STORMSHIELD

CYBERSÉCURITÉ & RÉSEAUX OPÉRATIONNELS

Vers une prise en compte du risque au niveau de l'industrie du futur ?

BAROMÈTRE RÉALISÉ EN COLLABORATION
AVEC L'USINE DIGITALE 2022

Sommaire

Cinq chiffres à retenir 04

01

DIRECTES OU INDIRECTES, DES CYBERATTAQUES AUX EFFETS PALPABLES

1.1 — À quoi ressemblent les attaques qui affectent les environnements industriels ? 06
1.2 — La place de la cybersécurité dans l'univers des systèmes industriels 07
1.3 — Des perceptions parfois éloignées de la réalité des risques 10
1.4 — Cas pratique : Connecter trois usines en toute (cyber)sécurité 13

02

DES SOLUTIONS QUI SUIVENT LES USAGES

2.1 — Un déploiement en phase avec les priorités des projets de sécurisation 16
2.2 — Un déploiement hétérogène en fonction de la maturité des industries concernées 19
2.3 — Quelles solutions pour l'avenir ? 23
2.4 — Interview croisée — Vers un écosystème interopérable 24
2.5 — La sensibilisation des industriels : l'adaptation comme facteur clé 25

03

LES BONNES INTENTIONS À L'ÉPREUVE DU RÉEL

3.1 — La pénurie de talents spécialisés 28
3.2 — Une chaîne de prestation à sécuriser 30
3.3 — Des budgets plus conséquents à allouer à la cybersécurité industrielle 32

Conclusion 33
Solutions Stomshield 34
Bibliographie/Sources et références 35

Pendant trois années consécutives, Stormshield et L'Usine Digitale ont étudié la transformation numérique des entreprises et son impact sur leur sécurité informatique.

Cette année, nous nous sommes attachés à établir un état des lieux des pratiques en matière de cybersécurité dans les environnements opérationnels des entreprises de l'industrie.

L'informatique industrielle (ou OT pour *Operational Technology*) recouvre tous les systèmes numériques qui assurent l'automatisation de processus physiques, tout en garantissant le bon fonctionnement d'une ligne de production. Ces systèmes opérationnels, de plus en plus connectés aux systèmes d'information classiques (IT pour *Information Technology*), doivent ainsi faire l'objet d'une vigilance accrue en matière de cybersécurité.

C'est pourquoi nous décrirons dans un premier temps les menaces et les risques cyber auxquels le secteur industriel est confronté. Nous détaillerons ensuite les solutions dont il dispose, avant de mettre en regard les déclarations d'intention et l'expression de la réalité du terrain révélée par l'étude. En effet, bien qu'ils embarquent toujours plus d'équipements connectés dans l'aventure de l'industrie 4.0, certains industriels semblent méconnaître ou sous-évaluer la nécessité d'investir dans la cybersécurité pour réduire au maximum ces nouvelles surfaces d'attaque.

Comme chaque année, nous espérons que ce baromètre vous apportera un éclairage constructif sur l'évolution du monde de la cybersécurité et en particulier celle des environnements industriels.

Cinq chiffres à retenir

51%

des répondants déclarent avoir subi **au moins une cyberattaque dans leur réseau opérationnel.**

32%

des répondants ont mis en place une **segmentation des réseaux OT.**

45 %

des répondants estiment que la **prise en compte des problématiques de sécurité constitue un frein** à leurs projets opérationnels.

27 %

des répondants ayant déjà subi une cyberattaque **ont vu leur production arrêtée ou perturbée.**

39 %

des répondants ont déployé **des solutions de protection de l'interconnexion IT/OT.**

Ces chiffres sont cohérents avec ce que nous observons sur le terrain : la cybersécurité est en train d'être mise en place. Il est par exemple encore rare de disposer d'une frontière IT/OT sécurisée, ce qui rend les systèmes industriels particulièrement vulnérables aux rebonds (intentionnels) voire aux effets de bord (fortuits) de cyberattaques sur le système informatique (SI).

Thaïs L., auditrice senior pour un pure-player français de la cybersécurité

01

DIRECTES OU INDIRECTES, DES CYBERATTAQUES AUX EFFETS PALPABLES

1.1 — À quoi ressemblent les attaques qui affectent les environnements industriels ? 06
1.2 — La place de la cybersécurité dans l'univers des systèmes industriels 07
1.3 — Des perceptions parfois éloignées de la réalité des risques 10
1.4 — Cas pratique : Connecter trois usines en toute (cyber)sécurité 13

1.1.

À quoi ressemblent les attaques qui affectent les environnements industriels ?

Avec l'avènement du concept d'industrie du futur, la maturité en matière de cybersécurité progresse. Celle-ci concerne désormais la protection du système industriel, comme système global. Un système qui englobe le système d'information industriel (SII, autour de l'incontournable SCADA, des ICS/DCS et autres API), ainsi que les machines, logiciels, postes de travail et différents équipements réseau.

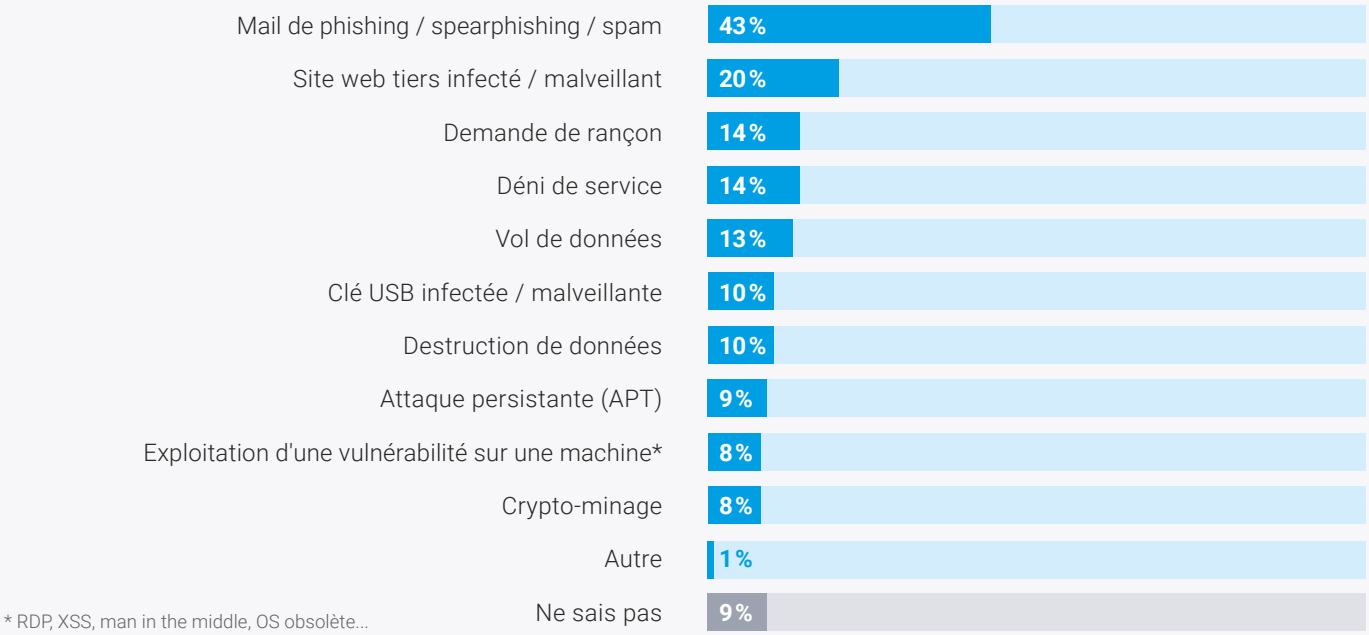
De ce fait, **51 %** des sondés déclarent avoir subi au moins une cyberattaque ciblant ce réseau opérationnel. Les récentes attaques sur les ports du nord de l'Europe laissent craindre que ce chiffre évolue à la hausse.

En ce qui concerne l'origine de ces cyberattaques, la plupart de celles qui affectent leurs outils de production trouvent leur point d'entrée dans les systèmes IT. Tout sauf une nouveauté tant l'interconnexion entre l'informatique classique et l'informatique opérationnelle tend à s'accélérer, faisant courir un risque majeur aux industries.

51 %

des répondants déclarent avoir subi au moins une cyberattaque ciblant ce réseau opérationnel

DE QUELS TYPES D'ATTAQUES S'AGISSAIT-IL ?



* RDP, XSS, man in the middle, OS obsolète...

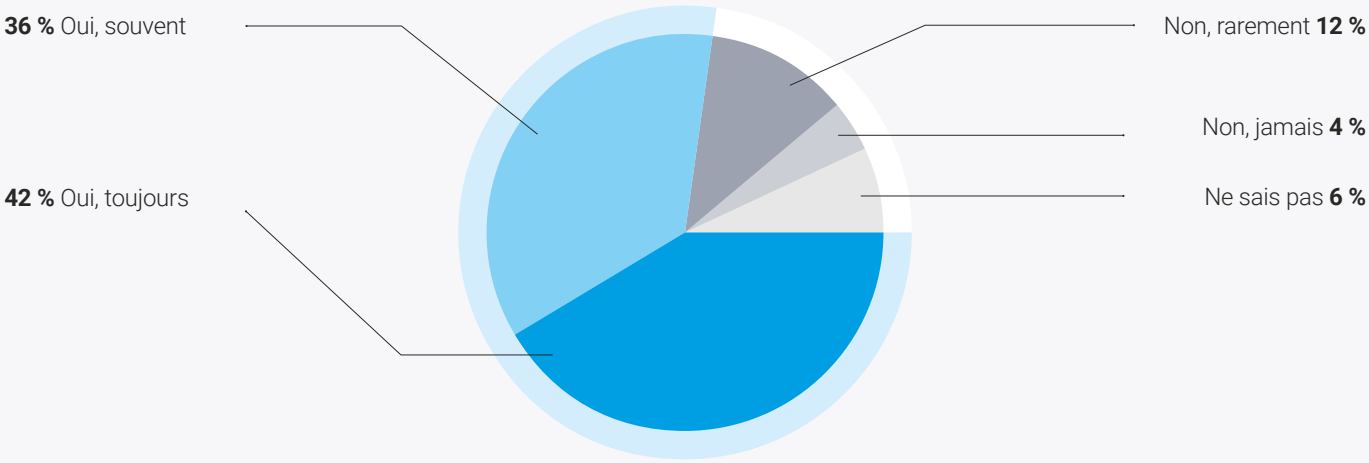
1.2.

La place de la cybersécurité dans l'univers des systèmes industriels

La convergence entre IT et OT est déjà une réalité depuis des années, sur le plan technique comme organisationnel. Ces deux univers, aux technologies autrefois très différentes et isolées, s'interconnectent. Et les principes de gestion cyber de l'IT doivent s'adapter au monde industriel, en répondant à un besoin de sureté et de gestion de risque spécifique.

