Rockwell Automation

RÉSULTATS DE L'ENQUÊTE 2022

Préparation des infrastructures critiques en matière de cybersécurité : éviter la paralysie totale

Table des matières

INTRODUCTION

Les secteurs des infrastructures critiques affrontent une véritable tempête dans le domaine de la cybersécurité. Les entités de production (OT) sont confrontées à des vulnérabilités croissantes, à des lacunes nouvelles et existantes en matière de cybersécurité, à une augmentation de la surface d'attaque et à des menaces mondiales en hausse.

Des acteurs capables de sophistication et disposant de nombreuses ressources, notamment des gangs spécialisés dans les rançonlogiciels et des acteurs étatiques, ciblent les opérateurs d'infrastructures critiques. In 2021, 83 % des opérateurs d'infrastructures critiques ont répondu avoir subi des violations de la cybersécurité[1]. Alors que les attaques continuent d'augmenter et que les vulnérabilités des infrastructures critiques ne sont toujours pas résolues, la paralysie totale, à savoir une catastrophe à grande échelle aux implications dommageables étendues, devient toujours plus réelle. Les entités des secteurs des infrastructures critiques ne peuvent rester spectatrices et démunies.

Pour comprendre l'état de la cybersécurité des infrastructures critiques et avoir une vue d'ensemble de la préparation et des meilleures pratiques des entités, Rockwell Automation a demandé à l'ISMG de réaliser une enquête auprès de responsables de l'informatique et de la cybersécurité dans différents secteurs d'infrastructures critiques. Ce rapport présente nos conclusions, de même que les enseignements tirés et des recommandations.

Nous avons structuré ce rapport en cinq thèmes principaux alignés sur le cadre de cybersécurité du NIST (Identifer, Protéger, Détecter, Répondre et Reprendre). Ce cadre sert aussi à Rockwell Automation de feuille de route fondamentale pour l'évaluation et le renforcement de la cybersécurité des infrastructures critiques.

[1] Skybox Security (via Yahoo! Finance) : 83 % des entités des secteurs des infrastructures critiques ont subi des intrusions, selon une étude de 2021 sur la cybersécurité, 11 novembre 2021

RÉSUMÉ

Les acteurs malveillants qui souhaitent provoquer le chaos ou rentabiliser rapidement leur investissement ont trouvé dans les entités des secteurs des infrastructures critiques une cible de choix. Par exemple, les gangs spécialisés dans les rançonlogiciels ciblent souvent les services publics, ainsi que les producteurs d'énergie et les entreprises du secteur pétrolier et gazier. Ils sont, parmi tous les acteurs de ces secteurs, ceux qui paieront le plus probablement une rançon[2] car ils ne peuvent pas courir le risque d'un arrêt.

La complexité de l'environnement informatique (IT) et de l'environnement de production (OT) rend aussi une reprise plus difficile pour ces entités, et les dommages liés à des arrêts peuvent être immenses, à savoir des temps d'arrêt, des pertes financières et des menaces pour la sûreté et le bien-être publics.

L'enquête de l'ISMG montre que les entités des secteurs des infrastructures critiques avancent dans la bonne direction. Elles prennent des mesures pour améliorer leur préparation et leur résilience en matière de cybersécurité. Néanmoins, l'enquête montre aussi la lenteur des progrès par rapport à l'urgence de la situation. Nombre d'entités doivent surmonter des obstacles tels que les contraintes budgétaires et la pénurie de talents, l'absence de priorité accordée par la direction et le manque de perspective sur la meilleure manière de consolider immédiatement les défenses.

La majorité ne met pas en place, ou trop lentement, des mesures fondamentales telles que les évaluations d'inventaire, la segmentation du réseau et la surveillance des menaces. Par conséquent, les vulnérabilités persistent sur l'ensemble des infrastructures critiques.

