audit a également mis en évidence un manque de contrôle d'accès au réseau, ainsi que la présence d'équipements OT vulnérables, obsolètes ou issus de déploiements d'urgence réalisés durant la période Covid. Ces constats ont permis de définir des actions prioritaires de sécurisation.

Cyberium

Cyberium est une start-up française spécialiste de la segmentation réseau basée sur du matériel, pour les environnements critiques (OT, défense, infrastructures vitales). Complémentairement aux pare-feux, Cyberium propose une barrière physique inviolable combinée à un logiciel multi-protocoles, pour sécuriser la convergence IT/OT sans compromis sur la protection ni sur l'opérabilité.

Automatisation sécurisée de la gestion des correctifs OT pour un opérateur de distribution de gaz en environnement air-gap.

Besoin

Un opérateur de distribution de gaz devait maintenir à jour ses systèmes OT dans un réseau isolé d'Internet.

La gestion manuelle des correctifs WSUS entre IT et OT générait des surcharges opérationnelles, des risques de corruption et des vulnérabilités non patchées, tout en devant répondre aux exigences réglementaires NIS2 et LPM.

Solution

Cyberium a déployé sa solution OWA (One-Way-Appliance) à 1 Gbps, créant une architecture unidirectionnelle stricte entre l'environnement IT et le réseau OT isolé. Un connecteur SFTP assure le transfert fiable des paquets de mise à jour validés. Un agent de synchronisation WSUS dédié automatise la réplication des dépôts Microsoft vers l'OT, sans établir de connexion entrante bidirectionnelle et donc sans risque de compromission du réseau opérationnel.

Bénéfices

Le déploiement a permis à l'opérateur d'automatiser intégralement la gestion des correctifs OT, sans intervention manuelle ni rupture du niveau de sécurité permis par la séparation air-gap. Les bénéfices sont multiples : conformité totale aux réglementations NIS2 et LPM, élimination des risques de corruption lors des transferts de fichiers volumineux, suppression d'une solution tierce peu fiable et réduction significative de la charge opérationnelle des équipes IT/OT. La barrière physique de Cyberium garantit que le réseau de contrôle reste strictement masqué du réseau IT et évite les risques liés à une éventuelle compromission de l'environnement IT.

cyberwatch

Cyberwatch est un éditeur de logiciel français créé en 2015, acquis par Framatome en 2022, spécialiste de la gestion des vulnérabilités et de la conformité.
Cyberwatch accompagne tout type de clients (secteur privé, public, CAC40, PME, ETI, ministères régaliens, ...) dans la supervision des vulnérabilités et de la conformité.

Gestion de la vulnérabilité et de la conformité dans les environnements industriels et OT de façon générale.

Besoin

Les clients souhaitent utiliser des gestionnaires de vulnérabilité afin de remonter les vulnérabilités critiques présentes sur leurs systèmes industriels et OT. Cependant ces systèmes sont extrêmement sensibles et un scan standard tel qu'il serait effectué en environnement IT pourrait faire tomber le système OT et avoir un impact extrêmement important sur la production du client.

Solution

Cyberwatch propose des scans non intrusifs appelés Safe Queries. Ils peuvent avoir plusieurs formes : scans SNMP dédiés OT, scans Air gap, scans via protocoles dédiés (S7, Modbus, ...) ou bien s'interfacer avec des sondes OT du marché afin de récupérer les informations sur les actifs présents sans effectuer le moindre scan.
Cyberwatch est compatible avec tous les environnements OT principaux du marché et peut en ajouter de nouveaux à la demande.

Bénéfices

Le client peut avoir confiance dans la solution Cyberwatch et sait qu'avec cette solution il réduit grandement les risques liés aux scans standards du marché. Un autre enjeu majeur : la remédiation. Celle-ci ne peut se faire généralement qu'une à quatre fois par an ou ponctuellement en cas de faille critique. Cyberwatch vous aide à bien identifier l'ensemble des patchs nécessaires lors de la mise à jour annuelle, semestrielle ou trimestrielle. Et dans le cas où une intervention ponctuelle serait nécessaire, Cyberwatch vous aide via le module de priorisation 3D à bien identifier les vulnérabilités les plus critiques ne pouvant pas attendre.

