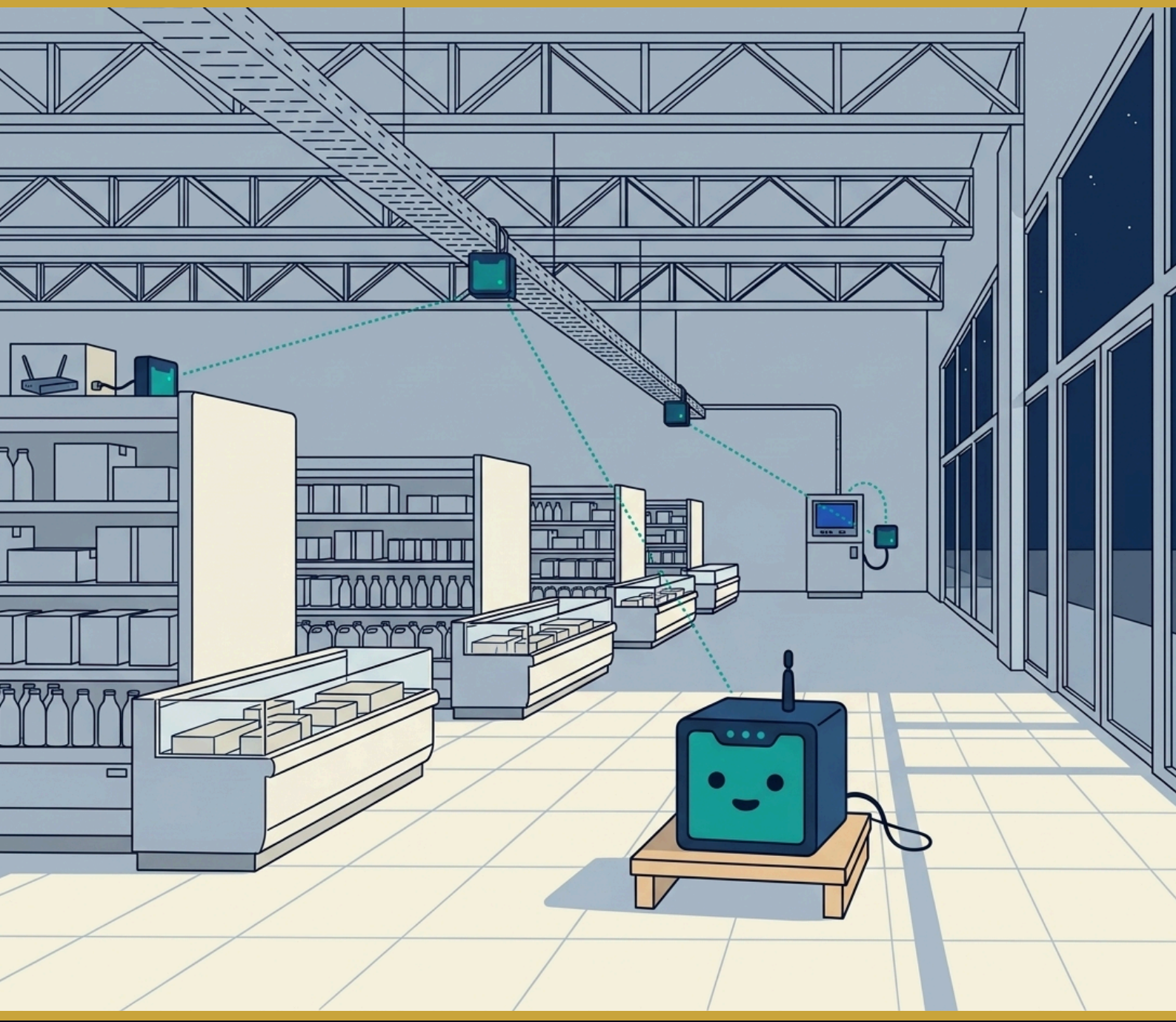
TRUST-BUSTER · ANALYSES ET SOLUTIONS PRÉCONISÉES

Une analyse à froid d'une affaire brûlante

Les frigos piratés de 2026 : ce que révèlent les attaques, et nos solutions pour reprendre la main sur la télémaintenance



Trust-Buster

© Novembre 2026 · trust-buster.fr

TRUST-BUSTER
POWERED BY OPS-DEVICES

Sommaire

	Avant-propos	3
Chapitre 1	Le dégivrage venu de loin	4
Chapitre 2	Pourquoi les frigos restaient ouverts	8
Chapitre 3	Observer sans lire : la légitimité d'un accès distant	12
Chapitre 4	Un satellite pour le Wi-Fi du magasin	16
Chapitre 5	Écouter sans pouvoir parler : les diodes sentinelles	20
Chapitre 6	Les règles du responsable de site : alerter, suspendre, révoquer	24
	Pour aller plus loin	28
	Sources	29

Avant-propos

Ce document s'adresse aux responsables de site, qu'il s'agisse d'un magasin, d'un atelier, d'une usine ou d'un entrepôt, aux frigoristes et prestataires de maintenance, et à tous les détenteurs d'équipements industriels connectés. Il part d'un cas réel : les attaques de l'automne 2026 contre les superviseurs de froid de la grande distribution. Nous n'avons pas vécu ces incidents sur le terrain, mais nous en avons connu de semblables dans des contextes tout aussi sensibles. Maintenant que l'agitation est retombée, voici notre analyse des faits et des problèmes, pour vous livrer un avis éclairé fondé sur notre compréhension et nos retours d'expérience.

Les chapitres 1 et 2 portent sur les faits et les failles. Ils rappellent ce qui s'est passé, trient ce qui en a été dit et expliquent pourquoi ces failles sont si difficiles à refermer.

Les chapitres 3 à 6 décrivent la façon dont nous l'abordons avec le Cube et ses satellites. Il s'agit d'observer les accès distants sans lire les échanges, de placer le superviseur derrière une seule porte, d'écouter les câbles sans pouvoir y écrire, puis d'appliquer les règles du responsable de site.

Ce document donne une information générale, pas un conseil adapté à votre installation. Toute modification d'une installation de froid se décide avec votre frigoriste, après avoir vérifié la garantie du constructeur, le contrat de maintenance et votre assurance.

L'équipe Trust-Buster, novembre 2026.

CHAPITRE 1

Le dégivrage venu de loin



Les faits

La nuit du 11 au 12 octobre, en France

L'attaque n'a pas visé les réfrigérateurs, mais les **superviseurs** qui les pilotent. Ils centralisent les régulateurs de chaque meuble et de chaque chambre froide. Ils relèvent aussi les températures et transmettent les alarmes. Enfin, ils pilotent les dégivrages. Le frigoriste s'y connecte à distance. Cette nuit-là, l'attaquant a porté leurs paramètres de dégivrage à des valeurs extrêmes. Les températures ont alors grimpé jusqu'à 50 °C dans certains cas. Selon le bilan de l'ANSSI, l'attaque a visé environ **700 sites**. Le même bilan compte au moins 15 départs de feu. Pour un magasin, cela peut signifier des denrées à jeter et un local à expertiser. S'y ajoute parfois un dossier chez l'assureur.

L'alerte du CERT-FR vise les superviseurs Danfoss AK-SM et AK-SC. Elle vise aussi les superviseurs XWEB de Dixell, marque du groupe Copeland. Elle désigne une cause principale : une interface d'administration exposée sur Internet. Selon Danfoss, les unités touchées étaient surtout des modèles en fin de vie. Or le constructeur ne les met plus à jour. Devant le Sénat, le directeur de l'ANSSI a parlé de « défauts de sécurisation élémentaires ». Il citait l'exposition directe, l'administration non protégée et les mots de passe faibles. Il a aussi précisé que l'attaque n'avait pas exploité les failles publiées par des chercheurs.

Novembre, deuxième vague et attribution

La nuit du 1er au 2 novembre, en Europe. Le même scénario a frappé des magasins dans sept pays. Aux Pays-Bas, selon un porte-parole de Danfoss cité par Xenospectrum, les systèmes visés n'étaient pas sur un réseau protégé. D'après lui, **personne n'avait jamais changé leurs mots de passe par défaut**. Deux groupes prorusses ont ensuite revendiqué cette vague, sans vérification indépendante à ce jour.

La même nuit, l'Établissement français du sang. Un attaquant a compromis le prestataire frigorifique de trois sites de l'EFS. Il a alors modifié des consignes de température et de dégivrage de chambres froides. Mais un technicien de permanence et les alarmes auraient repéré les anomalies à temps. L'EFS déclare n'avoir perdu aucun produit sanguin.

Le 9 novembre, l'attribution. La France attribue l'épisode d'octobre à l'unité Shahid Kaveh des Gardiens de la révolution iraniens. Elle s'appuie sur un faisceau d'indices. L'enquête relève aussi, chez le même acteur, des reconnaissances massives visant d'autres automatismes industriels en Modbus TCP. Ce protocole ne prévoit ni authentification ni chiffrement. Mais l'enquête ne le désigne pas comme la voie d'entrée. Cette attribution ne couvre ni la vague de novembre ni l'EFS.