Dans cet univers industriel où la disponibilité reste la priorité, la dimension cybersécurité serait prise en considération en amont de la majorité des projets (**78 %**).

LA CYBERSÉCURITÉ EST-ELLE INTÉGRÉE EN AMONT DES PROJETS LIÉS À VOS ENVIRONNEMENTS OPÉRATIONNELS ?



78 % OUI / NON 16 %

L'interconnexion entre IT et OT est là mais ses effets ne sont pas encore parfaitement pris en compte. Pourtant, les conséquences d'une cyberattaque dans ces environnements peuvent être beaucoup plus violentes que dans le cas d'une attaque informatique classique.

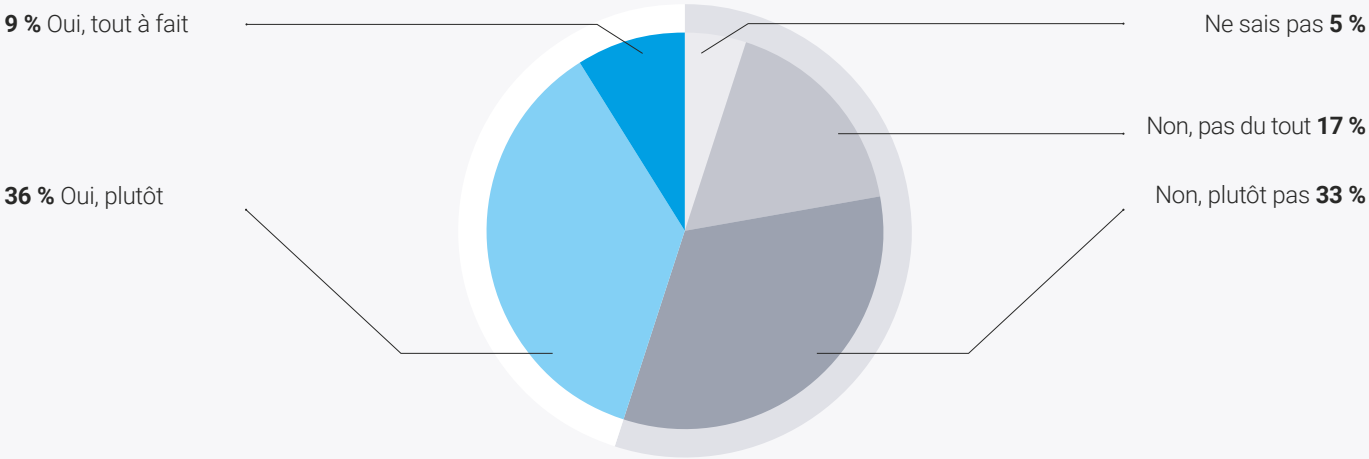
Marc Fromager, Vice-président Industrial Automation & End Users, Schneider Electric France

Toutefois, tenir compte des problématiques de sécurité est encore considéré comme un frein au développement de projets opérationnels par près de la moitié des sondés.

45 %

des répondants déclarent que tenir compte des problématiques de sécurité est encore considéré comme un frein au développement de projets opérationnels

SELON VOUS, LA PRISE EN COMPTE DES PROBLÉMATIQUES DE SÉCURITÉ REPRÉSENTE-T-ELLE UN FREIN AU DÉVELOPPEMENT DE VOS PROJETS OPÉRATIONNELS ?



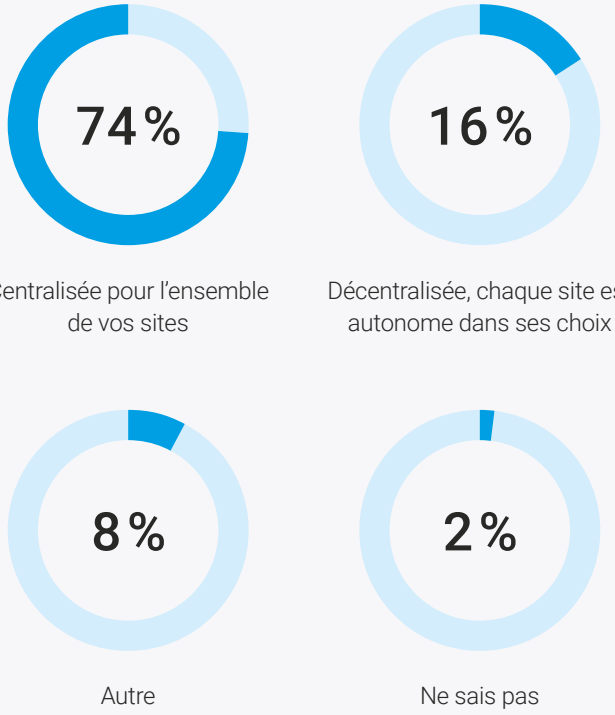
45 % OUI / NON 50 %

C'est à nous, experts en cybersécurité, de nous adapter aux contraintes opérationnelles, de trouver des solutions faciles à mettre en œuvre comme l'authentification par badge plutôt que de demander aux opérateurs de retenir un mot de passe différent par machine.

Thaïs L., auditrice senior pour un pure-player français de la cybersécurité

Au chapitre de la gouvernance, près de **3 répondants sur 4** ont opté pour la centralisation de la politique de cybersécurité industrielle. Cette organisation permet d'homogénéiser la sécurité sur l'ensemble des systèmes d'information industriels, tout en conservant une marge de manœuvre locale, et ainsi de répondre aux spécificités de chaque site. Ce management centralisé de la sécurité pose un référentiel pour garantir un niveau de sécurité minimal, en s'appuyant sur des RSSI ou des référents dédiés à l'OT sur site.

DANS VOS ENVIRONNEMENTS OPÉRATIONNELS, LA GOUVERNANCE DE LA CYBERSÉCURITÉ EST-ELLE :



L'IT et l'OT restent deux mondes différents. Mais nous allons vers une gouvernance partagée et des équipes uniques, composées d'experts à la double compétence, cyber et industrielle.

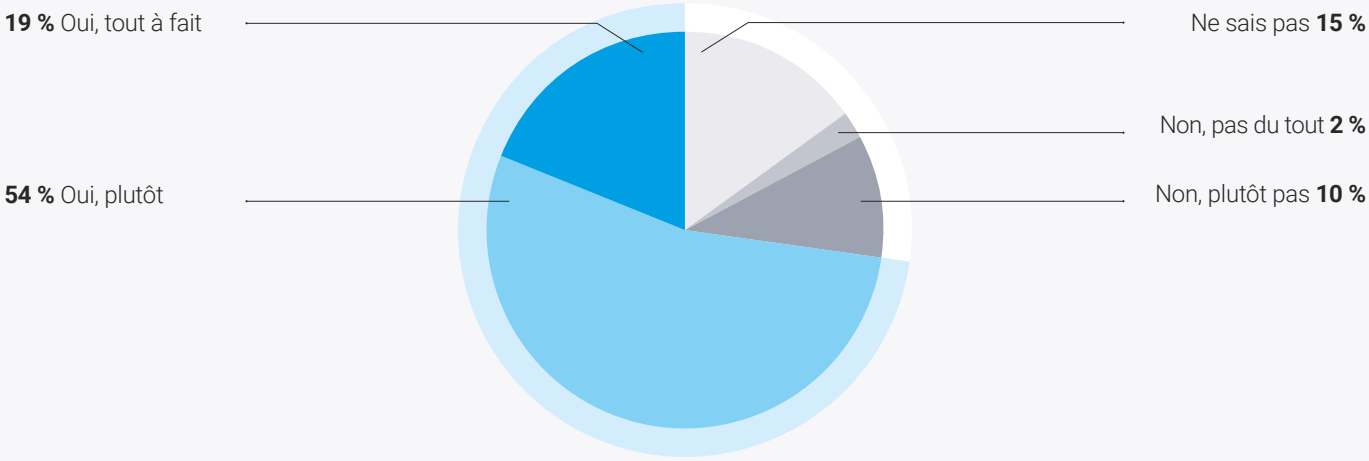
Rodolphe de Beaufort, Délégué Général Adjoint du GIMELEC et Animateur du Club CyberOT

1.3.

Des perceptions parfois éloignées de la réalité des risques

D'un point de vue technologique, les répondants semblent satisfaits de l'offre à leur disposition. Ils sont en effet **73 %** à estimer que les technologies existantes répondent à l'ensemble de leurs enjeux en matière de cybersécurité. Il est important de souligner qu'en fonction de la manière dont sont utilisés ces moyens techniques, le niveau de protection réel peut fortement varier. L'enjeu consiste donc à déployer les bons outils aux bons endroits, puis à les faire fonctionner correctement au quotidien.

LES TECHNOLOGIES EXISTANTES RÉPONDENT-ELLES À L'ENSEMBLE DE VOS ENJEUX EN MATIÈRE DE CYBERSÉCURITÉ ?

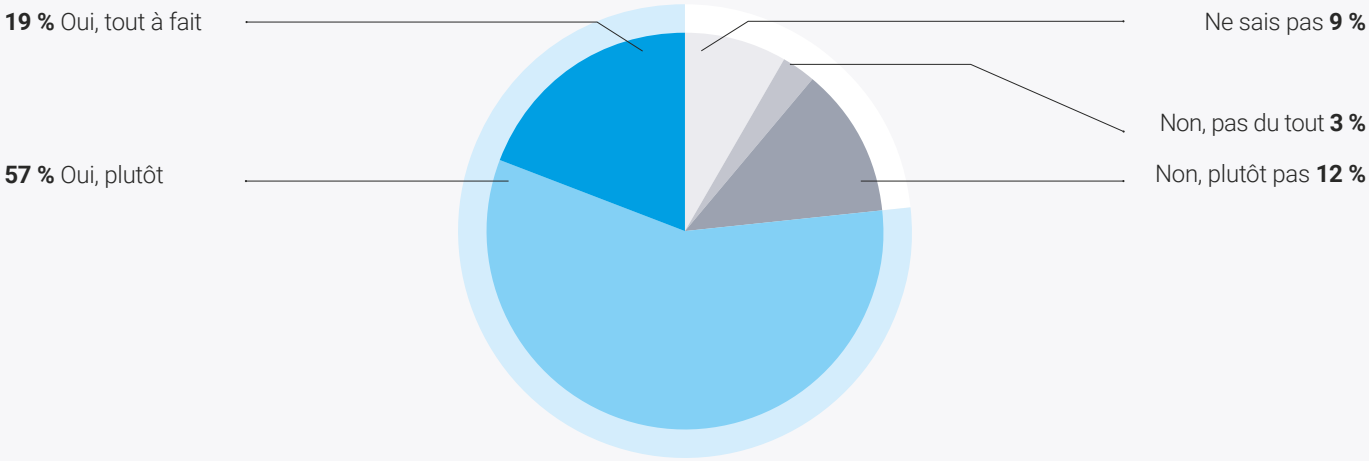


73 % OUI / NON 12 %

L'étude révèle également qu'une proportion étonnante de décideurs accordent une très grande confiance à la cybersécurité de leurs systèmes industriels (**76 %**), et ce, même en phase de maintenance (**70 %**).