Cybi

Issue des laboratoires du LORIA et d'Inria, CyBi développe une technologie brevetée d'IA défensive qui modélise les chemins d'attaque réels. CyBi transforme les données de cybersécurité en décisions, en identifiant les actions offrant le meilleur gain de sécurité pour chaque euro et chaque heure investis.

Un hôpital privé de l'Ouest de la France décide d'isoler ses matériels médicaux et de gérer ses vulnérabilités.

Besoin

Dans un environnement hospitalier mêlant systèmes d'information et équipements médicaux critiques, souvent non patchables, le RSSI devait réduire le risque cyber malgré des ressources limitées.

Il recherchait une solution capable de prioriser les remédiations et de recommander les mesures compensatoires les plus pertinentes.

Solution

Accompagné par son MSSP, cet hôpital privé a choisi la plateforme Scuba de CyBi pour transformer les données de cybersécurité en décisions opérationnelles.

L'analyse des chemins d'attaque et l'IA de priorisation ont permis d'identifier les actifs réellement critiques et de guider les équipes vers les actions de remédiation les plus efficaces.

Bénéfices

Les bénéfices ont été immédiats. Le temps consacré à l'analyse des vulnérabilités et à la planification des remédiations est passé de plusieurs semaines à quelques jours, permettant aux équipes IT de se concentrer sur des actions à forte valeur ajoutée. Au-delà d'une meilleure gestion des correctifs, Scuba a permis de protéger efficacement les équipements médicaux non patchables en identifiant et en neutralisant, en amont, les chemins d'attaque susceptibles de les atteindre. Cette approche a renforcé la continuité d'activité, réduit les interruptions du système d'information et optimisé l'utilisation des ressources humaines et financières, tout en améliorant durablement le niveau global de sécurité.

Evicys est un cabinet de conseil spécialisé dans la cybersécurité industrielle (OT) et des systèmes d'information. Nous accompagnons les entreprises dans la sécurisation de leurs infrastructures critiques, la gestion des risques cyber et la conformité réglementaire, en alliant expertise technique de pointe et approche stratégique sur mesure pour protéger leurs actifs.

Sécurisation et mise en conformité réglementaire des infrastructures d'automatisme et des systèmes d'information industriels (OT) d'un site de production critique.

Besoin

Le client, exploitant d'infrastructures critiques, devait cartographier ses actifs industriels et évaluer la vulnérabilité de ses réseaux d'automatisme face aux cybermenaces.

Son besoin principal consistait à se mettre en conformité avec les réglementations de sécurité tout en garantissant la continuité de sa production et la disponibilité de ses outils industriels.

Solution

Evicys a déployé une démarche globale combinant audit d'architecture et analyse des risques industriels. Nous avons cartographié les flux, segmenté les réseaux OT et mis en place des solutions de détection des menaces adaptées aux contraintes de production.

Enfin, nous avons rédigé les politiques de sécurité (PSSI-OT) et accompagné les équipes dans l'adoption des bonnes pratiques de cyberrésilience.

Bénéfices

Grâce à l'intervention d'Evicys, le client bénéficie d'une gouvernance cyber robuste et d'une conformité réglementaire totale, éliminant les risques de sanctions. Sur le plan opérationnel, la segmentation des réseaux et la détection des menaces garantissent la continuité d'activité des lignes de production contre les propagations de malwares. La maîtrise de la cartographie assure une gestion optimisée des dépendances avec les tiers et les maintenanciers, et permet d'avoir un inventaire des actifs de la chaîne de production. Enfin, la résilience globale du site est considérablement renforcée, protégeant l'outil industriel, les collaborateurs et l'image de marque de l'entreprise face aux crises cyber.

eXcelsior Safety

Forts de 25 ans d'expertise terrain en sécurité fonctionnelle (IEC 61508/61511) et cybersécurité OT (IEC 62443), nous accompagnons vos équipes dans la maîtrise des risques, la gouvernance cyber, les audits de conformité et le déploiement de solutions opérationnelles avec un plan de continuité robuste pour sécuriser votre activité.

Conformité aux standards internationaux, gestion des risques : rassurez les investisseurs, les assureurs et les régulateurs avec des pratiques cyber irréprochables.