> **Mise à jour du 11 novembre 2026.** Le rapport du Centre de coordination des crises cyber, publié le 9 novembre par le CERT-FR, détaille ce faisceau d'indices : une infrastructure d'attaque employée à la même période pour des reconnaissances, l'usage de l'outil de recherche FOFA, un relais de l'attaque par un média dès le 13 octobre et des traces de farsi. Il mentionne d'autres victimes dans l'agroalimentaire, dont plusieurs petites boucheries, un abattoir et des usines coopératives, et le ciblage concomitant d'équipements de petites installations hydroélectriques, avec des effets qualifiés de modérés. Il ne dit pas comment les contrôleurs de froid ont été atteints, et il ne traite ni de la vague de novembre ni de l'EFS. Le même jour, le parquet de Paris a ouvert une information judiciaire visant le chef de l'unité et ses deux adjoints. Le ministère des Affaires étrangères a convoqué l'ambassadeur d'Iran et annonce qu'il proposera des sanctions à ses partenaires européens, et l'Iran a rejeté ces accusations le 10 novembre.

Ce que l'on ignore

Site par site, on ignore encore le chemin de l'attaquant. Il a pu utiliser un mot de passe par défaut ou deviné. Un compte de technicien réutilisé, une liaison 4G de maintenance ou un VPN restent aussi possibles. Selon les relevés de Censys, les interfaces Danfoss StoreView visibles depuis Internet sont passées de 3 004 le 9 octobre à 708 le 5 novembre, et les interfaces XWEB de Copeland et Dixell de 3 708 à 2 420, si bien que les superviseurs encore exposés seraient surtout des XWEB. Selon Bitsight, des leurres posés depuis l'attaque gonflent toutefois ces comptages. Le vôtre en fait-il partie ? Posez la question à votre frigoriste.

Date (2026)	Événement
Nuit du 11 au 12 octobre	Dégivrages forcés sur environ 700 sites en France.
Du 12 au 16 octobre	Alerte du CERT-FR, puis ses mises à jour.
Le 21 octobre	Le directeur de l'ANSSI parle de défauts élémentaires devant le Sénat.
Nuit du 1er au 2 novembre	Deuxième vague en Europe, et trois sites de l'EFS touchés.
Le 9 novembre	Attribution de l'épisode d'octobre à une unité iranienne.

Ce qu'en a retenu le grand public

Trois lectures des frigos piratés ont alors dominé. Chacune contient une part de vrai. Mais chacune déplace un peu le sujet.

« Les frigos connectés se font pirater. » Le mot est trompeur. En effet, ce n'est pas le meuble réfrigéré qui était joignable. C'était le superviseur de l'installation. Un tiers gère cet appareil professionnel. Les conseils donnés ensuite aux particuliers ne sont pas faux. Mais ils parlent d'un autre objet. La confusion a un coût. Elle fait d'un problème de sous-traitance une affaire d'hygiène individuelle.

« Pourquoi diable connecter un frigo à Internet ? » C'est la bonne question. Elle a une réponse, que donne le chapitre 2.

« C'est la guerre hybride. » Ce récit a précédé toute preuve. Or l'attribution officielle, un mois plus tard, n'a pas confirmé les premières hypothèses. **Pour un exploitant, la question de l'auteur passe pourtant au second plan.** Une unité militaire ou un amateur seraient sans doute passés par la même porte. Certes, leurs intentions et leur persistance diffèrent. Mais l'attribution change la réponse diplomatique, pas la vulnérabilité.

> **Mise à jour du 11 novembre 2026.** Si l'auteur désigné n'est pas celui des premières hypothèses, les textes officiels décrivent bien une opération d'État : le C4 parle d'attaques « à but de déstabilisation » et le ministère des Affaires étrangères y voit une campagne de sabotage sur le sol français. L'attribution change la réponse diplomatique, pas la porte d'entrée.

Ce qu'en ont dit les professionnels

La parole des spécialistes a été abondante et souvent juste sur le fond. Deux raccourcis sont pourtant revenus souvent. Les liens ci-dessous servent à situer les raisonnements, pas à viser des personnes.

Les solutions qui semblaient évidentes

« Il suffisait de changer le mot de passe et de mettre à jour. » Vrai en partie. Mais les unités les plus touchées étaient pour la plupart en fin de vie. Aucune mise à jour n'était donc possible. Un installateur belge rappelle qu'il faut alors modifier physiquement l'installation.

« Il ne fallait pas les brancher sur Internet. » C'est bien la première recommandation du guide de l'ANSSI de 2014. Mais le CERT-FR lui-même demande de vérifier ce que prévoit le contrat d'assurance. Il faut le faire avant de couper la remontée des températures vers le frigoriste. Le lien existe parce qu'il sert.

« Chacun accuse le voisin. » Le constructeur pointe les mots de passe de ses clients. La fédération du commerce réclame la transparence du constructeur et des frigoristes. Tout est vrai localement. Mais rien ne décrit le système entier.

Les raccourcis

Une faille publiée n'est pas forcément la porte utilisée. Des chercheurs avaient montré qu'un modèle Danfoss génère un mot de passe du jour déductible de sa date. Puis un expert invité à la radio et la presse spécialisée y ont vu la clé de l'attaque. Or l'ANSSI a indiqué que l'attaque n'avait pas exploité cette faille. La nuance compte. Une faille se corrige par un correctif, une mauvaise configuration par une organisation.

Trois épisodes ne font pas forcément une campagne. La France attribue octobre à l'Iran. Des groupes prorusses revendiquent novembre sans preuve. Rien ne rattache l'EFS à un auteur. Une porte ouverte attire plusieurs visiteurs.

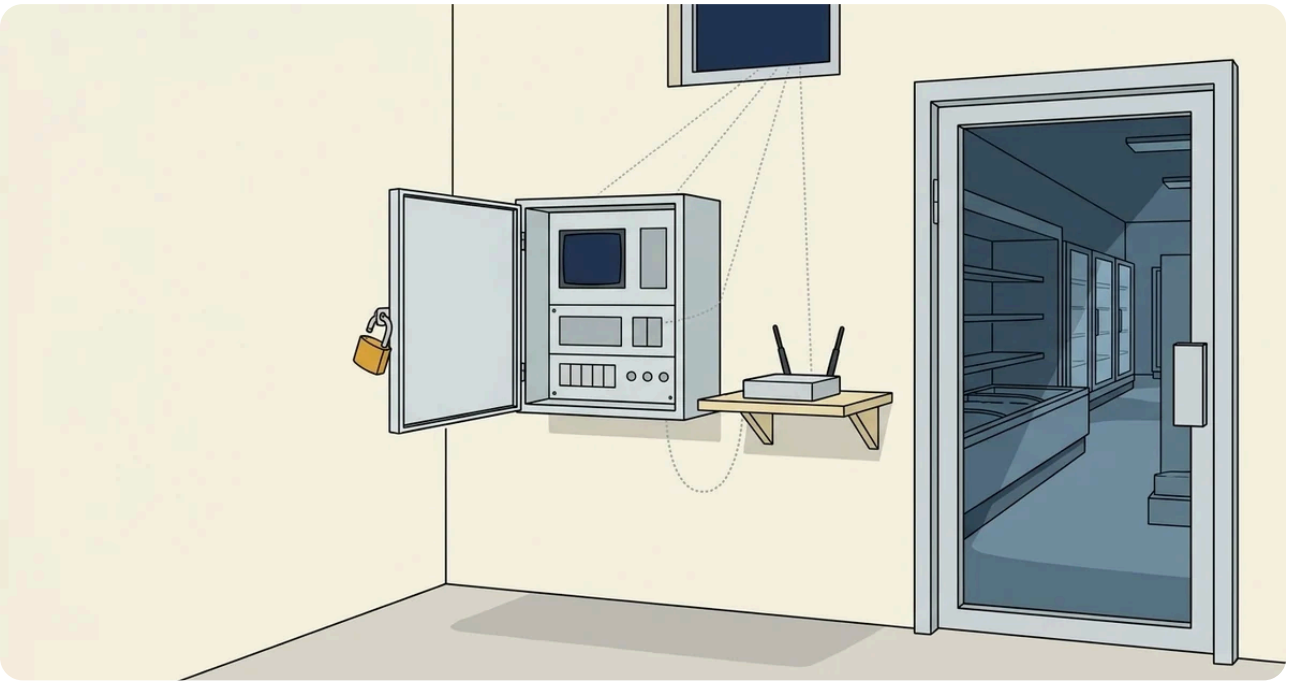
L'informatique industrielle n'est pas l'informatique de gestion. On a parlé de rançongiciels, de sauvegardes et de notification à la CNIL. Or l'attaque n'a volé ni chiffré aucune donnée connue. **Le système n'a pas été bloqué. Il a obéi.**

Des remèdes connus

On connaît les faits principaux. On connaît aussi les remèdes. Il s'agit de ne pas exposer, de changer les mots de passe et de mettre à jour. Pourquoi ne sont-ils pas appliqués ? Ce n'est pas seulement par négligence. Le chapitre 2 dresse la liste des sept failles qui se cumulaient. Il montre aussi ce qui rend chacune difficile à refermer.