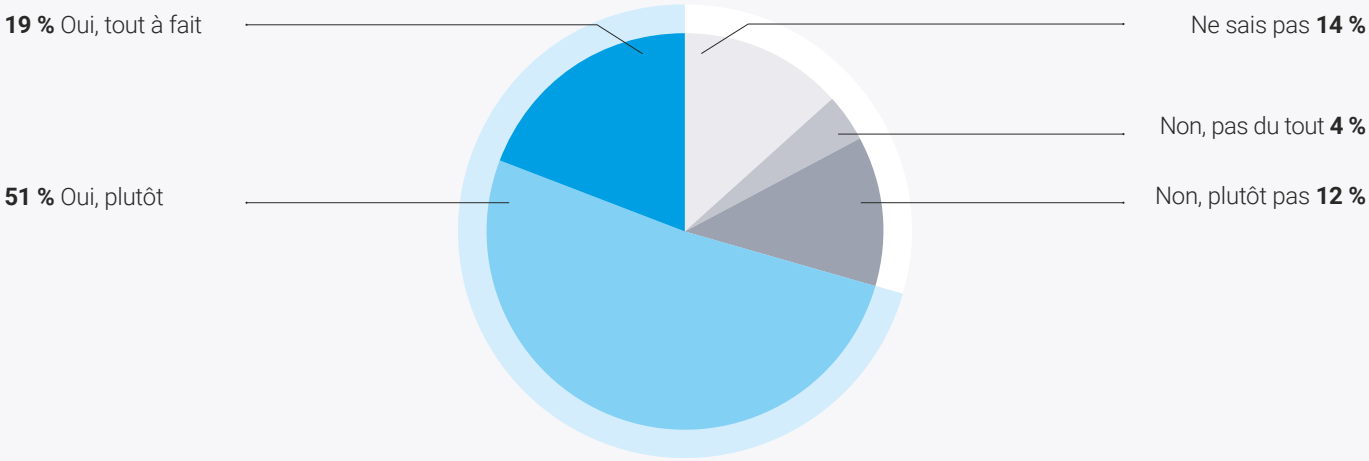
En regardant les chiffres de plus près, les plus confiants sont les directions générales, directions des opérations et directions R&D (**85 %**), les DSI (**76 %**), les directions de production ou de maintenance (**75 %**) ainsi que les directions de la stratégie numérique (**69 %**). La proportion diminue pour les publics des directions de la sûreté-sécurité (**56 %**) et des directions des risques (**50 %**).

DIRIEZ-VOUS QUE VOTRE ENTREPRISE EST SUFFISAMMENT PROTÉGÉE EN MATIÈRE DE CYBERSÉCURITÉ DANS SON ENVIRONNEMENT OPÉRATIONNEL ?



76 % OUI / NON 15 %

DIRIEZ-VOUS QUE VOTRE ENTREPRISE EST SUFFISAMMENT PROTÉGÉE EN MATIÈRE DE CYBERSÉCURITÉ DANS LES PHASES DE MAINTENANCE ?



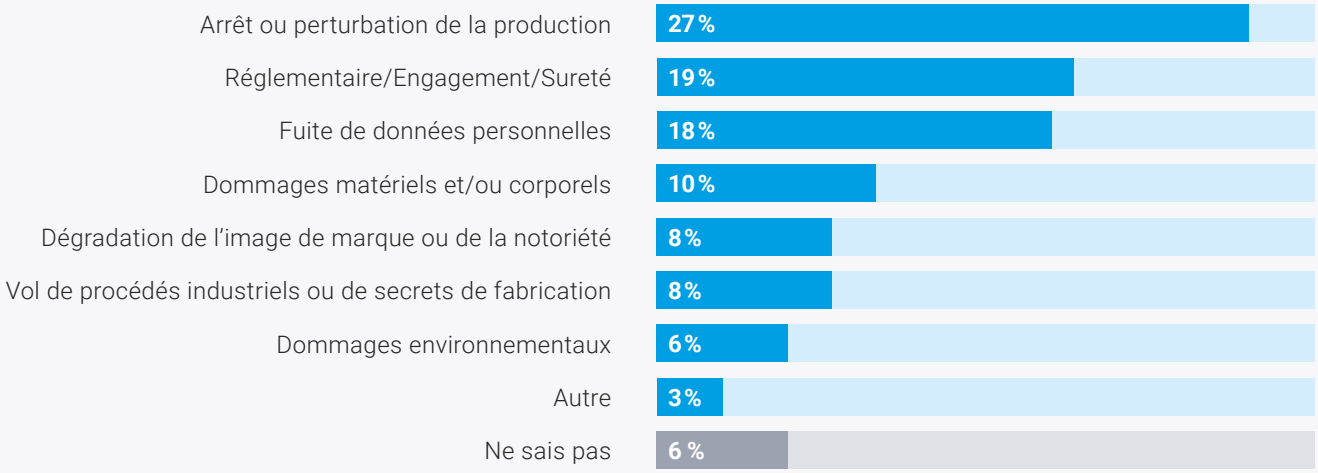
70 % OUI / NON 16 %

Pourtant, les cyber-criminels tirent déjà parti de l'augmentation indéniable de la surface d'attaque des systèmes industriels : parmi les sondés victimes de cyberattaques, **27 %** ont répondu que celles-ci avaient conduit à un arrêt ou à une perturbation de la production.

27 %

des répondants déclarent que les cyberattaques qu'ils ont subies ont conduit à un arrêt ou une perturbation de la production

QUELLES CONSÉQUENCES LES CYBERATTAQUES ONT-ELLES EU ?



Les exemples, de plus en plus médiatisés, ne manquent pas. Ainsi, en mars 2019, le spécialiste norvégien de l'aluminium Norsk Hydro a fait les frais d'une attaque de rançongiciel (LockerGoga) impactant directement son SI industriel. Contraint de déconnecter ses différents sites et usines, l'industriel a estimé à 46 millions d'euros l'impact de la cyberattaque, et ce, sans avoir payé la rançon demandée. De nombreux médias ont salué à l'époque la communication de crise du groupe. Depuis, la liste des entreprises victimes de cyberattaques ne cesse de s'allonger et la posture très transparente de Norsk Hydro fait désormais figure d'exemple.

Comment expliquer alors le décalage apparent entre sentiment de sécurité et niveau de protection réel des industries ? Il semble qu'une certaine méconnaissance des risques persiste, mieux connus des experts en cybersécurité que des exploitants industriels. Plus proches de l'opérationnel, ces derniers sont chargés du bon fonctionnement des processus mais ne sont pas encore pleinement sensibilisés aux aspects cyber. Un rapprochement doit donc s'opérer entre ces deux champs de compétences complémentaires.

La conscience du risque est encore émergente chez certains industriels qui n'imaginent pas que leur industrie pourrait être prise pour cible.

Thaïs L, auditrice senior pour un pure player français de la cybersécurité

CAS PRATIQUE

Connecter 3 usines en toute (cyber)sécurité

Un des clients industriels de Stormshield souhaitait interconnecter trois usines en France. Avec chacune plus d'une centaine d'équipements, la dimension cybersécurité du projet était prépondérante pour éviter une éventuelle infection par un logiciel malveillant, la prise de contrôle d'une machine, le vol de données critiques, l'espionnage économique, etc.

Très vite, Stormshield a identifié la nécessité de sécuriser les données métier du logiciel de pilotage de la production (MES) et des serveurs d'historisation tout en proposant un accès, sécurisé lui aussi, aux exploitants et mainteneurs du système.

PROTÉGER LES POINTS D'ENTRÉE ET LES INTERCONNEXIONS

La solution Stormshield Network Security a été retenue pour assurer la sécurité des systèmes d'information de l'industriel. Un cluster de SN2100 a été mis en place sur chacun des trois sites pour optimiser la segmentation et la séparation des réseaux OT de chacun d'entre eux du reste du système d'information (IT), où sont remontées et centralisées toutes les données industrielles liées à l'exploitation.

Une dizaine de firewalls SNi40, spécifiquement conçus pour protéger les automates, a été déployée en complément pour assurer une sécurisation au plus proche des équipements.

LE POINT FORT DE LA SOLUTION STORMSHIELD

Ces boîtiers permettant également une uniformisation des plans d'adressage IP via la fonctionnalité « Network Address Translation » (NAT). Notamment pour les îlots de machines dites « homologuées », fournies par des équipementiers externes et disposant de leurs propres adresses IP non modifiables pour des raisons de garantie constructeur. Les pare-feux SNi40 offrent ainsi la possibilité de réaliser une traduction de l'adresse de l'équipement au niveau de la passerelle de connexion à Internet, entre l'adresse interne de la machine et l'adresse IP de la passerelle, ce qui permet d'intégrer un API de façon transparente dans le plan d'adressage du client. En déployant les équipements Stormshield, le client a également pu améliorer la visibilité de son système d'information industriel grâce au mécanisme « Intrusion Detection System » (IDS), qui permet de détecter un trafic malicieux et de lever une alarme.

LES + DE LA SOLUTION

- une installation facile grâce à des fonctions d'intégrations réseaux transparentes permettant de s'adapter au contexte métier et opérationnel rapidement,
- une technologie basée sur des plugins applicatifs pour une protection maximale contre les menaces connues et les attaques de type Zero Day,
- des capacités d'inspection protocolaires permettant d'assurer la conformité des protocoles industriels pour éviter les attaques et les erreurs humaines,
- une faible empreinte des équipements sur la latence dans le réseau industriel,
- un logiciel unique pour un processus d'administration en une étape, quel que soit le domaine de protection (OT ou IT).

EXPLOITER PLEINEMENT L'ENSEMBLE DES DONNÉES INDUSTRIELLES

Entièrement satisfait par l'interconnexion de ses réseaux IT et OT, ce grand groupe industriel continue d'accorder sa confiance à Stormshield pour équiper l'ensemble de ses sites européens dans les prochains mois et à plus long terme, ses sites dans le monde.