Besoin

Réduire les risques industriels, satisfaire les auditeurs institutionnels et répondre aux exigences légales propres à chaque pays et à chaque zone de production. Comment harmoniser la gouvernance cyber et contraintes opérationnelles dans les zones de production internationales, pour une conformité solide sans compromis sur la performance ?

Solution

Prise de connaissance des systèmes opérationnels du client et de ses procédures en mode opérationnel, analyses des risques et du GAP versus standard IEC62443-2-1, entretiens avec les différents services opérationnels et pays, recommandations techniques et organisationnelles, mise en place d'une politique et stratégie d'un planning de déploiement suivant les urgences et le niveau d'investissement possible.

Bénéfices

Le client a ainsi pu bénéficier d'une gouvernance du risque dans son intégralité, en étant accompagné par des experts métier qui s'appuient sur une longue connaissance et expérience des processus industriels, et sur une approche pragmatique qui tient compte des besoins opérationnels et adaptée à toutes les structures. D'autres bénéfices ont également été obtenus pour le client : accès à un networking et à des solutions techniques adaptées, mise en place d'un processus d'amélioration continue et d'indicateurs de mesure, aide à la réorganisation structurelle de l'entreprise, et renforcement du PCA/PRA afin de pallier toute situation liée aux zones géographiques diverses et activités critiques.

Fenrisk conjugue audit offensif et recherche en vulnérabilités. Ses chercheurs découvrent et publient des failles inédites dans des produits largement déployés. Cette pratique nourrit directement les missions : chaque évaluation est conduite manuellement, jusqu'à l'exploitation effective, des applications web aux environnements industriels. Une sécurité éprouvée par démonstration, non par conformité.

Test d'isolation sur des infrastructures industrielles critiques et shadow IT en bonus.

Besoin

Le client, industriel de premier plan, effectue des tests réguliers sur l'intégralité de ses périmètres industriels. Construites en autonomie partielle par les équipes locales à chaque site, les missions sont toutes différentes.

Le risque principal est l'arrêt de la production sans planification : on estime à un mois la perte engendrée par tout arrêt inopiné en dehors des fenêtres de maintenance.

Solution

Depuis un simple accès physique au réseau bureautique de l'usine, sans aucun compte, Fenrisk compromet plusieurs postes de collaborateurs ayant accès au périmètre industriel, puis y pénètre par une route non documentée. Nos experts y découvrent un équipement 4G, posé par les équipes locales pour alerter les astreintes, mal configuré, qui expose ainsi le périmètre OT sur Internet, via une vulnérabilité découverte aussi par nos chercheurs. Après fourniture du rapport d'audit détaillé, le client a remédié à cette exposition critique.

Bénéfices

Ce scénario démontre un risque concret là où les audits classiques s'arrêtent à la théorie : une chaîne complète menant du réseau bureautique au cœur OT, sans identifiant initial, révélant la dépendance à des tiers mal maîtrisés et le shadow IT industriel. Pour le RSSI commanditaire, le rapport devient un outil pédagogique auprès des équipes des sites de production, souvent éloignées des enjeux de sécurité. Il offre surtout un levier pour amener progressivement une véritable structuration et harmonisation de la sécurité de ses périmètres OT, en priorisant ce qui menace réellement la continuité de production.

GATEWATCHER

Gatewatcher est un éditeur français de cybersécurité (certifié & qualifié par l'ANSSI) spécialisé dans la détection et la réponse réseau (NDR). Sa plateforme analyse les flux IT, IoT, OT, Biomed en temps réel grâce à plusieurs technologies de détection embarquées (IA, ML, AV, CTI) pour identifier les menaces avancées et ainsi protéger les infrastructures critiques.

Visibilité unifiée IT/OT dans une infrastructure industrielle critique : détection précoce des cybermenaces sur les réseaux de production.

Besoin

Un opérateur d'infrastructure critique dans le secteur de l'énergie devait sécuriser des environnements OT hétérogènes regroupant automates industriels, SCADA et systèmes de supervision, cloisonnés, mais interconnectés au SI d'entreprise. L'absence de visibilité sur les flux est-ouest et l'incapacité à détecter des mouvements latéraux constituaient des angles morts significatifs face à des attaquants ciblant spécifiquement les systèmes de contrôle industriels.