CHAPITRE 2

Pourquoi les frigos restaient ouverts



Sept failles

Faille	Constat	Pourquoi elle dure
Interface d'administration exposée	Jugée contraire aux bonnes pratiques par le CERT-FR. Censys comptait plus de 3 000 interfaces web de superviseurs Danfoss visibles dans le monde le 9 octobre.	C'est le moyen le plus simple d'offrir la télémaintenance.
Mots de passe faibles ou par défaut	Cités par l'ANSSI. Certains superviseurs avaient un compte « Admin » livré avec le mot de passe « Admin ».	Le mot de passe est aussi le secret partagé d'un métier.
Équipements en fin de vie	AK-SM 800 sans support depuis 2021, AK-SC 355 depuis 2016.	Un superviseur survit souvent longtemps à son support constructeur.
Vulnérabilités connues non corrigées	Non exploitées cette fois selon l'ANSSI, mais publiées et corrigées, sans que le correctif soit appliqué partout.	Le suivi des correctifs de ce matériel n'est souvent confié à personne.

Aucune de ces failles n'est nouvelle.

Pourquoi elles ont duré

Faille	Constat	Pourquoi elle dure
Commande légitime détournée	Le dégivrage est une fonction normale. Prolongé, il a fait monter les températures à 50 °C sur certains sites.	Les agences américaines demandent désormais de borner les consignes à des plages raisonnables.
Pas de détection indépendante	Là où seul le superviseur donnait l'alerte, rien n'a sonné. L'EFS, doté d'une astreinte, fait exception.	Le superviseur compromis est aussi celui qui produit les alarmes.
Responsabilités dispersées	Gestion partagée entre enseigne, magasin, frigoriste et constructeur.	Personne ne possède donc l'inventaire complet.

D'après les informations publiées, l'attaquant n'a eu à forcer aucune protection de l'équipement. Il a envoyé un ordre qu'un technicien aurait pu envoyer. Ce qui était anormal, c'était l'heure, la valeur, la durée, et des centaines de sites recevant le même ordre la même nuit.

Pourquoi chaque remède se heurte au terrain

Intervenir à distance est un besoin métier. Un frigoriste surveille des dizaines, parfois des centaines d'installations la nuit. La réglementation impose d'enregistrer la température des entrepôts de surgelés et de conserver ces relevés. De plus, le CERT-FR demande de vérifier les conditions d'assurance avant de couper la remontée vers le frigoriste. **Le lien distant fait donc partie de la sécurité de la chaîne du froid.**

Un VPN ne dit rien de ce qu'on fait dans le tuyau. Le CERT-FR recommande à juste titre de passer par un VPN. Mais les accès reposent souvent sur des comptes partagés entre techniciens. De plus, les équipements VPN sont eux-mêmes la cible de campagnes de force brute. Quant aux routeurs 4G des prestataires, qu'un constructeur recommande, ils isolent bien l'équipement, mais le rendent invisible pour le magasin.

Le chiffrement protège le contenu, pas l'intention. Il est indispensable. Pourtant, un attaquant muni d'un identifiant valide envoie des ordres chiffrés. La consigne de dégivrage aurait ainsi été aussi destructrice dans un tunnel irréprochable.

Une affaire d'organisation

Le mot de passe par défaut est un problème d'organisation. Sur un site, le changer prend une minute. Mais sur des centaines de sites, avec des techniciens d'astreinte qui tournent et des sous-traitants, c'est un projet. Les consignes publiées depuis l'attaque demandent des comptes nominatifs et des dates d'expiration pour les intervenants. Or c'est de la gestion

des identités, encore peu outillée dans ce métier. Nous en avons parlé dans Un IAM pour vos équipements électriques.

Dans la plupart des magasins, personne ne regarde le canal d'administration. Car le superviseur commande et alerte à la fois : compromis, il peut faire tomber les deux.

Et la responsabilité reste diffuse. Le constructeur vend un produit, l'installateur le raccorde, le frigoriste l'entretient, le magasin le paie, l'enseigne le subit. L'ANSSI n'a pas les moyens de contraindre un supermarché. La transposition de NIS2 est toujours en discussion. Pour l'alimentaire, d'ailleurs, la directive vise la distribution en gros et la production industrielle, pas nécessairement le magasin. **Personne n'a la charge de la sécurité du canal d'administration. En pratique, c'est pourtant l'exploitant du magasin qui répond de la marchandise perdue.**

> **Mise à jour du 11 novembre 2026.** Le projet de loi Résilience, qui transpose NIS2, a été examiné en séance à l'Assemblée nationale les 9 et 10 novembre, avec un vote solennel annoncé pour le 17 novembre. Il doit encore achever son parcours, et la question du périmètre pour le commerce alimentaire de détail demeure.

Quatre questions à poser dès maintenant

- À votre frigoriste : mon superviseur est-il joignable depuis Internet ? Par quel chemin, y compris un routeur 4G de maintenance ?
- Toujours à votre frigoriste : qui a un compte dessus ? Le mot de passe d'origine a-t-il été changé ?
- À votre frigoriste : mon modèle reçoit-il encore des correctifs du constructeur ?
- À votre assureur : mon contrat exige-t-il la remontée des températures, et que prévoit-il en cas de sabotage à distance ?

> **Mise à jour du 11 novembre 2026.** Selon des courtiers cités par Reuters, les polices cyber ne couvrent en général pas les pertes physiques, et l'exclusion des actes de guerre pourrait compliquer les déclarations lorsqu'un État est désigné. En France, l'indemnisation des pertes dues à une atteinte à un système informatique suppose aussi une plainte déposée au plus tard 72 heures après sa découverte (article L12-10-1 du Code des assurances).

Ce que nous en retenons

Relisons la nuit du 11 au 12 octobre, en frigoriste expérimenté. **Quatre signaux se détachent : l'heure, la valeur, la durée et la simultanéité.**

L'heure et la durée d'une session se voient sans rien lire des échanges. En revanche, la valeur demande de lire la consigne. Enfin, la simultanéité ne se voit qu'en regardant plusieurs sites. Aucun ne suffit seul, car un dégivrage de nuit est banal, mais chacun suffisait à poser la question.

Les frigos restaient ouverts d'abord parce que leurs superviseurs étaient joignables depuis Internet, avec des mots de passe faibles ou jamais changés. C'est la première chose à corriger. Mais même corrigée, la commande à distance restera possible, puisque la télémaintenance l'exige.

Ce qui a manqué ensuite, c'est que rien ne mette en doute sa **légitimité**. Qui l'envoie, d'où, quand, avec quelle amplitude ? Ressemble-t-elle à ce que ce site fait d'habitude ? Cette question peut se traiter sans lire les échanges, sans remplacer le parc ni couper le lien du frigoriste. Elle peut aussi se passer du superviseur à protéger.