02

DES SOLUTIONS QUI SUIVENT LES USAGES

2.1 — Un déploiement en phase avec les priorités des projets de sécurisation **16**
2.2 — Un déploiement hétérogène en fonction de la maturité des industries concernées **19**
2.3 — Quelles solutions pour l'avenir ? **23**
2.4 — Interview croisée — Vers un écosystème interopérable **24**
2.5 — La sensibilisation des industriels : l'adaptation comme facteur clé **25**

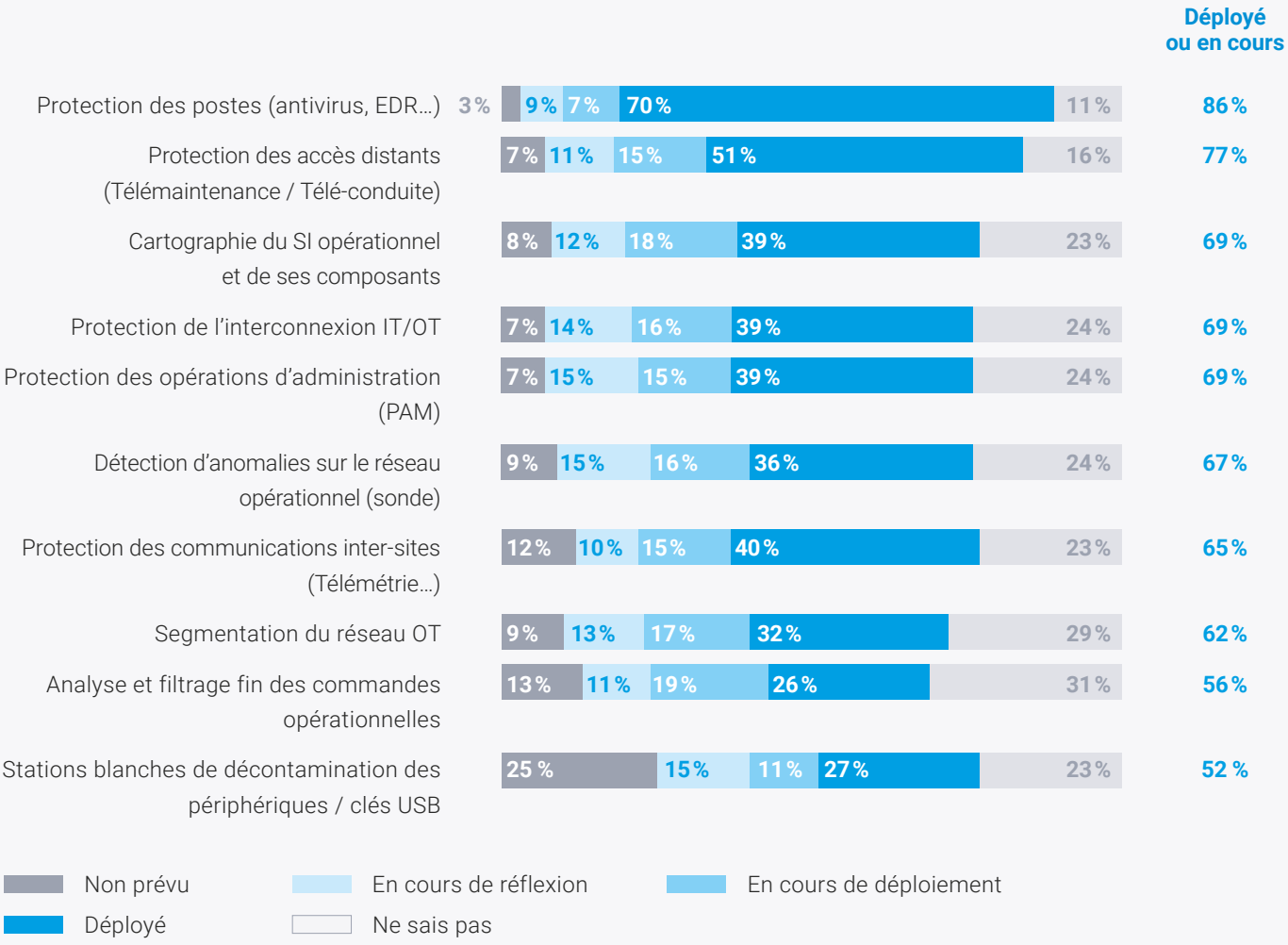
2.1.

Un déploiement en phase avec les priorités des projets de sécurisation

Parmi les premières solutions qui viennent à l'esprit, la **protection des postes** via une solution d'antivirus ou d'EDR est largement déployée dans les environnements opérationnels des sondés (**70 %**).

En parallèle, **52 %** des répondants disent recourir ou réfléchir à l'utilisation de stations blanches de décontamination des périphériques.

QUELLES SONT LES PROTECTIONS DÉPLOYÉES OU À VENIR AU SEIN DE VOTRE ENTREPRISE POUR SÉCURISER VOS ENVIRONNEMENTS OPÉRATIONNELS ?

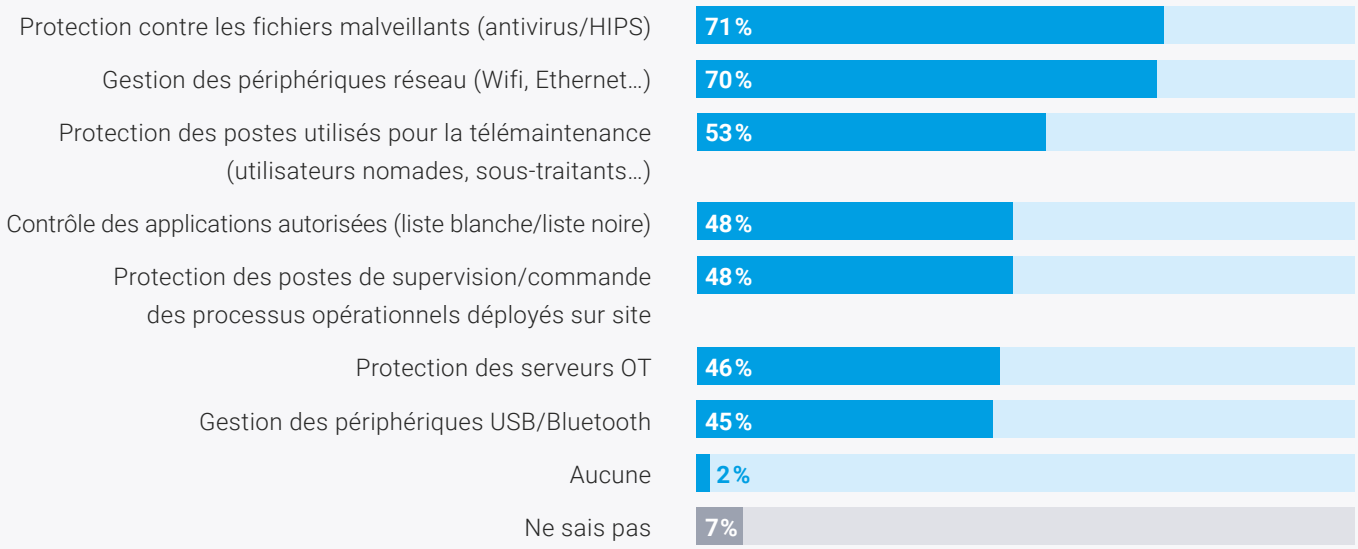


Avec l'entrée de l'IoT et des tablettes de supervision dans les usines, la gestion de périphériques réseau (Wifi, Ethernet, USB et Bluetooth) est d'ailleurs citée comme un périmètre fonctionnel à sécuriser par de nombreux répondants (respectivement **70 %** et **45 %**).

La **protection des accès distants** est en place pour la moitié d'entre eux. Ce chiffre s'explique en partie par l'accélération du recours à la télémaintenance, notamment pendant la pandémie de Covid-19. Plus pratiques, ces accès qui ne sont malheureusement pas toujours identifiés, créent de nouvelles portes d'entrée qui doivent impérativement être sécurisées.

La **cartographie** de l'ensemble de l'environnement OT est également un préalable à sa sécurisation, mais n'est une réalité que chez **39 %** des répondants.

SUR QUEL PÉRIMÈTRE FONCTIONNEL VOTRE ENTREPRISE A-T-ELLE DÉPLOYÉ OU PRÉVOIT-ELLE DE DÉPLOYER DES SOLUTIONS DE PROTECTION DES POSTES ?



Les sondes de détection et de cartographie permettent d'identifier les équipements réellement présents sur le réseau, de repérer les vulnérabilités ou les défauts de configuration. Grâce à ces informations, il est possible d'orienter les priorités pour les autres solutions et de prendre les bonnes décisions en matière d'affectation de budgets et de fenêtres de maintenance.

Vincent Dély, Nozomi Networks

La même proportion de sondés indique avoir déployé des solutions de protection de l'interconnexion IT/OT et des opérations d'administration (PAM). L'amélioration de l'**authentification** fait ainsi partie des grands chantiers de ces infrastructures industrielles qui, pour la plupart, sont dépourvues d'Active Directory et disposent d'une gestion peu efficace des accès et des privilèges.

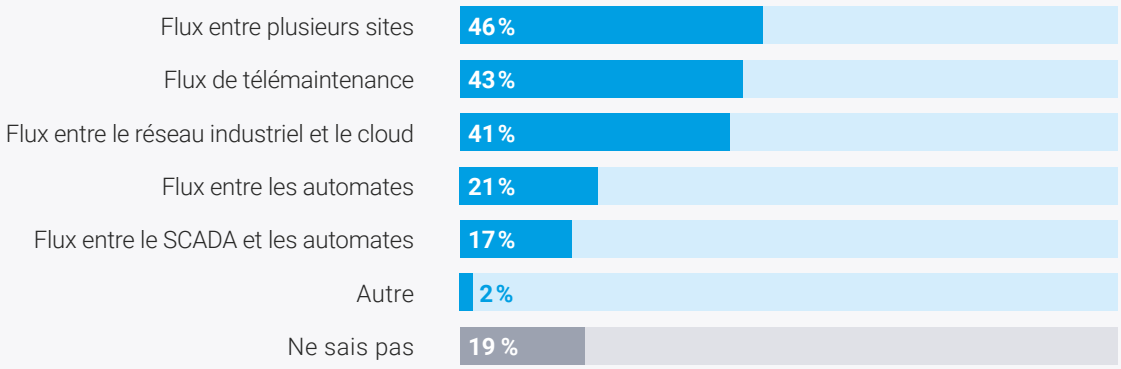
La **protection des communications inter-sites** est quant à elle en place chez **40 %** des répondants et présente également des enjeux importants, comme l'illustre la cyberattaque subie par Honda en 2020 : plusieurs de ses sites de production à travers le monde ont été bloqués par un ransomware. L'éventuelle compromission de ses systèmes de contrôle qualité a dû être écartée avant que le constructeur automobile puisse reprendre ses activités.

32 %

seulement des sondés indiquent avoir déployé une segmentation du réseau OT

Ces flux entre plusieurs sites font partie des **flux opérationnels sécurisés ou à sécuriser** pour **46 %** des sondés. Ils ne sont que 17 % à mentionner les flux entre le SCADA et les automates, sans doute pas considérés comme prioritaires dans la démarche de sécurisation.

QUELS FLUX OPÉRATIONNELS AVEZ-VOUS OU ENVISAGEZ-VOUS DE SÉCURISER ?