Solution

Les sondes réseau NDR de Gatewatcher ont été positionnées sur les segments réseau OT et IT, sans perturbation des systèmes de production. Ce positionnement a permis une cartographie exhaustive des actifs du système d'information afin d'éliminer les problématiques de shadow IT/OT.

La corrélation automatique des événements offre une vision unifiée des incidents IT/OT et accélère ainsi leur qualification par les équipes SOC.

Bénéfices

L'opérateur a recouvré une visibilité complète sur l'ensemble de ses flux IT/OT, permettant pour la première fois d'identifier des connexions anormales aux automates. La continuité d'activité a ainsi été préservée par l'intégration de la solution NDR avec zéro impact sur les systèmes de contrôle. L'opérateur répond désormais aux exigences de la directive NIS2, dispose d'une traçabilité complète des incidents et renforce sa résilience face aux menaces cyber, même avancées (APT) ciblant le secteur de l'énergie.

P4S développe des solutions de cybersécurité réseau 100% matérielles, conçues et produites en France. Grâce à sa technologie souveraine SOFTLESS, sans système d'exploitation, ses équipements intègrent les fonctions de chiffrement, pare-feu, anti-DDoS et Health Monitoring, garantissant une sécurité renforcée, une latence minimale et une conformité aux exigences NIS2.

La direction des routes d'Île-de-France (DiRIF) souhaite protéger les postes d'appel d'urgence (PAU) et chiffrer leurs communications.

Besoin

La Direction des Routes d'Île-de-France (DiRIF) souhaite renforcer la cybersécurité de ses Postes d'Appel d'Urgence (PAU) afin de garantir la disponibilité du service, protéger les équipements contre les cyberattaques et assurer la confidentialité des communications entre les PAU et les centres d'exploitation.

Solution

La DiRIF a choisi P4S pour protéger ses équipements et les flux de données. Un SF-106-2 sera positionné entre chaque PAU et le réseau de communication. Des SF-106-8 seront positionnés dans chaque centre de supervision. Le SF-106-2 et le SF-106-8 sécuriseront les flux dès leur émission avec leurs fonctions de chiffrement/déchiffrement, pare-feu, protection Anti-DDoS. Les équipements sont protégés et les communications sont chiffrées sans avoir à modifier l'infrastructure du réseau existant.

Bénéfices

Toutes les communications entre les PAU et le centre d'exploitation sont chiffrées de bout en bout. Les PAU sont protégés contre les tentatives d'intrusion réseau, les scans malveillants, les attaques en DDoS et les accès non autorisés. Grâce à l'architecture 100% hardware P4S, il y a une latence extrêmement faible permettant un fonctionnement en temps réel et une utilisation de 100% de la bande passante. Le déploiement est simple car il ne demande aucune modification des PAU et l'installation est complètement transparente sur l'infrastructure réseau actuelle. Enfin, P4S contribue à la conformité NIS2 car les équipements permettent de renforcer la résilience des infrastructures critiques, de protéger les flux et d'améliorer la visibilité et la supervision des équipements.

PROVENRUN

ProvenRun développe des solutions de cybersécurité de confiance pour les systèmes critiques. Nos technologies s'appuient sur ProvenCore, OS formellement prouvé et certifié Common Criteria EAL7 et sur ProvenHSM, un HSM souverain conçu pour protéger les clés, certificats, secrets et opérations cryptographiques critiques.

Sécuriser les identités machines et la signature de firmware dans les environnements industriels critiques.

Besoin

Un industriel exploitant plusieurs sites OT doit sécuriser les identités machines, les certificats, les secrets applicatifs et les firmwares utilisés dans ses environnements industriels.

Les clés sont parfois stockées en logiciel ou réparties localement, ce qui complexifie leur renouvellement, leur traçabilité et la protection de la chaîne de mise à jour.

Solution

ProvenHSM est déployé comme racine de confiance cryptographique.

Il protège les clés privées, les certificats et les secrets critiques dans un HSM souverain, administrable à distance, tout en permettant de sécuriser les échanges mTLS, les accès distants, la PKI industrielle et la signature de firmwares avant leur déploiement en zone OT.