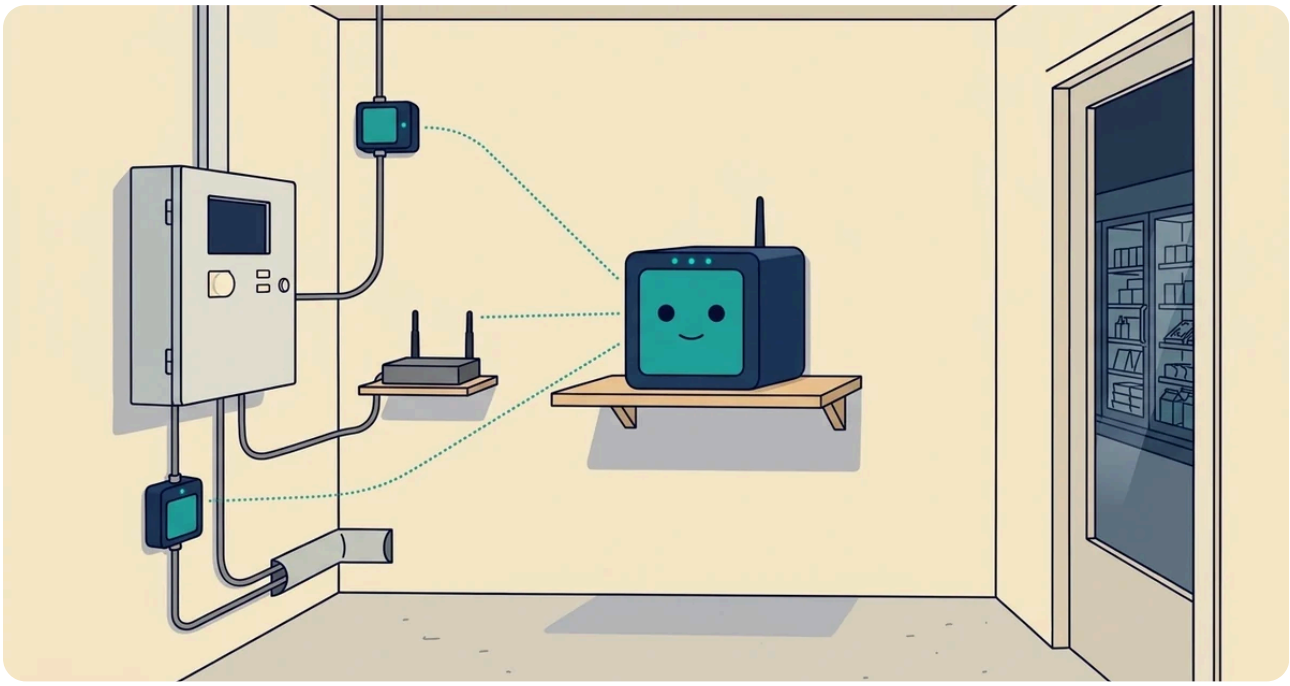
Un dernier rempart

Le magasin subit, alors que son responsable n'a en général ni équipe de sécurité ni budget dédié. Il lui faut donc un dernier rempart, qui l'alerte et suspend l'accès distant entrant selon des règles qu'il a lui-même posées. Il rouvre l'accès aussi simplement quand le frigoriste en a besoin. Suspendre l'accès entrant ne touche ni au froid ni à la remontée des alarmes, pourvu que celles-ci aient un chemin séparé. Les régulateurs continuent en effet de fonctionner sur place.

Les chapitres 3 à 6 décrivent comment nous l'abordons avec le Cube et ses satellites.

CHAPITRE 3

Observer sans lire : la légitimité d'un accès distant



La question du responsable de site

Prenons le responsable de site, c'est-à-dire le directeur ou le responsable technique du magasin, de l'atelier, de l'usine ou de l'entrepôt. Une connexion à son superviseur de froid a eu lieu cette nuit. Il ne peut pas savoir si elle venait de son frigoriste. Pour l'aider, nous proposons d'**observer sans lire** ce qui passe.

Après l'attaque, on a souvent lu que « l'air-gap est un mythe, passez au Zero Trust ». Certes, la télémaintenance a percé l'isolement (l'air-gap) des installations. Mais le Zero Trust, où chaque accès est vérifié, reste un nom de catégorie. Il ne dit pas qui le paiera dans des centaines de magasins.

Les agences américaines sont plus modestes. D'abord, elles isolent les équipements industriels sur un réseau virtuel (VLAN) dédié. Ensuite, elles restreignent l'accès aux adresses autorisées. Elles demandent de relire les journaux. Elles recommandent aussi de « définir des plages de consignes raisonnables, avec une alerte en cas d'écart ». Nous confions donc ce travail à un boîtier qui ne dépend pas du superviseur surveillé.

Les signaux d'une intervention légitime

Un frigoriste qui intervient à distance a des habitudes, même non écrites. Il se connecte depuis son agence, plutôt en journée sauf panne, quelques minutes. Surtout, il vise rarement des dizaines de sites dans la même heure. Ces habitudes forment le **comportement de référence** du site. Il permet alors de juger un accès distant OT sans en lire le contenu.

Question	Ce que l'on observe	Faut-il lire ?
Qui	L'appareil ou le compte, s'il est identifiable	Non
D'où	Derrière un tunnel, seulement l'adresse du routeur, du concentrateur VPN ou du cloud	Non
Quand	L'heure, rapportée aux horaires habituels	Non
Combien	La durée et le volume échangé	Non
À quelle fréquence	Le nombre de sessions par semaine	Non
Avec quelle valeur	La consigne écrite, par exemple une durée maximale de dégivrage	Oui
Sur combien de sites	La même action, la même nuit, ailleurs	Il faut voir plusieurs sites

Les quatre signaux du chapitre 2 (heure, valeur, durée, simultanéité) se retrouvent dans ces sept questions. Pour voir la simultanéité, le serveur d'administration met en commun les alertes de plusieurs sites.

Le comportement de référence s'apprend sur au moins une semaine complète. Il lui manque alors les interventions mensuelles ou saisonnières. Tant qu'il reste pauvre, des règles écrites avec le frigoriste valent mieux. Une anomalie déjà en cours serait d'ailleurs apprise comme normale. Mieux vaut donc vérifier d'abord la configuration, notamment les plages de dégivrage, comme le demande le CERT-FR.

Observer sans lire, puis lire seulement ce qui compte

Observer sans lire n'est pas une coquetterie. Les échanges avec le superviseur sont de plus en plus chiffrés, pas toujours sur les modèles anciens. Or les métadonnées restent visibles. Elles suffisent à repérer bien des comportements inhabituels, sans toucher aux réglages du froid.

Reste la valeur. En effet, des températures poussées jusqu'à 50 °C sur certains sites ne se devinent pas depuis la durée d'une session. Une partie des consignes se lit en clair sur la liaison série. Celle-ci relie le superviseur à ses régulateurs, souvent en Modbus RTU. Une partie seulement, car les plannings de dégivrage et les fonctions coordonnées vivent dans le superviseur. Sur le bus, ils ne passent que comme ordres de départ. Aucune source publique ne désigne Modbus comme la voie d'entrée des attaques. Il s'agit seulement d'y lire ce que le superviseur a ordonné.

Les diodes sentinelles

Dans le local technique, le Cube sert ici de **superviseur d'accès** du site, à ne pas confondre avec le superviseur de froid. Il remonte ses journaux et ses alertes par son propre lien cellulaire, et le téléphone du responsable de site peut lui servir de relais. Lui ne règle pas le froid, mais regarde qui accède à ceux qui le règlent. Il s'appuie notamment sur des satellites nommés **diodes sentinelles**, parce qu'ils observent sans pouvoir écrire.

Le mot diode est une image. Ce ne sont pas des diodes de données certifiées : elles n'en revendiquent pas le niveau d'assurance. En aval, le Cube échange avec un serveur d'administration, celui de l'exploitant ou le nôtre selon le contrat, et ce lien ne transporte que des règles signées et des journaux, jamais d'ordre vers le froid.

La sentinelle Wi-Fi repère les appareils qui s'associent, sans déchiffrer les échanges. Elle écoute le 2,4 GHz, canal par canal, mais ne voit ni le 5 GHz ni un superviseur câblé. Or une radio sait émettre : son silence repose sur le logiciel. Nous la rangeons dans la famille pour son rôle.

La diode Ethernet se pose en prise passive sur le câble du superviseur. Elle voit les sessions, leurs origines et leurs durées, sans être joignable sur le réseau.

La diode série se branche sur la liaison RS-485, ou RS-232 sur certains équipements, quand les régulateurs parlent Modbus RTU. Son montage n'a aucun étage d'émission. Le chapitre 5 détaille ces deux diodes.

Pour l'Ethernet et la série, en revanche, le sens unique repose sur le matériel. Aucun élément du montage ne sait émettre. Les diodes ne coupent rien. Si le responsable de site l'a prévu, un autre satellite suspend l'accès distant entrant. Il ne vise jamais le froid ni les alarmes sortantes.

Quel satellite pour quel existant

Votre frigoriste sait décrire l'existant.

- **Sur le Wi-Fi du magasin** : la passerelle Wi-Fi du chapitre 4, avec la sentinelle Wi-Fi en complément.
- **En Ethernet** : la diode Ethernet, qui ne voit pas la consigne quand l'interface est chiffrée.

- **Régulateurs en Modbus RTU** : la diode série, qui lit les consignes mais sans savoir qui a donné l'ordre.
- **Routeur 4G du prestataire** : une diode Ethernet derrière le routeur. Avec l'accord écrit du prestataire, on ajoute aussi une prise pilotée sur son alimentation, qui ne le coupe en marche que si l'exploitant l'a inscrit sur la liste des équipements qu'on peut couper à chaud (voir Couper le courant n'est pas un arrêt d'urgence).
- **Cloud constructeur** : une diode Ethernet en sortie, l'identité du technicien restant connue du seul constructeur.

Attention : couper un routeur 4G qui porte aussi les alarmes les coupe avec lui. Il leur faut donc d'abord un chemin séparé. Sur les grands sites, bastions et sondes industrielles font déjà ce travail, avec une équipe dédiée. Nous visons le magasin qui n'en a pas.

Ce que l'observation prouve, et qui en répond

L'observation prouve une anomalie de comportement, pas une intention. Une session à trois heures du matin peut être une vraie panne (faux positif). Mais une session à dix heures, depuis l'adresse habituelle, peut venir d'un attaquant (faux négatif).