Des solutions comme l'**analyse et le filtrage de commandes opérationnelles** sont encore moins répandues – malgré leurs promesses de sécurité avancée. Ces dernières nécessitent une forte maturité cyber de la part des industries concernées : il s'agit de rentrer dans le détail du processus industriel et cela suppose d'avoir déjà mis en place d'autres actions de protection prioritaires.

En définitive, la cybersécurisation d'environnements opérationnels est un travail de longue haleine et les chiffres recueillis correspondent au déroulé du déploiement de la protection dans ces milieux. La **segmentation du réseau OT** par exemple prend du temps, surtout quand elle implique plusieurs sites industriels, car elle suppose de mettre en œuvre une passerelle (DMZ) entre le réseau entreprise (IT) et les opérations (réseau OT). Cela pourrait expliquer que **68 %** des répondants ne l'ont pas encore déployée. Il faut noter également que la notion de priorisation dans le déploiement de la cybersécurité industrielle est d'autant plus importante que les fenêtres d'intervention sont réduites, puisque la production ne peut être arrêtée ni très longtemps ni très souvent.

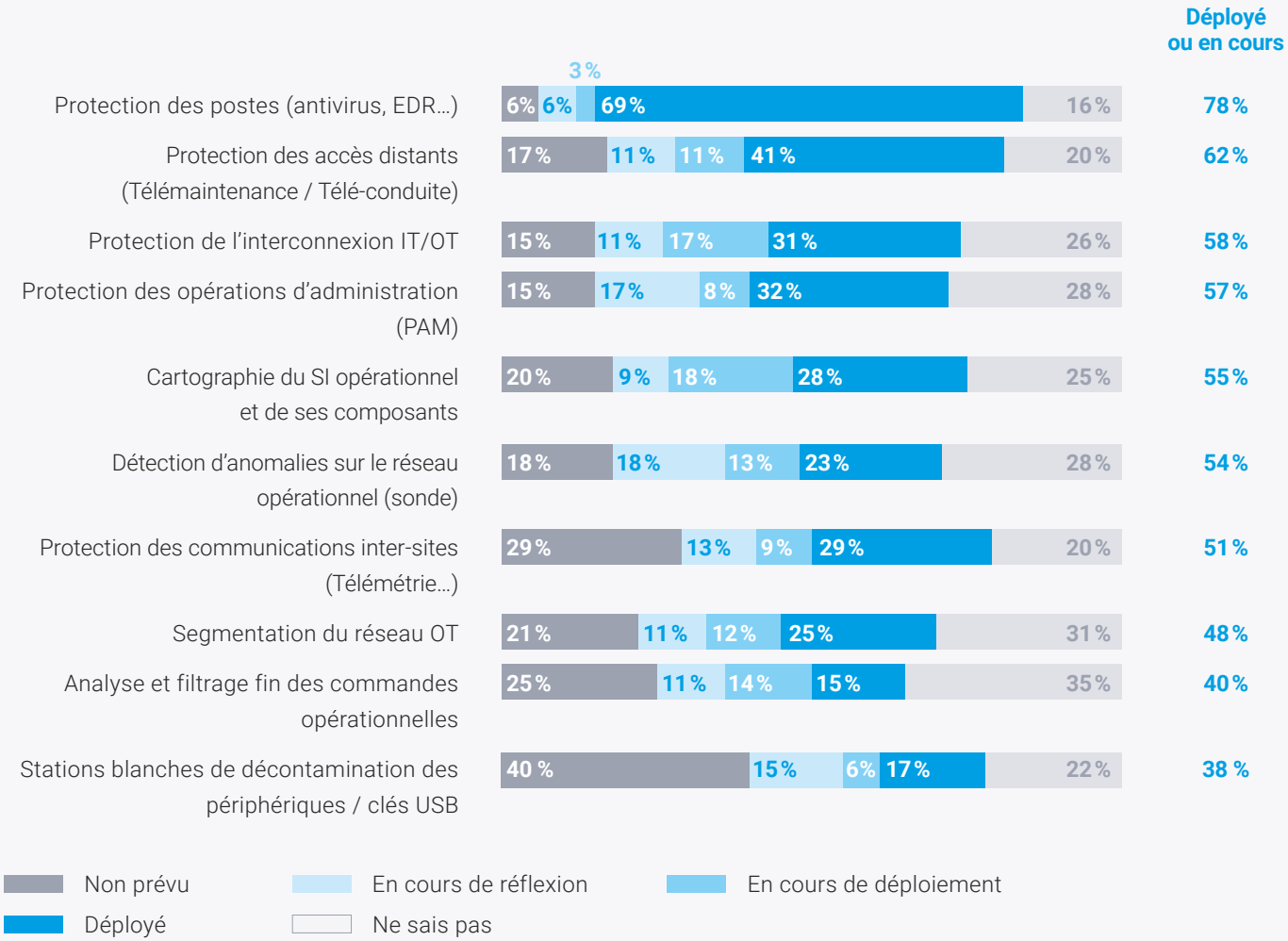
2.2.

Un déploiement hétérogène en fonction de la maturité des industries concernées

Le nombre et le type de solutions de cybersécurité déployées varie selon la typologie d'industries. Les TPE/PME déclarent ainsi moins d'investissement cyber, les ETI sont celles qui réfléchissent ou déploient le plus de solutions de protection, là où les grandes entreprises semblent déjà équipées.

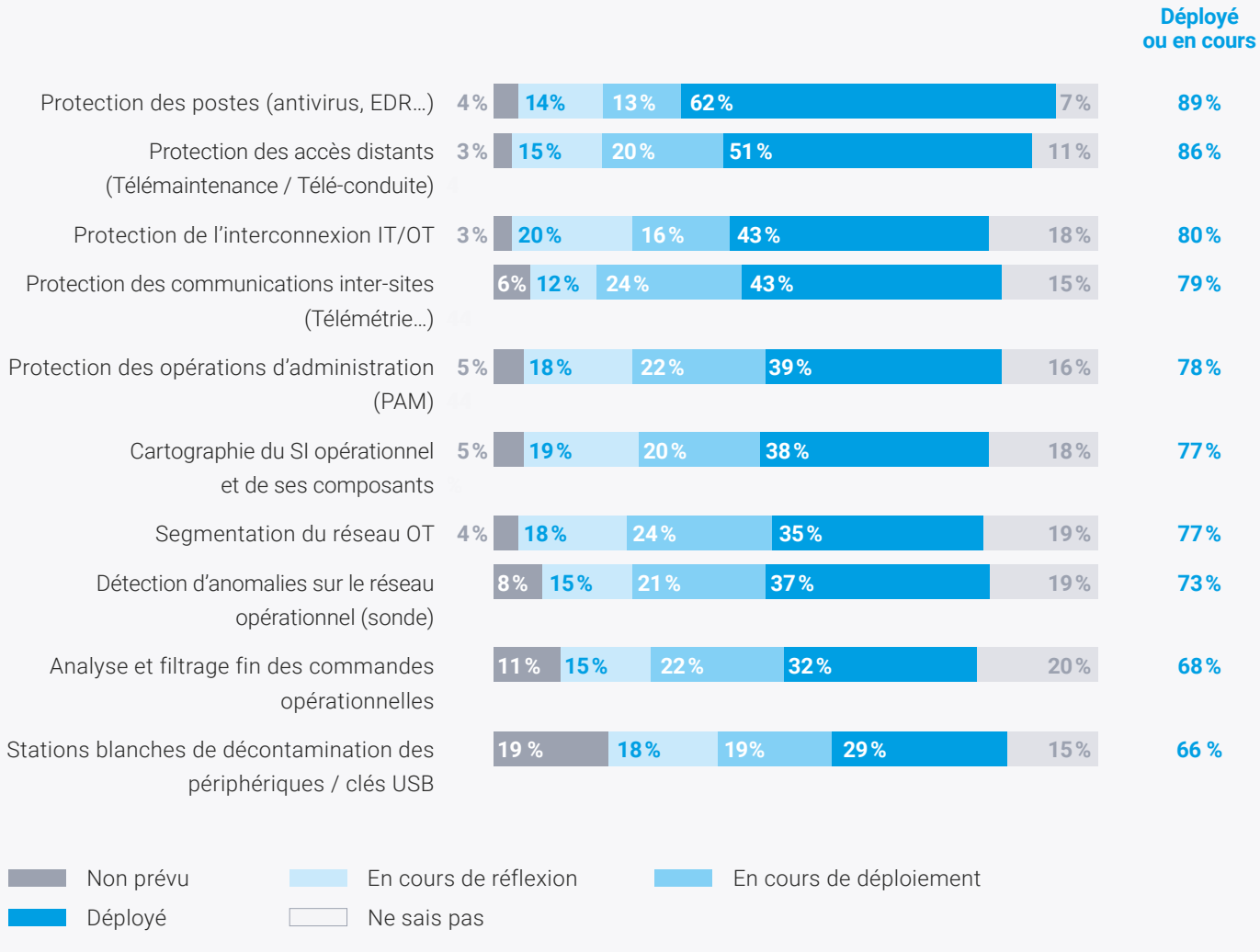
FOCUS TPE/PME

QUELLES SONT LES PROTECTIONS DÉPLOYÉES OU À VENIR AU SEIN DE VOTRE ENTREPRISE POUR SÉCURISER VOS ENVIRONNEMENTS OPÉRATIONNELS ?