Conclusions principales pour être au premier plan sur le plan économique et de la sécurité :

1. **Les entités des secteurs des infrastructures critiques demeurent largement ouvertes aux cyberattaques.** L'enquête montre des lacunes significatives dans des domaines hautement prioritaires tels que la surveillance de l'inventaire des actifs, la gestion des accès à distance, la gestion des correctifs, la sécurité des terminaux, la segmentation du réseau, la planification de la réponse aux incidents et de la reprise, les évaluations de la sécurité de la chaîne logistique, et enfin la sensibilisation des employés à la sécurité. Par exemple, moins de 20 % des entités interrogées réalisent des audits d'inventaire des actifs selon la fréquence appropriée. Un tiers seulement a des pratiques efficaces de gestion des correctifs pour les technologies de la production. Par ailleurs, la détection continue des menaces est un angle mort pour toutes, avec 60 % des entités n'ayant pas de détection des menaces en temps réel. Le secteur de la fabrication et des machines ressort particulièrement, avec seulement 37 % des personnes interrogées indiquant avoir des mesures en place pour tous les aspects. Chose étonnante, les 63 % restantes ne font rien, c'est donc seulement une question de temps avant d'en voir les conséquences catastrophiques.
2. **La résolution des failles doit devenir une priorité urgente.** Des attaques publiées récemment montrent les coûts élevés des cyberattaques en termes de temps d'arrêt et de risque de paralysie des opérations, mais aussi de perturbations de la vie courante. Les attaques contre des réseaux de systèmes de commande de production (OT), dans des secteurs présentant un risque de répercussions sur la sûreté publique, notamment l'eau, l'agroalimentaire, le pétrole et le gaz, la santé et les transports, augmentent en volume et en intensité. Face à cela, les opérateurs d'infrastructures critiques ne vont pas assez vite pour réduire leur risque. Par exemple, 56 % seulement des personnes interrogées sont aujourd'hui capables d'analyser, de contenir et d'atténuer des attaques entrantes.
3. **Des budgets inappropriés augmentent le risque et freinent les avancées.** Les responsables de la sécurité ont cité le manque de financement comme un frein à leur capacité de mettre en oeuvre des processus et outils connus de réduction des risques, notamment les évaluations d'inventaire et la gestion des correctifs. Au vu du paysage des menaces et des dommages potentiels d'une cyberattaque, les opérateurs doivent reconnaître que le coût de l'inaction (ou d'une action trop lente) peut impacter considérablement la durée de fonctionnement, compromettre les systèmes et, au final, impacter les clients finaux, l'économie, voire la sécurité nationale.
4. **Les opérateurs n'anticipent pas suffisamment.** Le gouvernement américain resserre son action sur la cybersécurité à mesure que les risques géopolitiques augmentent. Le gouvernement fédéral envisage d'allouer 1 milliard de dollars en subventions pour la cybersécurité des opérateurs des infrastructures critiques, mais moins de 30 % des personnes interrogées disposent d'un plan de cybersécurité visant à identifier les lacunes en la matière et à faciliter la soumission d'une demande de subvention pouvant justement les aider à éliminer ces lacunes.
5. **Les opérateurs d'infrastructures critiques doivent agir rapidement.** Sur la base de ces conclusions, les experts en cybersécurité de Rockwell Automation recommandent les étapes de base suivantes :
   - Réaliser des évaluations précises des risques et vulnérabilités pour localiser les vulnérabilités majeures.
   - Élaborer un plan de cybersécurité basé sur les résultats des évaluations.
   - Segmenter et durcir les réseaux avec une zone démilitarisée industrielle (IDMZ) et des pare-feux.
   - Mettre en œuvre une surveillance des menaces.
   - Préparer et répéter les plans de réponse aux incidents.

CATÉGORIES REPRÉSENTÉES DANS L'ÉTUDE

L'enquête a été réalisée en janvier 2022 et a engrangé 122 réponses. L'ISMG a interrogé des responsables chevronnés de la sécurité industrielle, dont les fonctions vont du CISO au directeur commercial, en passant par le chef de la sécurité et l'ingénieur d'usine. Les CISO et les directeurs ou responsables de la sécurité ont constitué les deux plus grands groupes, à savoir près de 25 % et 19 % respectivement.

Les domaines des personnes interrogées ont englobé près de 20 secteurs de production, 57 % représentant des opérateurs d'infrastructures critiques, y compris le pétrole et le gaz, l'énergie, la chimie, ou encore le traitement de l'eau/des eaux usées. Les entreprises de fabrication ont, avec 18 %, eu le nombre le plus élevé de réponses pour un seul secteur.

[2] Sophos, « The State of Ransomware 2021 », avril 2021

SECTION 1

Identification et évaluation des risques

La sécurité des infrastructures critiques devient plus complexe ces dernières années. Les acteurs malveillants consacrent des ressources considérables afin de comprendre le mode de fonctionnement des nouveaux réseaux et systèmes d'infrastructures critiques interconnectés, et d'identifier des points faibles exploitables. Les opérateurs d'infrastructures critiques, toutefois, sont en retard dans l'obtention de cette visibilité pour eux-mêmes, afin d'identifier leurs risques et de prioriser les stratégies de défense.