Bénéfices

Le client réduit son exposition aux secrets logiciels et renforce l'authentification des équipements, services et prestataires intervenant dans l'environnement OT. ProvenHSM apporte un point de contrôle centralisé pour les opérations cryptographiques sensibles, tout en facilitant la gestion multisites des certificats et des signatures.
La solution améliore l'intégrité de la chaîne de mise à jour, limite les risques d'usurpation ou d'injection de code et contribue à l'alignement avec les recommandations ANSSI, l'IEC 62443 et les exigences de conformité cyber industrielle.

Seclab est un éditeur/constructeur français qui propose une plateforme de cybersécurité OT conçue pour protéger les infrastructures industrielles sans perturber les opérations. Seclab Xcore Platform offre visibilité et cartographie des actifs, protection USB et isolation réseau par Electronic Air Gap, détection continue des anomalies et des attaques.

Sourcéo sécurise l'eau potable d'un million d'habitants grâce à une visibilité totale sur ses réseaux OT.

Besoin

En charge de la production d'eau potable pour la Métropole Européenne de Lille, Sourcéo exploite des réseaux OT complexes et partiellement documentés.

Ses équipes avaient besoin d'une visibilité complète sur leurs infrastructures industrielles, d'une autonomie opérationnelle vis-à-vis de l'IT, et d'une mise en conformité NIS2, le tout avec une solution souveraine et française.

Solution

Sourcéo a déployé la solution Seclab Xplore et ses sondes pour superviser l'ensemble de ses sites industriels. Seclab Xplore apporte une cartographie en continu de ses réseaux OT, analyse les flux réseau et identifie proactivement les vulnérabilités.

La solution s'est intégrée facilement dans l'environnement industriel de Sourcéo, offrant aux équipes OT une interface claire et une prise en main rapide pour superviser jusqu'à 1 000 équipements connectés.

Bénéfices

Sourcéo dispose aujourd'hui d'une cartographie dynamique et temps réel de l'ensemble de ses réseaux industriels. Les équipes OT pilotent et sécurisent leurs infrastructures en toute autonomie, sans dépendre de l'IT. La détection proactive des vulnérabilités permet d'anticiper les incidents avant qu'ils n'impactent la production. La solution a également fluidifié la collaboration entre les équipes IT et OT, réduisant les frictions techniques et renforçant la sérénité opérationnelle au quotidien. Résultat : un réseau critique, complexe et vital, enfin pleinement maîtrisé.

snowpack

Snowpack, spin-off duale de cybersécurité du CEA, réduit drastiquement la surface d'attaque externe des systèmes d'information grâce à une technologie brevetée rendant invisibles sur Internet utilisateurs, données, applications et infrastructures. Seuls les utilisateurs autorisés les voient et y accèdent. Avec Snowpack, les attaquants ne vous voient pas, donc ils ne vous attaquent pas !

Accès distants invisibles aux SI industriels exposés sur Internet, et réduction drastique de la surface d'exposition.

Besoin

Un opérateur d'infrastructures énergétiques devait maintenir des capacités de télémaintenance et de télémétrie sur des sites industriels distants malgré des équipements d'accès hérités, une segmentation IT/OT limitée et une exposition directe sur Internet.

Cette configuration multipliait les vecteurs d'attaque et le risque de compromission des environnements industriels.

Solution

Déploiement des solutions Snowpack sur les sites industriels concernés afin de rendre invisibles les points d'entrée exposés sur Internet (services, serveurs et composants d'infrastructure). Les ressources ne deviennent accessibles qu'aux utilisateurs autorisés et lorsque c'est nécessaire, selon une approche Zero Trust, sans aucun port ouvert vers l'extérieur. Le dispositif renforce également le cloisonnement entre les zones exposées et les environnements industriels.

Bénéfices

La solution globale permet de maintenir en condition de sécurité des équipements qui ne peuvent plus être mis à jour, tout en préservant les capacités de télémaintenance et de remontée de télémétrie. Les points d'entrée exposés sur Internet deviennent invisibles et accessibles uniquement aux utilisateurs autorisés, aux moments voulus. Le déploiement est simple, avec un équipement Snowpack par site industriel protégeant l'ensemble des ressources en aval. Enfin, l'architecture réduit les coûts, la complexité opérationnelle et les contraintes d'exploitation des accès distants par rapport aux approches traditionnelles de sécurisation des accès distants.