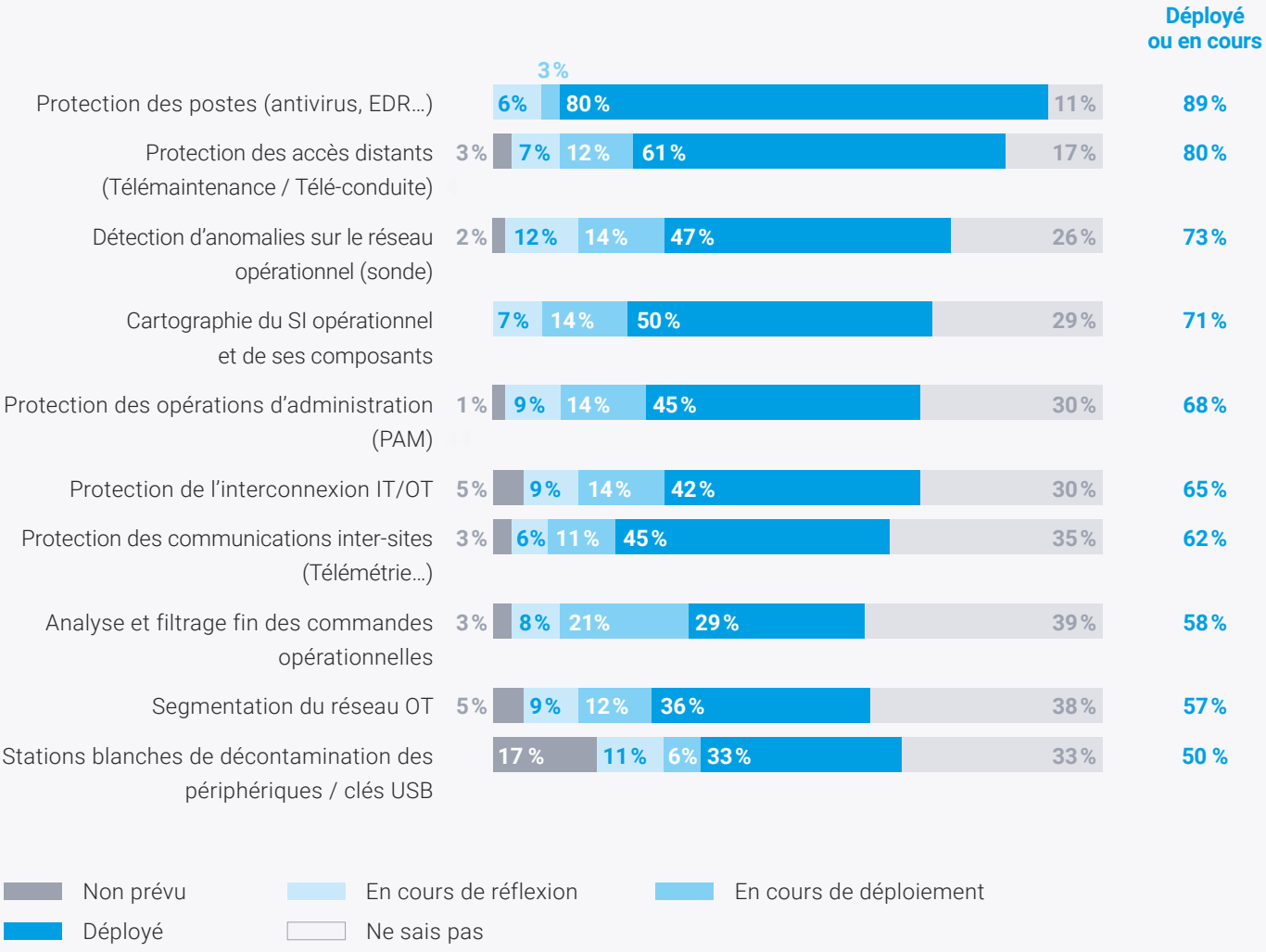
FOCUS ETI

QUELLES SONT LES PROTECTIONS DÉPLOYÉES OU À VENIR AU SEIN DE VOTRE ENTREPRISE POUR SÉCURISER VOS ENVIRONNEMENTS OPÉRATIONNELS ?



FOCUS GRANDES ENTREPRISES

QUELLES SONT LES PROTECTIONS DÉPLOYÉES OU À VENIR AU SEIN DE VOTRE ENTREPRISE POUR SÉCURISER VOS ENVIRONNEMENTS OPÉRATIONNELS ?



Cette situation hétérogène s'explique par les niveaux de ressources très différents entre grands groupes et petites structures, mais pas seulement : de par leur activité considérée comme critique, certaines structures industrielles sont soumises à de fortes obligations règlementaires quand d'autres sont laissées libres d'agir selon leur appréhension du risque. Du moins pour l'instant.



La règlementation vise aujourd'hui au premier chef les industries dites critiques comme l'énergie, les transports ou la chimie. D'ici 2 à 5 ans, tous les secteurs industriels seront concernés.

Rodolphe de Beaufort, Délégué Général Adjoint du GIMELEC et Animateur du Club CyberOT

L'avance des grands groupes en matière de cybersécurité industrielle tient également à la meilleure sécurisation de leur SI classique : ils peuvent désormais se concentrer sur la protection de leurs environnements opérationnels.

2.3.

Quelles solutions pour l'avenir ?

Outre des solutions déjà mentionnées comme la cartographie des systèmes ou la sécurisation des accès, les répondants évoquent différents moyens pour mieux protéger leurs environnements opérationnels. Parmi eux, de grands classiques tels qu'une meilleure sensibilisation des employés, le changement régulier des mots de passe, la sauvegarde extérieure quotidienne, la mise en place de firewalls ou encore la détection de fuite de données.

Deux grandes tendances se dessinent également, avec :

- le développement de **nouveaux composants hardware** pour les produits. Cette nouvelle génération d'automates, de capteurs et de protocoles intègre et intégrera la sécurité nativement.
- le déploiement de **solutions cloud**, au-delà de la cybersécurité. Certaines industries envisagent de déployer des infrastructures cloud pour augmenter leur puissance de calcul. Cette migration permet de traiter de plus gros volumes de données, dont les données de production remontées par les capteurs IoT et nécessaires au développement de la maintenance prédictive par exemple. Le recours au cloud permet également d'optimiser les infrastructures et la productivité en déportant le non-essentiel pour se concentrer sur l'excellence opérationnelle. De nouvelles solutions de cybersécurité apparaissent pour sécuriser ce nouveau périmètre.

Jean-Yves Poichotte, Directeur de la cybersécurité du groupe Sanofi, a ainsi par exemple récemment déclaré que l'objectif de Sanofi était d'avoir à terme **50 %** de son infrastructure dans le cloud. À l'opposé du spectre stratégique, certains répondants se disent quant à eux favorables à l'internalisation du système.



Les équipes R&D de Schneider Electric ont adopté une approche cybersécurité by design : la question est prise en compte sur l'ensemble de nos produits connectés ou connectables, dès la conception et avant même le développement de fonctionnalités.

Marc Fromager, Vice-président Industrial Automation & End Users, Schneider Electric France

INTERVIEW CROISÉE

Vers un écosystème interopérable

Avec Vincent Nicaise, Responsable écosystème et partenariats industriels Stormshield, et Khobeib Ben Boubaker, Head of Industrial Security Business Line Stormshield.

COMMUNIQUER POUR MIEUX PROTÉGER

Khobeib Ben Boubaker — L'interopérabilité, c'est-à-dire la capacité de systèmes à opérer ensemble, existe depuis longtemps dans le champ de l'IT. Pour ce qui est de l'OT, c'est encore en train de se mettre en place.

Vincent Nicaise — Parler de solutions de cybersécurité industrielle interopérables englobe aussi bien des solutions 'pure OT' que des solutions OT/IT : on pense par exemple à des firewalls déployés dans l'environnement opérationnel qui remontent des informations comme des logs de sécurité dans un SOC IT.

SERVIR LE PRINCIPE DE DÉFENSE EN PROFONDEUR

Vincent Nicaise — L'interopérabilité permet de faciliter la gestion et d'accroitre l'efficacité d'un environnement technique composé des meilleures solutions dans chaque domaine. Cette approche multi spécialiste ou best-of-breed participe à l'application du principe de défense en profondeur aux systèmes d'information, classiques comme industriels.

Khobeib Ben Boubaker — La bonne coopération entre les meilleurs éditeurs en cybersécurité est bien entendu importante. Mais la volonté d'interopérabilité doit aussi être portée par l'ensemble de l'écosystème, à commencer par les industriels eux-mêmes qui doivent accepter de partager de la donnée.

UN EXEMPLE DE COOPÉRATION RÉUSSIE

Vincent Nicaise — Nous avons établi un partenariat technologique avec le fournisseur de sondes industrielles Nozomi Networks. Celles-ci assurent l'inventaire et la détection avancée de cyber-menaces dans les environnements industriels mais ne permettent pas de répondre directement aux incidents détectés. L'intégration avec un firewall Stormshield permet d'acquérir cette capacité. En effet, lorsque la sonde Nozomi Networks détecte une vulnérabilité sur le réseau, elle fournit automatiquement une règle au firewall pour neutraliser l'attaque ou réduire son impact. Le partage de l'état des équipements identifiés sur le réseau entre les deux solutions facilite également la gestion des règles de sécurité.

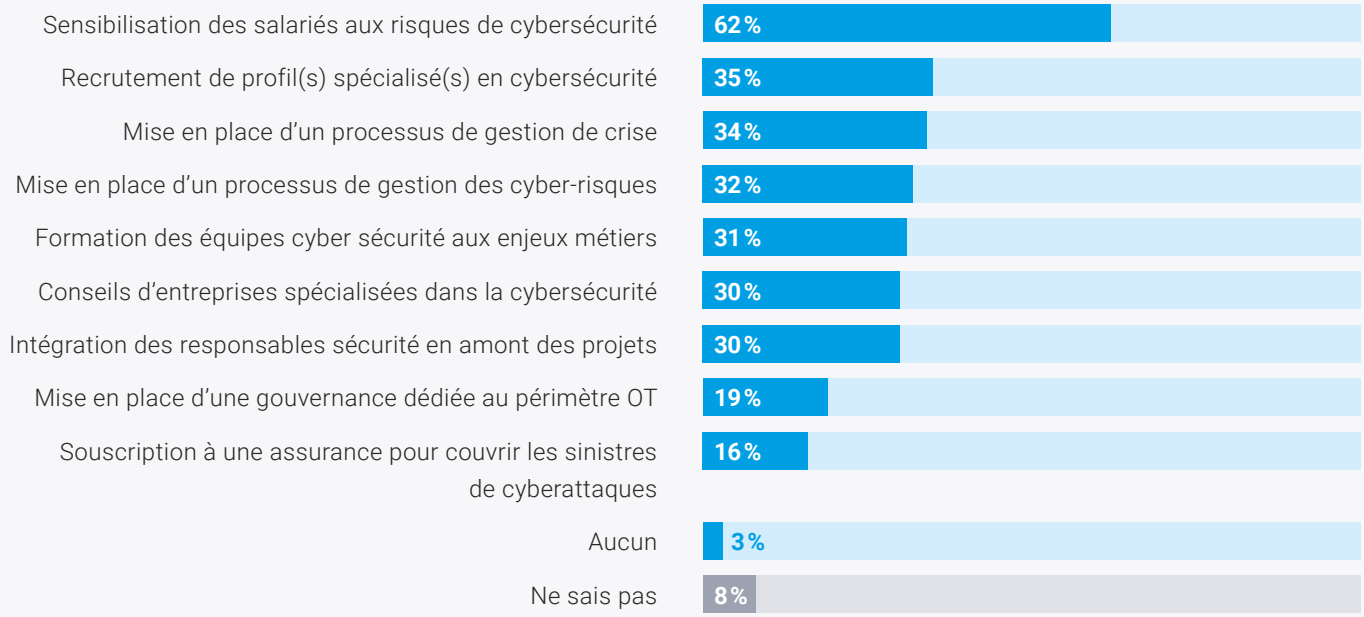
Khobeib Ben Boubaker — Il y a une logique naturelle au rapprochement de nos solutions, complémentaires et certifiées CSPN : elles permettent au monde industriel de passer à un mode de cybersurveillance actif !

2.4.

La sensibilisation des industriels : l'adaptation comme facteur clé

La sensibilisation est le premier moyen mis en œuvre pour faire face aux défis de la cybersécurité en milieu opérationnel. Elle est citée par **62 %** des répondants.