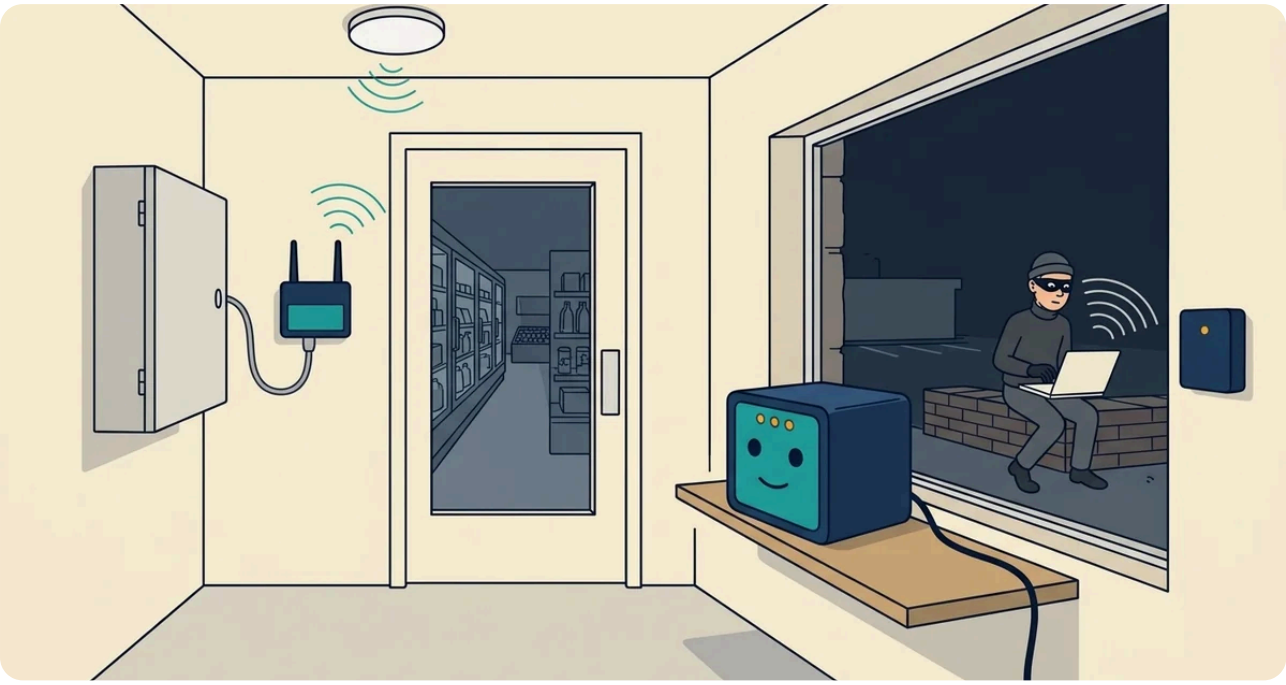
Une intervention annoncée dans une fenêtre accordée ne déclenche aucune alerte. Elle entre au journal et au résumé du jour. En revanche, hors fenêtre ou au-delà de l'amplitude permise, l'alerte est immédiate. Le faux positif coûte alors un appel au frigoriste, puis un geste pour acquitter sur le téléphone. Le faux négatif est plus sérieux. Un attaquant qui imite le comportement de référence échappe aux métadonnées. La lecture de la consigne réduit ce risque sans l'annuler.

Qui en répond ? Le frigoriste reste responsable de ses interventions, et le responsable de site de ses règles. Nos satellites tiennent deux promesses : ne pas pouvoir écrire, et journaliser fidèlement ce qu'ils ont vu. Les engagements correspondants sont précisés au contrat.

Le chapitre 4 détaille le cas fréquent du Wi-Fi du magasin.

CHAPITRE 4

Un satellite pour le Wi-Fi du magasin



D'où l'on part

Le superviseur de froid est souvent raccordé de deux manières. Soit il partage le réseau du magasin avec les caisses, joignable par tout ce qui y circule. Soit le prestataire a posé son propre routeur 4G, ce que recommande Dixell France. L'équipement est alors bien isolé. Mais le magasin ne voit plus ce qui y entre. **On gagne en cloisonnement ce que l'on perd en visibilité.**

Le CERT-FR demande de retirer ces interfaces d'Internet et de ne rétablir l'accès que par un VPN sécurisé ou un réseau protégé. En urgence, il admet toutefois le filtrage des adresses IP des prestataires. Mais cette solution « ne doit pas être considérée comme pérenne ».

Les passerelles de télémaintenance industrielles du marché offrent déjà tunnel sortant, accès à la demande et journal. Notre passerelle ne les remplace pas. Elle ajoute le rattachement au Cube, qui décide de la fenêtre selon les règles du responsable de site. Il garde aussi la preuve hors du réseau du magasin.

Ce que fait la passerelle

La passerelle est un petit boîtier posé près du superviseur. **En amont, elle rejoint le Wi-Fi du magasin. En aval, elle offre un port Ethernet.** On y rebranche le superviseur et les appareils qui dialoguent avec lui. C'est de la segmentation réseau à l'échelle d'un magasin. Rien ne joint plus ce segment sans passer par elle.

La pose se fait lors d'une visite du frigoriste, de préférence pendant une intervention prévue. Il rebranche le superviseur sur le boîtier. Puis il vérifie avec le responsable de site que les alarmes partent toujours. Aucun réglage du froid n'est touché. Il peut cependant falloir revoir l'adressage du superviseur, sa passerelle réseau et son serveur d'envoi des alarmes. Le frigoriste le fait ou le valide.

Côté frigoriste, la passerelle ne fournit pas l'accès. Le technicien garde son chemin habituel. C'est le VPN de son entreprise, le cloud du constructeur ou le bastion de l'enseigne. Ce **tunnel existant** aboutit désormais au boîtier. Celui-ci le laisse passer ou non selon la fenêtre du responsable de site. Il journalise chaque session et alerte hors fenêtre. L'authentification forte du technicien reste l'affaire de cet accès et de son opérateur. Trust-Buster n'exploite aucun service d'accès distant.

Fenêtre et journal

Le tunnel du frigoriste ne passe que pendant la **fenêtre d'intervention** accordée dans les règles du Cube. Par exemple, de 8 h à 10 h ce mardi. La nuit, l'astreinte valide d'un geste sur son téléphone, comme le détaille le chapitre 6. Le filtrage IP s'ajoute à la fenêtre sans la remplacer.

Chaque session est tracée : quel compte ou quel appareil, à quelle heure, combien de temps. Dans la fenêtre, la session entre seulement au journal. Hors fenêtre ou au-delà de la durée permise, l'alerte est immédiate. Pour l'entreprise de froid, ce journal est aussi une preuve de service.

La passerelle ne bloque jamais volontairement les alarmes sortantes. Elles passent toujours vers les destinations connues. Seule la télémaintenance dépend donc de la fenêtre.

Un piège pour les tentatives locales

Les attaques d'octobre sont venues d'Internet. Le leurre vise une menace locale, moins probable mais peu coûteuse à guetter. Ce serait quelqu'un qui tenterait sa chance depuis le parking.

Le boîtier annonce un **leurre Wi-Fi** sous un nom propre au site. Aucun appareil légitime n'a de raison de le chercher (« admin » attirerait les téléphones du personnel). Personne ne connaît sa clé WPA2. L'association peut réussir, mais l'échange de clés échoue. Le leurre écoute un canal à la fois et remonte au Cube quatre familles d'événements :

- Un appareil qui **cherche ce réseau par son nom**.
- Une **tentative de connexion** dont l'échange de clés échoue.
- Un **faux point d'accès** imitant le leurre ou le magasin, ce qui suppose de connaître la liste des bornes légitimes.
- Une **rafale de désauthentification**.

C'est de la détection seule, sans brouillage ni riposte. Le leurre ne gêne donc ni les caisses ni le Wi-Fi des clients, et sa liaison avec le Cube est signée.

Depuis l'attaque, beaucoup ont posé sur Internet des leurres qui imitent la page de connexion de ces superviseurs. Selon Bitsight, ils gonflent les comptages d'équipements exposés. Le nôtre ne guette que ce qui se passe à portée radio du magasin.

Où se place la diode sentinelle Wi-Fi

La **diode sentinelle Wi-Fi** écoute les annonces et les trames de gestion sans jamais s'associer. Son silence repose sur le logiciel, et non sur le matériel comme pour les diodes Ethernet et série. En revanche, elle évite de recâbler et ne coupe rien.

Elle surveille aussi le Wi-Fi dont le boîtier dépend. Un brouillage ou une rafale de déconnexions couperait en effet la télémaintenance. Le Wi-Fi du magasin devrait protéger ses trames de gestion (802.11w, imposé en WPA3). Un brouillage pur reste toutefois indiscernable d'une panne radio.

Si la passerelle tombe

Le froid continue, car les régulateurs pilotent les meubles sur place. **La télémaintenance s'arrête**, ce qui est le comportement sûr. Le frigoriste rebranche alors l'ancien chemin le temps de remplacer le boîtier.

Les alarmes ne doivent pas dépendre de la passerelle seule. Sinon, une panne du boîtier les ferait taire. Nous recommandons donc de garder un chemin séparé, qui existe souvent. Ce peut être une sortie d'alarme par contact, un transmetteur ou un routeur du prestataire réservé aux alarmes. Le Cube remarque qu'un satellite se tait. Il le signale aussitôt par son propre lien cellulaire, et le téléphone du responsable de site peut aussi relayer l'alerte.