Wallix est un éditeur européen de solutions de cybersécurité spécialisé dans la gestion des accès et des identités à privilèges. L'entreprise accompagne les organisations industrielles dans la sécurisation des accès aux systèmes critiques IT/OT, en conciliant exigences de cybersécurité, continuité des opérations et souveraineté.

Sécuriser les accès distants des prestataires et équipes internes aux environnements industriels sans dégrader les opérations.

Besoin

Les industriels doivent permettre l'accès distant aux fournisseurs et équipes de maintenance pour assurer la continuité des opérations.

Cependant, les accès VPN traditionnels exposent les systèmes OT à des risques élevés (mouvements latéraux, comptes partagés, manque de traçabilité) tout en étant complexes à opérer pour les équipes terrain.

Solution

La solution WALLIX Secure Remote Access pour OT permet de contrôler, sécuriser et tracer tous les accès distants sans déployer d'agent ni modifier les environnements industriels.

Elle repose sur une approche centralisée des identités et des privilèges, avec authentification forte, cloisonnement des sessions, enregistrement vidéo et contrôle en temps réel des accès aux équipements critiques.

Bénéfices

La solution améliore significativement la posture de sécurité en supprimant les accès directs et en garantissant une traçabilité complète des actions. Elle facilite également l'exploitation en simplifiant l'accès pour les utilisateurs et les prestataires, favorisant l'adoption. Enfin, elle contribue à la continuité d'activité en réduisant les risques d'incident et en permettant des interventions rapides et sécurisées, tout en répondant aux exigences réglementaires (NIS2, IEC 62443).

L'association en quelques mots...

L'UNION FAIT LA FORCE !

Hexatrust regroupe et fédère les champions français et européens de la cybersécurité, du cloud de confiance et des plateformes collaboratives.

L'association rassemble des startups, PME et ETI à la pointe de l'innovation : éditeurs de solutions de cybersécurité, fournisseurs de cloud de confiance (SaaS, PaaS, IaaS), intégrateurs, hébergeurs, avocats, courtiers en assurance, établissements de financement et acteurs publics.

Ce collectif incarne l'excellence technologique européenne, avec un portfolio de solutions de confiance assurant protection, transparence et efficacité. Présents à l'international, les membres d'Hexatrust déploient leurs technologies innovantes et expertises de pointe à travers le monde.

Bibliographie

ANSSI (11/03/2026) - *Panorama de la cybermenace 2025*
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf

ANSSI (11/04/2025) - *La cybersécurité des systèmes industriels - Méthode de classification*
https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels

ANSSI (30/05/2025) - *Approche SSI pour l'Internet des objets industriels :*
https://cyber.gouv.fr/publications/approche-ssi-pour-linternet-des-objets-industriels

CLUSIF (29/09/2025) - *Guide cybersécurité des systèmes industriels :*
https://clusif.fr/publications/guide-cybersecurite-des-systemes-industriels/

GIMELEC (12/03/2025) - *livre blanc dédié au Maintien en Condition de Sécurité (MCS) pour les systèmes industriels*
https://gimelec.fr/wp-content/uploads/2025/03/GIMELEC-Cyber-OT-Livre-blanc-MCS-2025-web.pdf

MITRE – *MITRE ATT&CK® for ICS*
https://attack.mitre.org/matrices/ics/

ISA - *ISA/IEC 62443 Series of Standards*
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Union Européenne - *NIS2 Directive*
https://eur-lex.europa.eu/eli/dir/2022/2555/oj

HEXATRUST, 5-7 rue Bellini, 92800 Puteaux
Date de publication : septembre 2026
Les crédits : FIX Illustration - AdobeStock : 1043451562, 1900510512
Imprimé en France par : SCV imprimeur

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

ADRESSE

5 rue Bellini

92800 Puteaux

CONTACT

contact@hexatrust.com

www.hexatrust.com

Les menaces évoluent rapidement. Les référentiels structurent les approches. Les technologies de confiance existent.

Ce livre blanc montre qu'un écosystème français et européen est aujourd'hui capable d'apporter des réponses complémentaires aux principaux défis de la cybersécurité industrielle.

L'enjeu n'est plus de rechercher une solution unique, mais de construire, collectivement, une architecture de confiance adaptée aux besoins de chaque organisation.