QUELS SONT LES MOYENS MIS EN ŒUVRE PAR VOTRE ENTREPRISE POUR FAIRE FACE AUX DÉFIS DE LA CYBERSÉCURITÉ DE VOS ENVIRONNEMENTS OPÉRATIONNELS ?

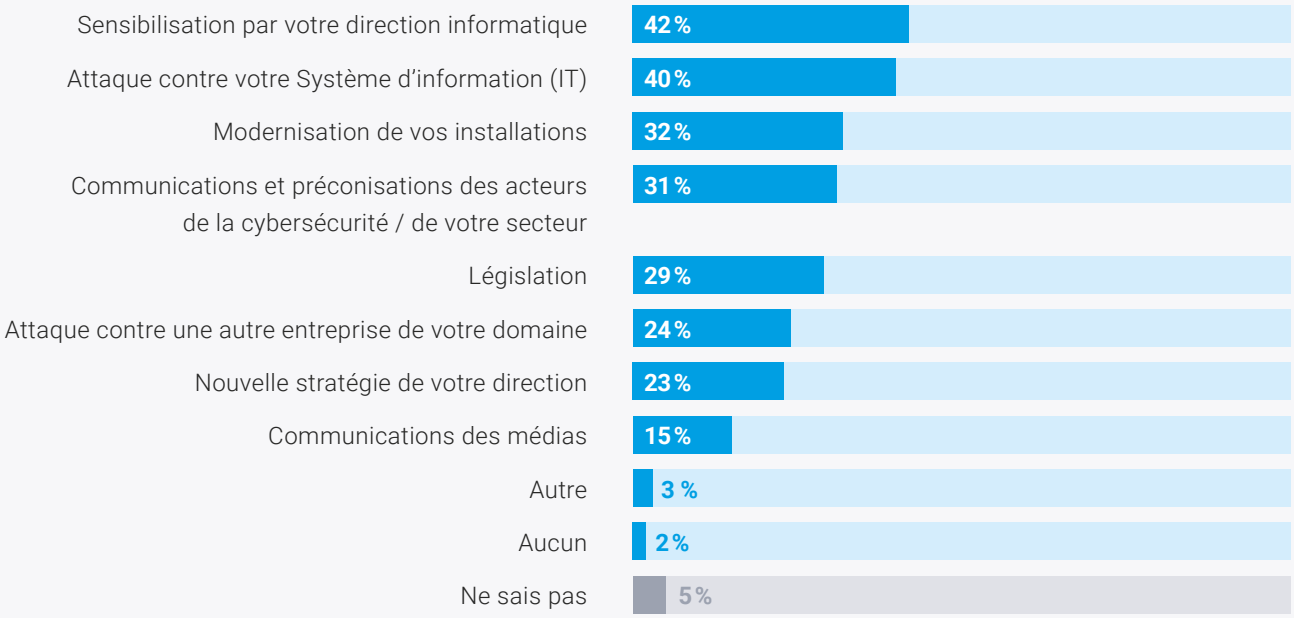


Les opérateurs industriels ont beau être assez sensibilisés à la cybersécurité dans leur utilisation personnelle des outils informatiques, des actions de formation pragmatiques, adaptées à leur contexte, sont indispensables.

La sensibilisation doit par ailleurs s'étendre à l'ensemble de la chaîne logistique de l'industriel. Tant que d'autres réponses comme les composants sécurisés ne seront pas plus matures, elle demeure en effet l'un des leviers les plus efficaces face à la problématique cyber.

La sensibilisation est également citée comme un déclencheur à la mise en place de solutions de cybersécurité en milieu opérationnel par **42 %** des répondants.

QUELS SONT LES ÉLÉMENTS DÉCLENCHEURS À LA MISE EN PLACE DE SOLUTIONS DE CYBERSÉCURITÉ DANS VOTRE ENVIRONNEMENT OPÉRATIONNEL ?



La prise en compte de la cybersécurité industrielle est encore assez neuve et réactive. Nous sommes souvent sollicités pour réaliser des audits post-rétablissement à la suite d'une attaque, plus rarement en prévention.

Thaïs L., auditrice senior pour un pure-player français de la cybersécurité

03

LES BONNES INTENTIONS À L'ÉPREUVE DU REEL

3.1 — La pénurie de talents spécialisés **28**
3.2 — Une chaîne de prestation à sécuriser **30**
3.3 — Des budgets plus conséquents à allouer à la cybersécurité industrielle **32**

3.1.

La pénurie de talents spécialisés

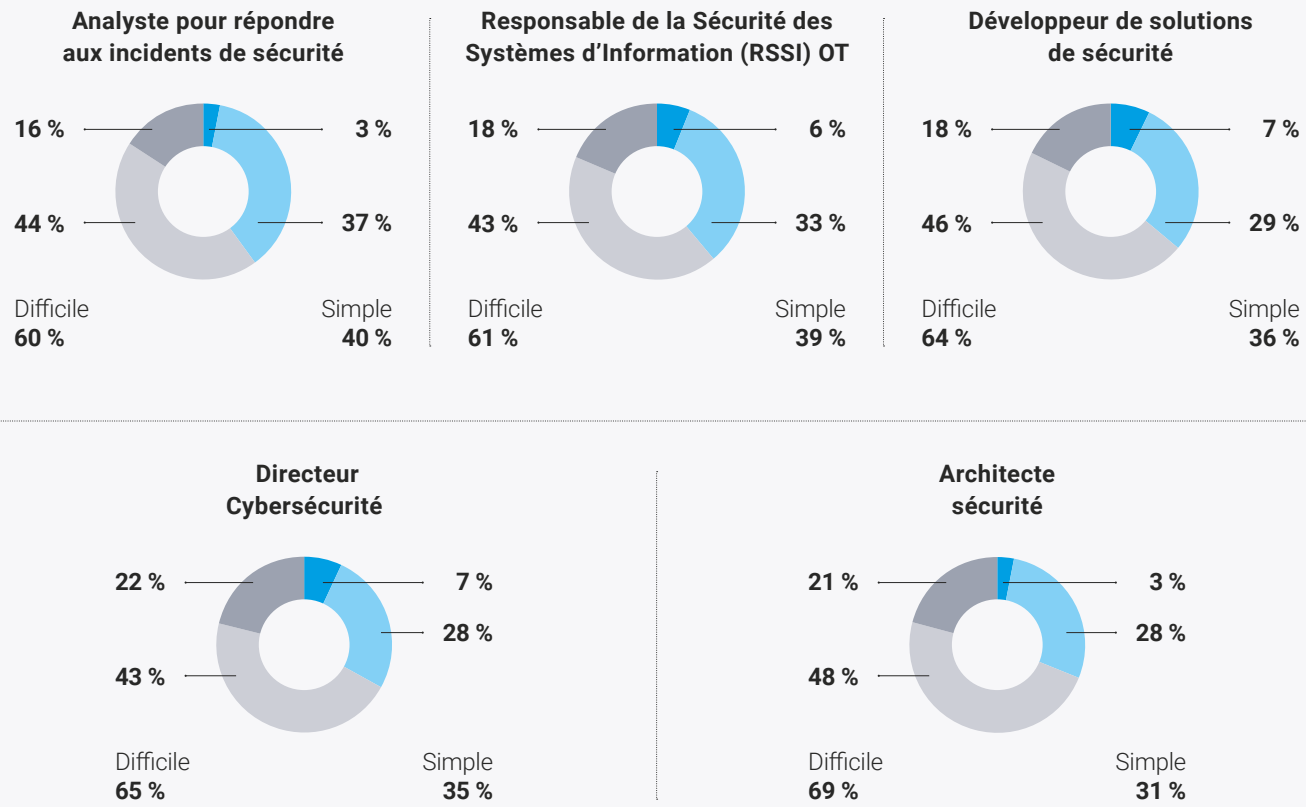
Les consultants cybersécurité figurent parmi les 8 « nouveaux » métiers très recherchés dans l'industrie selon Capital. Sur différents profils de postes liés à la cybersécurité industrielle, notre étude pointe de très fortes difficultés de recrutement. Entre **60 %** et **70 %** des répondants estiment que ces postes sont difficiles, voire très difficiles, à pourvoir. Une statistique peu étonnante au vu de l'état du marché de l'emploi cyber en général.

Pourtant, la cybersécurité industrielle a besoin de spécialistes car ses priorités sont très différentes : gestion des accès, sûreté, tout doit servir la disponibilité et la productivité.

70 %

Jusqu'à 70 % des répondants déclarent que les postes de cybersécurité sont difficiles, voire très difficiles, à pourvoir

DANS VOS ENVIRONNEMENTS OPÉRATIONNELS, LE RECRUTEMENT DE CES PROFILS DÉDIÉS À LA CYBERSÉCURITÉ EST-IL PLUTÔT SIMPLE OU DIFFICILE ?





Pour sécuriser une infrastructure faite d'automatismes, on a besoin de comprendre le procédé industriel.

Marc Fromager, Vice-président Industrial Automation & End Users, Schneider Electric France

Les écoles d'ingénieur ne proposent pas encore de formations académiques dédiées à faire émerger ces profils à la double compétence. Dans ces conditions, l'apprentissage se fait forcément sur le terrain et/ou via les modules de formation proposés par certains acteurs du secteur, comme Schneider Electric.

Alors vaut-il mieux faire monter en compétence les automaticiens, experts du contexte OT, ou former les experts cyber IT au contexte OT ? Le débat reste ouvert et laisse entrevoir une troisième voie, celle de la collaboration entre équipes cyber et équipes métier. Indispensable pour faire face sur un marché de la cybersécurité industrielle en croissance de plus **7 %** chaque année.