Les questions à poser avant la pose

Le superviseur est-il en Ethernet ? Parle-t-il à d'autres appareils à déplacer avec lui ? Le Wi-Fi est-il partagé avec les clients ou géré par l'enseigne ? C'est alors souvent l'enseigne qu'il faut appeler. Le superviseur dialogue-t-il sans cesse avec un service en ligne ? Il faudra alors autoriser ce flux à part, hors fenêtre. Votre frigoriste connaît en général les réponses. La pose se décide d'ailleurs avec lui.

Ce que la passerelle prouve, et ce qu'elle ne prouve pas

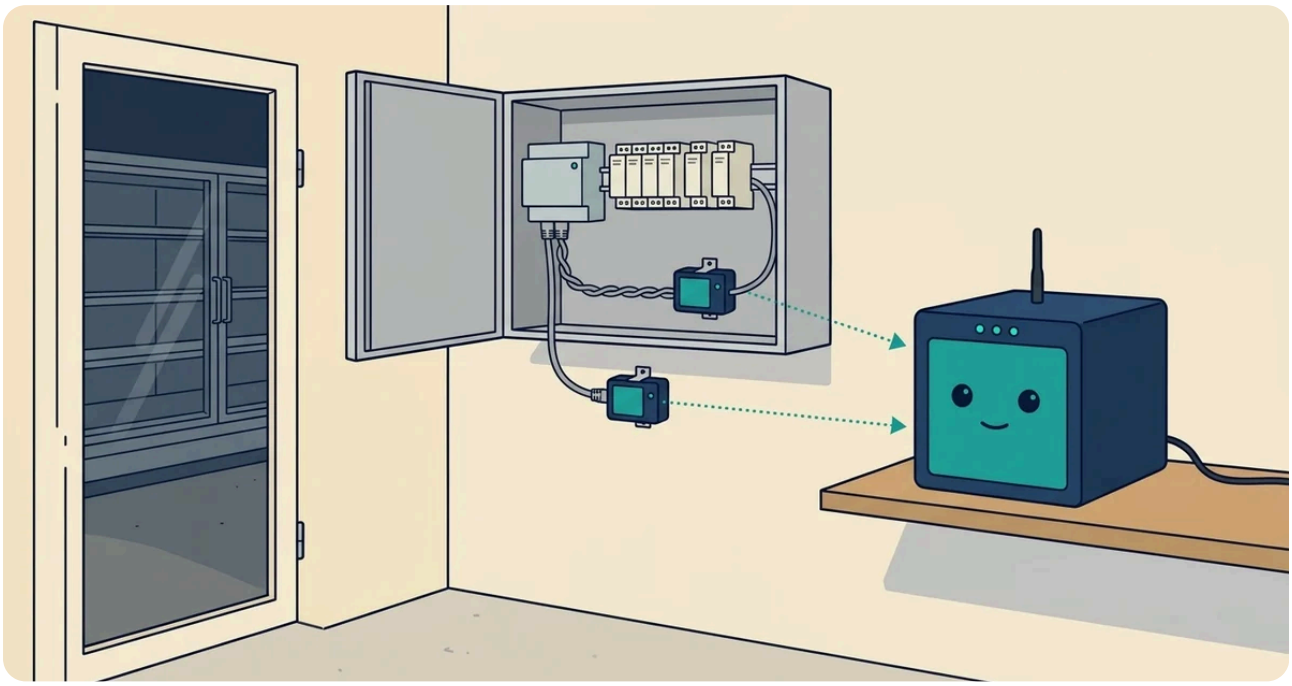
Mécanisme	Prouve	Ne prouve pas	Qui en répond
Segment et tunnel	Aucun chemin réseau prévu n'atteint le superviseur hors de la passerelle	La légitimité de la session	Le responsable de site, nous pour la passerelle
Fenêtre et journal	Quand et combien de temps	Ce qui a été fait	Le responsable de site
Filtrage IP	Une adresse connue	La bonne personne	Le prestataire
Leurre Wi-Fi	Une tentative locale	L'absence d'autres	Le responsable de site, alerté

La première ligne suppose d'avoir retiré l'ancien câblage, un second port Ethernet, un ancien routeur 4G ou un modem intégré.

Le piège ne voit pas un attaquant muni d'identifiants volés qui passe par le tunnel ouvert. C'est la limite principale, car cet attaquant ressemble au technicien attendu. Restent les signaux du chapitre 3 : une session plus longue ou une heure inhabituelle. Si l'on lit les échanges, s'y ajoute une consigne hors des habitudes du site. C'est le rôle des diodes Ethernet et série du chapitre 5.

CHAPITRE 5

Écouter sans pouvoir parler : les diodes sentinelles



Le principe

L'industrie connaît les diodes de données. Elles ne laissent passer l'information que dans un seul sens, par construction matérielle. Mais leur coût n'est pas celui d'un magasin. Nous en reprenons l'idée : écouter sans pouvoir parler, c'est-à-dire lire ce qui circule sur un câble. Aucun composant du montage ne sait y renvoyer quoi que ce soit.

Une diode sentinelle se pose sur le câble existant. Ce qu'elle observe remonte au Cube par un chemin séparé, selon notre habitude d'ajouter plutôt que de modifier.

Sur l'Ethernet du superviseur

La première diode se place sur le câble reliant le superviseur à son routeur ou à la passerelle du chapitre 4. Elle repose sur un **tap Ethernet passif**. Celui-ci recopie les signaux vers un port d'écoute et ne renvoie rien sur le lien surveillé.

Or un tap cuivre entièrement passif ne fonctionne qu'en 10BASE-T et 100BASE-TX. Sur un lien gigabit, il ramène ainsi la négociation à 100 Mbit/s, ce qui suffit à un superviseur. Il livre deux flux, un par sens. Sa pose coupe brièvement le lien. Quand le superviseur dépend de l'alimentation par le câble (PoE), il faut la vérifier.

En HTTPS, la diode voit qui se connecte, quand, combien de temps et avec quel volume, mais pas ce qui a été modifié. C'est déjà l'heure et la durée. Sur un protocole lisible, HTTP simple ou Modbus TCP, elle sait aussi reconnaître les écritures de consignes.

Sur la liaison série Modbus RTU

Entre le superviseur et les régulateurs circule souvent une liaison série. La spécification Modbus sur ligne série donne le RS-485 à deux fils comme le plus courant. Le RS-232 sert aux liaisons courtes de point à point. Chez Dixell, un régulateur XWi70K rejoint la ligne Modbus RTU par un module externe XJ485-CX branché sur son port HOTKEY. Certaines installations Danfoss utilisent un autre bus, le LON, que nous ne savons pas écouter. Votre frigoriste vous dira lequel équipe vos meubles.

La seconde diode se branche sur ce bus RS-485. Certains équipements en RS-232 demandent toutefois un autre récepteur. Son montage commence par un récepteur RS-485 sans étage d'émission. Vient ensuite un optocoupleur, que le signal traverse sous forme de lumière, puis un microcontrôleur. Un attaquant maître du microcontrôleur pourrait lui faire raconter n'importe quoi, mais pas envoyer un ordre aux régulateurs.

Ce que la diode écoute rejoint ensuite le Cube par un module sur rail DIN, le USR-DR164 de PUSR. Ce convertisseur RS-485 vers Wi-Fi bi-bande (2,4 et 5 GHz) sert aussi de passerelle Modbus RTU/TCP. Il s'alimente de 5 à 36 V et tient de -40 à 85 °C. Or, seul, il est bidirectionnel. La diode, réduite à son étage de réception, reste donc entre le bus et lui. Rien ne peut ainsi être émis vers les régulateurs, même par un module compromis.

Elle se raccorde en chaînage, entrée et sortie sur son bornier, comme un régulateur de plus. Elle n'a ni terminaison ni polarisation, car la spécification les réserve aux extrémités et à un seul point du bus. Le blindage est suivi sans être relié à la terre. Son récepteur ne présente qu'un quart de charge, plus la fuite de ses protections. Il pèse donc peu sur le bus. Des résistances série protègent son entrée. Un bus terminé mais non polarisé peut osciller au repos, ce que nous mesurons à la pose.

Lire la valeur d'une consigne

Sur ce bus, la diode lit surtout les écritures : quel régulateur reçoit quelle valeur, dans quel paramètre, à quelle heure. La diode distingue les lectures des écritures : codes fonction 05 et 06 (une sortie ou un registre), 0F et 10 (plusieurs), selon la spécification du protocole Modbus. C'est le signal de la **valeur**. Il demande toutefois la table des registres de chaque modèle, que tous les constructeurs ne publient pas.

La notice du XWi70K donne trois plages. Ainsi, la température de fin de dégivrage va de -55 à 50 °C. La durée maximale de dégivrage va de 0 à 255 minutes. Enfin, l'intervalle entre deux dégivrages va de 0 à 120 heures. Or l'appareil accepte chaque valeur prise seule. Mais c'est leur combinaison qui fait monter la température d'un meuble. C'est donc elle qu'une règle

surveille, dans l'esprit du FBI et de la CISA, qui demandent de définir des plages de consignes raisonnables, avec une alerte en cas d'écart. Par exemple, une combinaison jamais vue sur ce meuble, arrivée à trois heures du matin, ressort aussitôt.

> **Mise à jour du 11 novembre 2026.** Ransom-ISAC a publié le 6 novembre l'analyse d'un site de froid commercial attaqué la nuit du 2 novembre. Le contrôleur était joignable depuis Internet avec ses identifiants d'administrateur d'usine, et le rapport compte 743 écritures de paramètres sur 31 appareils, des consignes portées à 110 °C et 150 °C et plusieurs commandes de mise en sourdine des alarmes, sans attribution. Ces écritures en rafale sont le type de signal que décrit ce chapitre, et le rapport recommande lui aussi de vérifier les températures par des instruments indépendants.

Rien de ce qui a été publié ne désigne Modbus comme la voie d'entrée des attaques. Nous écoutons pourtant ce bus, car c'est là qu'une consigne arrive au régulateur. Son chemin d'entrée dans le superviseur importe peu. Sur un bus LON, il ne reste alors que la diode Ethernet.

Ce que cela prouve

Ce que cela prouve. Une diode sentinelle conçue sans élément d'émission ne peut ni écrire ni donc perturber l'installation par un ordre, même compromise. Elle donne aussi un témoin extérieur au superviseur, ce qui compte quand c'est lui qui est compromis. À l'EFS, un technicien de permanence et les alarmes auraient repéré les anomalies à temps.

Ce que cela ne prouve pas. La diode ne coupe rien. Elle signale au Cube, qui alerte le responsable de site. C'est la passerelle ou une prise pilotée qui suspend l'accès distant entrant. Si le routeur coupé porte aussi la remontée des alarmes, il leur faut d'abord un chemin séparé. La suspension ne vise jamais le froid.

Un **faux négatif** reste possible. La diode n'entend que son câble. Une attaque en cours pendant l'apprentissage serait apprise comme normale. Enfin, un superviseur compromis pourrait forger de fausses réponses de régulateur. C'est pourquoi une sonde de température indépendante reste utile sur un site critique.

Garantie, contrat et responsabilité

La garantie du constructeur. Un appareil tiers raccordé sur le bus peut-il être invoqué pour refuser une prise en charge ? La réponse dépend de chaque constructeur.

Le frigoriste. Il doit savoir qu'un appareil écoute et l'accepter. Le mieux serait qu'il pose la diode lui-même et la propose à ses clients. Rien ne change dans ses interventions. Le témoin montre aussi que ses réglages étaient dans les règles.

L'assureur. La question mérite de lui être posée. Un témoin indépendant peut aider à documenter un sinistre, mais sans en garantir la prise en charge.

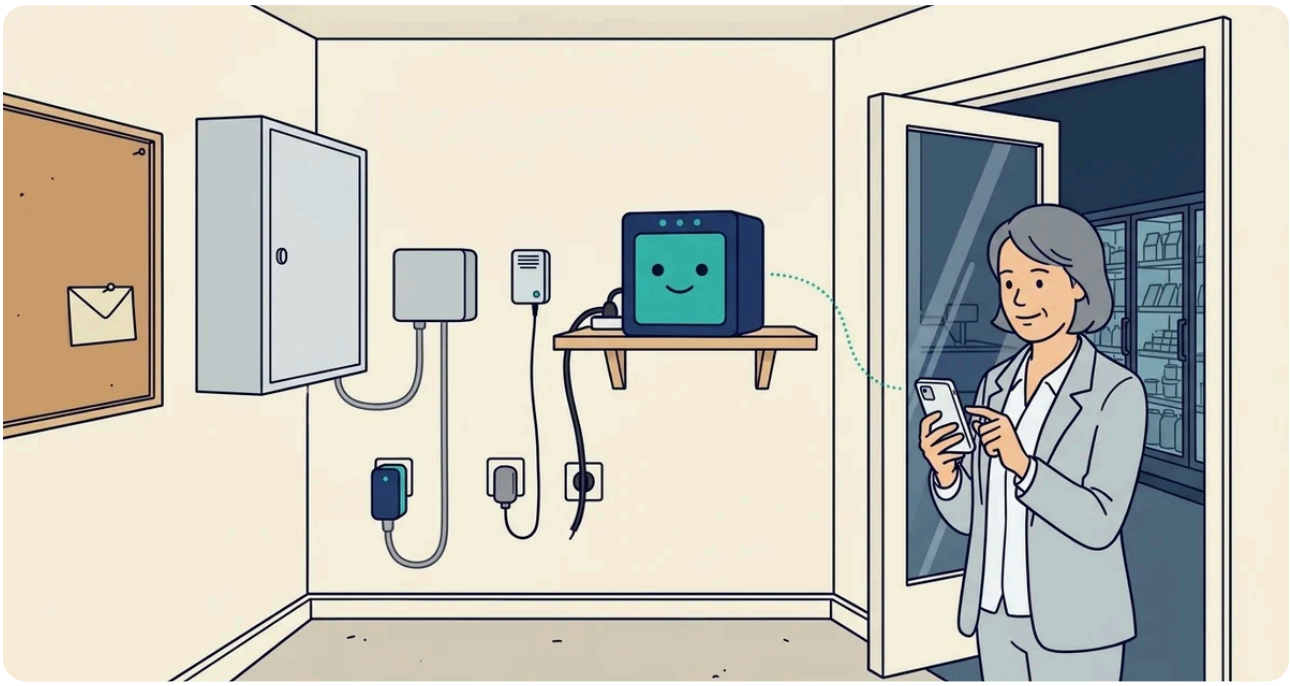
Celui qui pose. Si l'appareil perturbe le bus par un défaut électrique, qui en répond ? Et s'il n'a rien vu, qui est en faute ? Le montage ne sait pas émettre, par construction, et la question d'un défaut électrique se règle au contrat. Le raccordement dans une armoire reste l'affaire d'un professionnel du froid.

Sur ces points, nous recommandons une relecture juridique avant tout déploiement.

Les diodes voient sans couper. Reste à dire qui décide. C'est l'objet du chapitre 6.

CHAPITRE 6

Les règles du responsable de site : alerter, suspendre, révoquer



Une phrase par règle

Le responsable de site n'a en général pas de temps pour une console. Chaque règle tient donc en une phrase dite à voix haute. Par exemple : « l'entreprise de froid peut se connecter en semaine de 7 h à 19 h, depuis son adresse habituelle. Elle ne doit porter ni la température de fin de dégivrage au-delà de 12 °C, ni la durée maximale de dégivrage au-delà de 45 minutes. » Ces seuils de 12 °C et 45 minutes ne sont que des exemples, à valider par le frigoriste. Seule l'amplitude demande de lire la consigne. Une diode sentinelle série le fait.

Le Cube propose d'abord des règles à partir du comportement observé les premiers jours. Une anomalie déjà en cours serait alors apprise comme normale. D'où la vérification préalable de la configuration, décrite au chapitre 3. Le responsable de site les écrit ensuite avec son frigoriste, qui connaît les interventions mensuelles ou saisonnières. Une interface simple lui permet ensuite de les ajuster seul.

Révoquer doit être aussi simple que poser. Retirer un technicien, c'est rayer une ligne. Dans le Cube, les règles descendent signées du serveur. Un paquet mal signé est refusé. Chaque paquet porte aussi une date de validité. Or un Cube privé de réseau pourrait manquer une révocation. Une fois cette date passée, il refuse tout accès et l'inscrit en critique. Seul le bris de glace reste alors possible, jusqu'au retour de règles fraîches. Le délai d'une révocation est donc borné, au prix d'un refus général si le Cube reste trop longtemps sans nouvelles.

La fenêtre d'intervention, y compris la nuit

Un frigoriste d'astreinte doit pouvoir intervenir à 3 h du matin. Aujourd'hui, le secret tient souvent dans un mot de passe partagé. Depuis l'attaque, Dixell France demande de le remplacer par des comptes nominatifs à date d'expiration. Nous proposons d'aller plus loin : **la nuit, le mot de passe du superviseur ne suffit plus.** Le technicien est enrôlé par une application qu'il accepte d'installer. Cela se négocie avec chaque entreprise de froid. La fenêtre s'ouvre alors par un accord. Ses identifiants du superviseur, toujours nécessaires, ne servent à rien hors fenêtre.

L'accord peut venir d'une personne sur place, dont le badge ou le téléphone est reconnu par le Cube, comme pour autoriser une machine. L'accord peut aussi venir du responsable de site ou de l'astreinte. Le téléphone sonne, on voit qui demande et pour combien de temps, puis on accepte ou refuse d'un geste. La fenêtre se referme seule.