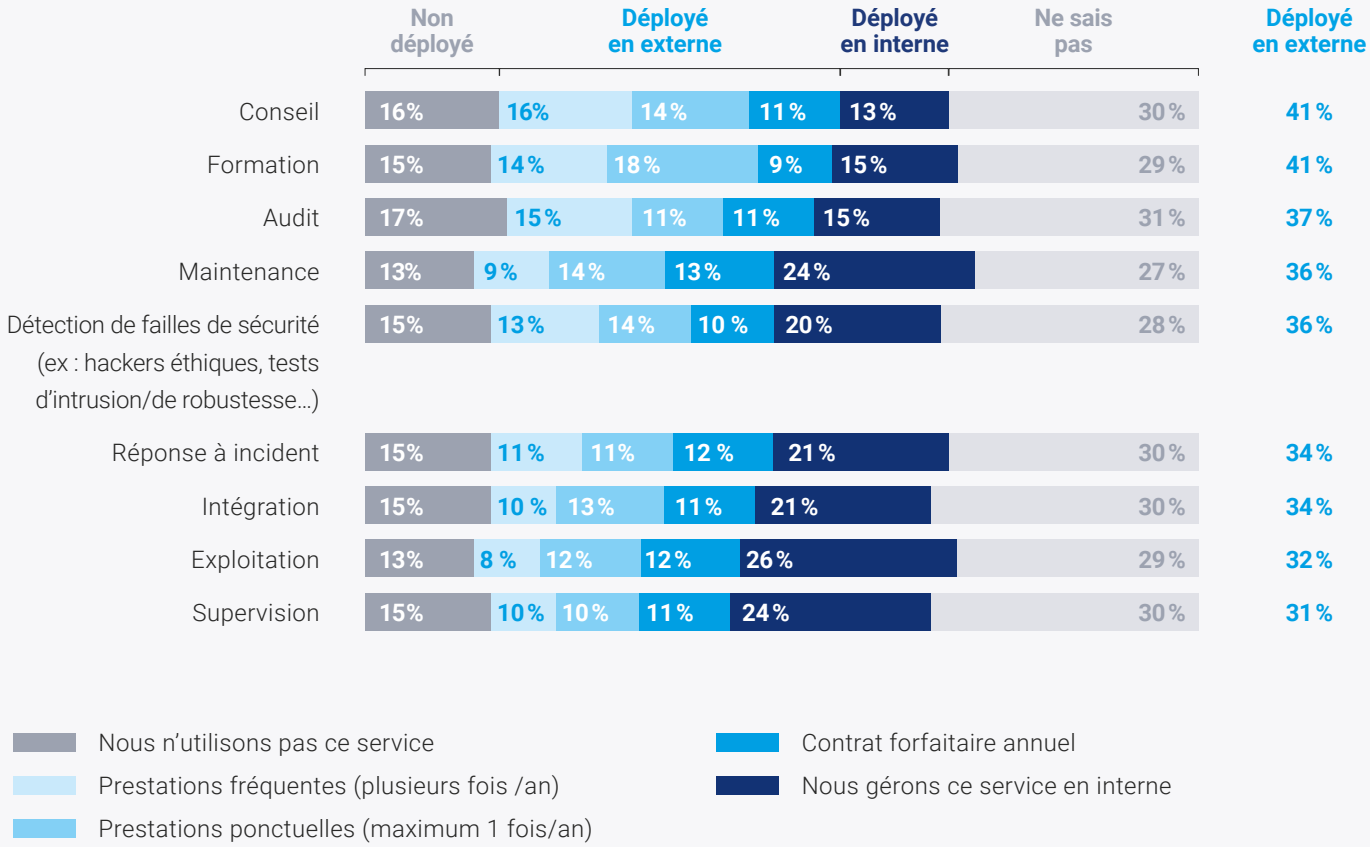
3.2.

Une chaîne de prestation à sécuriser

Les chaînes d'approvisionnement et de prestation des industriels ont toujours impliqué un grand nombre d'acteurs. À cette longue liste, il faut désormais ajouter les sociétés de cybersécurité puisque **41 %** des répondants font par exemple appel à des cabinets de conseil spécialisés dans ce domaine.

Qu'il s'agisse de réponse à incident (**34 %**), d'intégration (**34 %**), d'exploitation (**31 %**)ou encore de supervision (**32 %**), près d'un tiers des sondés fait également appel à une ou des sociétés externes. Et ce, au moins une fois par an. Près de **4 répondants sur 10** externalisent des missions de maintenance, d'audit ou de détection de failles de sécurité.

À QUELLE FRÉQUENCE FAITES-VOUS APPEL À DES SERVICES CYBER EXTERNES POUR VOS ENVIRONNEMENTS OPÉRATIONNELS ?



Externaliser la partie cyber permet de pallier le manque de compétences internes en contournant les difficultés de recrutement. Les industriels bénéficient également de la mutualisation opérée par ces sociétés de service.

Vincent Nicaise, Responsable écosystème et partenariats industriels, Stormshield

S'il est compréhensible, ce recours à l'externalisation doit cependant inciter des industriels confiants dans la cybersécurité de leurs propres systèmes opérationnels à redoubler de vigilance. Pour éviter une attaque de chaîne d'approvisionnement, il leur faut s'assurer que leurs prestataires et fournisseurs soient également bien protégés.

Le cas SolarWinds a malheureusement démontré que les sociétés de sécurité elles-mêmes n'étaient pas à l'abri et pouvaient propager malgré elles ce genre d'attaques par rebond. Tout commence en 2019, lorsque des cybercriminels (Nobelium) accèdent sans se faire repérer au système de production d'Orion. Ce logiciel, édité par la société texane SolarWinds, est utilisé dans de très nombreuses organisations, entreprises et industries, dont plusieurs agences gouvernementales américaines. Au total, ils réussiront à infecter 18 000 clients via une mise à jour malveillante, baptisée Sunburst. Parmi eux, 250 auraient été infiltrés par la suite dans le monde entier. Découverte fin 2020, cette attaque fait déjà date dans l'histoire de la cybersécurité.

Espérons qu'elle aura servi à inviter le sujet dans les discussions (et les contrats) entre partenaires et fournisseurs qui n'ont d'autre choix que de collaborer pour faire face à ces nouvelles menaces.

3.2.

Des budgets plus conséquents à allouer à la cybersécurité industrielle

D'après les résultats de notre étude, la cybersécurité industrielle représenterait moins de **10 %** du budget global de l'entreprise pour **1 répondant sur 2**. Elle constituerait moins de **10 %** du budget IT pour un peu plus de **4 sondés sur 10.** Enfin, **39 %** des répondants estiment que ce budget cybersécurité industrielle va augmenter dans les années à venir.

Les pouvoirs publics ont en effet démontré leur intérêt pour la modernisation de l'industrie, mais sans consacrer un budget spécifique à la question de la cybersécurité des réseaux OT en particulier pour l'instant. Les effets de plans comme France Relance ou France 2030 sont donc indirects pour le secteur de la cybersécurité industrielle et ne concernent que les nouveaux investissements. Ces plans de réindustrialisation et de transformation numérique de l'industrie restent néanmoins des opportunités d'embarquer plus de cybersécurité.

10 %

Un répondant sur deux déclare que la cybersécurité industrielle représente moins de 10 % du budget global de l'entreprise. Et moins de 10 % du budget IT pour un peu plus de 4 sondés sur 10.

Le renouvellement d'un parc machine se fait souvent ligne de production par ligne de production. Ces équipements neufs intègrent désormais la notion de cybersécurité mais se pose la question de leur maintien et celle de la mise à niveau des systèmes existants.

Rodolphe de Beaufort, Délégué Général Adjoint du GIMELEC et Animateur du Club CyberOT

Ces investissements sont encore insuffisants par rapport au besoin réel de sécurisation. Il peut être difficile de débloquer des budgets pour des projets cyber qui ne génèrent pas de rentabilité puisque leur rôle est avant tout assurantiel.

Marc Fromager, Vice-président Industrial Automation & End Users, Schneider Electric France

Conclusion

Le monde de la cybersécurité fait état de nombreuses cyberattaques aux conséquences sérieuses. Cette actualité, associée à un ensemble de signaux faibles issus de notre étude, laisse craindre une sous-évaluation du risque encouru. Ce faux sentiment de sécurité semble même concerner des entreprises ayant déjà subi une attaque et amorcé un travail de protection.

La cybersécurité industrielle constitue pourtant un prérequis indispensable pour espérer conduire sereinement la transformation numérique de l'industrie aujourd'hui et construire une industrie 4.0 robuste demain.

Le risque que l'interconnexion des réseaux fait peser sur les industries est (malheureusement) là pour durer. Il est donc crucial de le prendre en compte et d'investir dès maintenant dans une protection de tout le système de production. Tout en ayant conscience qu'il continuera d'évoluer et la cybersécurité industrielle avec lui.

Solutions Stormshield

Les principes de base pour cybersécuriser vos réseaux informatiques industriels sont les suivants :

→ Acquérir une vue d'ensemble
→ Protéger les réseaux par la segmentation
→ Authentifier et valider le trafic
→ Gérer les accès à distance
→ Protéger les postes
→ Adapter les équipements de sécurité aux contraintes opérationnelles de l'industrie

Pour vous y aider, Stormshield a conçu :



→ **SNi40 et SNi20, les solutions de firewalls industriels**
Ces firewalls disposent de boitiers renforcés pour répondre aux besoins des environnements à fortes contraintes. Faciles à monter en armoires électriques et idéaux pour toutes les questions de sous-segmentation de réseaux OT, ils peuvent être installés au sein du système opérationnel à protéger. D'un côté, le SNi40 est spécifiquement conçu pour protéger les API et les PLC. De l'autre, le SNi20 convient notamment aux réseaux distribués constitués de peu d'automates. Important à noter également que le SNi40 est le seul firewall industriel à disposer de la certification CSPN et de la qualification au niveau Standard de l'ANSSI.



→ **SNxr1200, pour embarquer la cybersécurité**
Ce pare-feu chiffreur est la seule solution de protection réseau intégrée dans un boitier ultra durci de série. Cette solution sécurisée convient donc tout particulièrement aux environnements à très forte contraintes – nécessitant des équipements de protection embarqués.



→ **Stormshield Endpoint Security (SES)**
La solution SES combine un moteur d'analyse comportementale, un moteur de contrôle des périphériques et une capacité à effectuer un whitelisting d'applications, rendant inactif tout logiciel qui n'est pas strictement nécessaire. Et pour une protection encore plus efficace, il est possible de maintenir une sécurité proactive, même lorsque le poste n'est pas connecté à un réseau de gestion ou à Internet.

Sources / Références

Baromètre des attentes et des besoins des décideurs face au déploiement de solutions dans les environnements opérationnels Stormshield/Usine Digitale.

Méthodologie : questionnaire auto administré en ligne, rempli entre le 17 novembre et le 12 décembre 2021 par 210 décideurs issus du secteur de l'industrie.

SOURCES

- Norsk Hydro : une communication exemplaire à l'épreuve des marchés — ZDnet
- Norsk Hydro chiffre à 46 millions d'euros l'impact de la cyberattaque au premier trimestre — Le Figaro
- Frappé par un ransomware, Honda suspend sa production — L'Usine Digitale
- Touché par un ransomware, Honda stoppe sa production — Le monde informatique
- Les leçons de l'attaque « SolarWinds » — La Presse
- Jean-Yves Poichotte (Sanofi) : « Depuis le début de l'année, nous avons bloqué 8 millions de cyberattaques » — Mindhealth
- Visés par une cyberattaque, des sites portuaires européens sont au ralenti — L'Usine Digitale
- Nautisme - le Groupe Bénéteau victime d'une cyberattaque — Actunautique.fr
- Cadres : 8 nouveaux métiers très recherchés dans l'industrie — Capital
- Guide pédagogique de la cybersécurité OT, publication fin avril 2022

Le **choix européen**
de la **cybersécurité**

www.stormshield.com

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privative sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.

Copyright © 2022 Stormshield