Sans réseau ni personne joignable, il reste le papier. Le Cube vérifie alors, hors ligne, un QR code de bris de glace rangé sous enveloppe. Son usage déclenche une alerte critique et laisse un reçu signé, remis au serveur au passage suivant d'un téléphone autorisé.

Au départ d'un technicien, on retire son téléphone. Il ne peut alors plus ouvrir de fenêtre. Des comptes nominatifs valent tout de même mieux qu'un compte partagé. Un téléphone prêté ou volé, déverrouillé, ouvre en revanche ce que son titulaire pouvait ouvrir. En effet, le Cube prouve qu'un appareil enrôlé était présent, pas qui le tenait.

Trois niveaux d'alerte

Une alerte qui sonne pour tout finit par ne plus être lue. D'où trois niveaux, que le responsable de site ajuste.

Niveau	Exemple	Réaction proposée
Information	Intervention annoncée, dans une fenêtre accordée.	Journal et résumé du jour.
Avertissement	Demande hors créneau, ou depuis une adresse inhabituelle.	Notification immédiate au responsable de site, qui accepte ou refuse.
Critique	Consigne au-delà de l'amplitude permise, bris de glace, plusieurs anomalies à la fois.	Notification immédiate, et suspension de l'accès distant si la règle le prévoit.

L'amplitude ne se voit que lorsqu'une diode sentinelle lit le bus. Ainsi, un réglage fait dans le superviseur lui-même, ou sur un bus LON, échappe au Cube. Le Cube classe selon ces trois niveaux ses propres événements comme les sessions de télémaintenance que lui signalent les satellites des chapitres 4 et 5.

Suspendre l'accès distant, jamais le froid

La suspension vise une seule chose. C'est **la porte par laquelle on entre dans le superviseur depuis l'extérieur.** Les régulateurs continuent de réguler et les alarmes de partir.

Avec la passerelle Wi-Fi du chapitre 4, il suffit de ne plus laisser passer le tunnel du frigoriste, ou de le fermer s'il est ouvert. Avec un routeur 4G du prestataire, la seule prise sûre est parfois son alimentation. Le Cube sait la piloter par un relais. Mais on ne la coupe qu'avec l'accord écrit du prestataire, et seulement si l'exploitant a inscrit ce routeur sur la liste des équipements qu'on peut couper à chaud (voir Couper le courant n'est pas un arrêt d'urgence). **Si ce routeur porte aussi les alarmes, le couper les ferait taire.** Il faut d'abord leur donner un chemin séparé, par exemple un transmetteur d'alarme indépendant. Le CERT-FR invite aussi à vérifier les conditions d'assurance avant de couper la remontée des données vers le frigoriste. L'enregistrement des températures reste obligatoire dans les locaux d'entreposage des surgelés, avec conservation d'au moins un an. Couper la remontée ne supprime toutefois pas l'enregistrement local.

Le Cube pilote des prises et des relais, met en quarantaine une prise que l'on tente de contourner, et journalise chaque coupure. L'ouverture bornée d'un routeur de superviseur reprend ces mêmes gestes.

Ce que le journal prouve, et ce qu'il ne prouve pas

Chaque entrée est liée à la précédente. Le lien passe par une empreinte cryptographique, et le Cube signe l'ensemble. Retirer ou modifier une entrée casse donc la chaîne de façon visible. Une perte est elle-même inscrite, comme détaillé dans « Un journal de preuve ». La clé de signature est protégée dans un élément sécurisé.

Il prouve qu'une fenêtre a été ouverte, quand, sous quelle règle, avec l'accord de quel appareil et pour combien de temps, et quelle règle a déclenché une suspension.

Il ne prouve pas ce que le technicien a fait dans le superviseur, sauf si une diode sentinelle a lu les consignes envoyées. Rien n'y dit non plus qui tenait le téléphone. Enfin, son heure est celle de l'horloge du Cube. Le journal a lui-même des limites. « Un journal de preuve » les détaille, des numéros de séquence à la tête de chaîne remise au serveur. Ce journal nomme des techniciens. Le badge ou le téléphone peut aussi révéler la présence de salariés. Il relève donc du RGPD. Les personnes concernées doivent en être informées, et les représentants du personnel consultés lorsque c'est requis.

Qui répond d'une coupure à tort ? Le responsable de site choisit la règle. Les modèles de règles que nous proposons et leur application se vérifient dans le journal. Le partage des responsabilités est précisé au contrat. Une suspension injustifiée n'arrête pas le froid. Mais pendant une vraie panne, elle retarde l'intervention. Cela peut coûter de la marchandise. Mieux vaut écrire, dans le contrat du frigoriste, comment il obtient une ouverture en urgence.

Trois questions à poser dès demain à votre frigoriste

Ces règles ne valent que ce que l'on sait de l'installation. Trois questions suffisent pour commencer.

1. Comment notre superviseur est-il raccordé, par le réseau du magasin, un routeur 4G, un modem intégré ?
2. Par quel chemin partent les alarmes, et est-ce celui de la télémaintenance ?
3. Qui détient aujourd'hui un accès distant, et avec quels comptes ?

Reste à savoir que faire quand le refus devient lui-même un risque. Nous l'avons abordé dans « IAM pour vos équipements électriques, partie 2 ».

Pour aller plus loin

Vous exploitez ou entretenez des installations télémaintenues, des superviseurs de froid ou des bus Modbus, et vous voyez d'autres contraintes ? Vous savez comment votre superviseur est raccordé, ou vous voulez le savoir ? Parlons-en. Nous vous montrons sur banc nos diodes sentinelles et notre passerelle, et la façon dont ces signaux se laissent observer. Et si votre site s'y prête, nous les installons chez vous en site pilote, avec votre frigoriste.

Pour prendre contact : contact@trust-buster.fr.

Sources

Autorités et textes officiels

- ANSSI, campagnes de déstabilisation et sabotage menées par la République islamique d'Iran (9 novembre 2026).
- CERT-FR, alerte CERTFR-2026-ALE-012.
- CERT-FR, rapport CERTFR-2026-CTI-009 du Centre de coordination des crises cyber (9 novembre 2026, PDF).
- Ministère de l'Europe et des Affaires étrangères, déclaration d'attribution à l'Iran.
- Assemblée nationale, examen du projet de loi Résilience (9 et 10 novembre 2026).
- Légifrance, article L12-10-1 du Code des assurances.
- CISA, FBI, HHS, USDA et DoT, fiche « Hardening Industrial Refrigeration and Cold Chain Monitoring Systems » du 5 novembre 2026 (PDF).
- Ministère de l'Agriculture, enregistrement des températures des surgelés.
- Directive NIS2, annexe II.

Normes et documentation technique

- Modbus Organization, Modbus Application Protocol Specification V1.1b3 (PDF).
- Modbus Organization, Modbus over Serial Line V1.02 (PDF).
- Dixell, notice du régulateur XWi70K (PDF).
- Danfoss, communications entre régulateurs et AK-SM 800A (PDF).
- Maxim, fiche du récepteur RS-485 MAX3095 (PDF).
- PUSR, fiche du module USR-DR164, RS-485 vers Wi-Fi bi-bande sur rail DIN.
- Garland Technology, principe des taps réseau passifs.
- Wikipédia, Network tap (taps passifs, 10/100, gigabit).

Presse et analyses

- Public Sénat, audition du directeur général de l'ANSSI (21 octobre 2026).
- AFP via Techniques de l'Ingénieur, défauts de sécurisation élémentaires et limites de l'ANSSI.
- Public Sénat, experts et fédération du commerce.
- Selectra, chambres froides de l'EFS.
- Selectra, deuxième vague et installateur belge.
- L'EFS, cité par Le Quotidien du Médecin.
- Euronews, la France accuse l'Iran.
- Next, pourquoi la France accuse l'Iran.
- 24matins, guide ANSSI de 2014.
- Refindustry, vulnérabilités Danfoss et Copeland corrigées.
- Sud Radio, « c'était d'une facilité déconcertante ».
- Journal du Net, l'arbuste qui cache la forêt.
- FrenchWeb, les installations locales, angle mort des enseignes.
- IT-Connect, cyberattaque des supermarchés et consigne de dégivrage à 50 °C.

- IT-Connect, force brute contre pare-feu et VPN.
- Solutions Numériques, retour de la loi Résilience à l'Assemblée.
- Hard2bit, modèles Danfoss touchés et fin de vie.
- Help Net Security, deuxième vague en Europe.
- Xenospectrum, déclaration de Danfoss sur les Pays-Bas.
- Cybernews, revendication de NoName057(16) et Z-Pentest.
- Analytics Insight, exposition selon Censys.
- Bitsight, données sur les attaques des superviseurs de froid des supermarchés.
- CTOL, consignes Dixell France et fin de support XWEB EVO.
- Franceinfo, information judiciaire du parquet de Paris.
- Xinhua, l'Iran rejette les accusations (10 novembre 2026).
- Reuters via Insurance Journal, polices cyber et pertes physiques.
- Ransom-ISAC, analyse de l'incident Copeland (6 novembre 2026).