Pour éviter la paralysie totale, les entités des secteurs des infrastructures critiques doivent prendre immédiatement des mesures urgentes pour appréhender les risques et éliminer les lacunes.

Évaluations de l'inventaire

L'audit de l'inventaire des actifs constitue une première étape clé de l'évaluation des risques. Il s'agit aussi d'un domaine dans lequel les entités éprouvent des difficultés à obtenir les bonnes informations et à adopter la fréquence de reporting appropriée. Selon une personne interrogée, « il est vraiment difficile de tenir l'inventaire à jour. Une machine virtuelle peut être mise en place et retirée avant même que l'équipe de gouvernance ait eu connaissance de son existence ».

Parmi les participants à l'enquête, la fréquence la plus courante d'évaluation de l'inventaire du parc installé est de moins d'une fois par trimestre, ce qui correspond à près de 30 % des réponses. Ce rythme est aussi le plus fréquent parmi trois secteurs très critiques : la fabrication et les machines ; les établissements de soins, la santé publique et les services d'urgence ; et enfin les secteurs de la pharmacie et de la chimie.

Globalement, 45 % des entités surveillent leur inventaire une fois par trimestre et moins d'une sur cinq réalise des audits quotidiens, ce qui constitue la pratique minimale recommandée par Rockwell Automation.

Pourquoi est-ce si important ?

Tout dispositif non pris en compte crée un point d'entrée vulnérable sur votre réseau. Il y a quelques années, des évaluations trimestrielles, voire mensuelles pouvaient être suffisantes. Désormais, avec la rapidité des attaques actuelles, des contrôles quotidiens sont, dans la majorité des cas, essentiels et certaines personnes interrogées indiquent avancer vers des évaluations en temps réel, ce qui est possible avec la conception de réseau appropriée et les bons outils de surveillance.

Nous avons aussi identifié une déconnexion du niveau de connaissance chez les opérateurs concernant les évaluations d'inventaire du parc installé. Des dirigeants interrogés (par ex., des directeurs financiers, des directeurs généraux et des directeurs de la production) ont été plus enclins à penser que les évaluations sont réalisées toutes les heures, quotidiennement ou une fois par semaine. Néanmoins, les technologues ayant une meilleure vue quotidienne des opérations de sécurité (par ex., les responsables de la sécurité, les directeurs ou architectes informatiques, ou les ingénieurs) ont dépeint un tableau moins positif, avançant systématiquement une fréquence mensuelle, trimestrielle ou encore plus espacée.

RECOMMANDATIONS

Les inventaires automatisés d'actifs améliorent la prévention ou le blocage d'attaques résultant d'un manque de visibilité. Une multitude d'outils et de services automatisés sont disponibles pour simplifier le processus d'évaluation d'inventaires, pour les technologies de l'information (IT) et les technologies de la production (OT), en utilisant la fréquence de votre choix au sein de votre seuil de tolérance de risque. Pour les opérateurs d'infrastructures critiques présentant un risque d'impacts démesurés sur la population, un inventaire en temps réel est une stratégie prudente et leur fournit une visibilité complète de leurs actifs de réseau.

Systèmes stratégiques

Selon notre enquête, seulement 56 % des entités avaient des systèmes stratégiques identifiés et priorisés. Cela indique que ce domaine est urgent (figure 1). Par ailleurs, selon l'expérience de Rockwell Automation, certaines entités sous-estiment l'efficacité de leurs protections autour des systèmes stratégiques. Les commentaires de l'enquête reflètent une partie de cette ambiguïté et une personne interrogée a indiqué avoir résolu cette étape avec un logiciel de sécurité robuste.

En réalité, le déploiement de contrôles de cybersécurité généraux n'assure pas forcément une protection adéquate des systèmes hautement critiques aux niveaux requis. Les systèmes opérationnels et de gestion les plus critiques doivent généralement être renforcés avec une segmentation de réseau supplémentaire, des contrôles des identités et des accès tels que l'authentification multi-facteurs, et les mesures associées. L'identification et la priorisation de la criticité garantissent d'abord que les bonnes stratégies de sécurité supplémentaires sont appliquées comme il se doit pour traiter le risque par système.

L'approche zéro confiance constitue une meilleure pratique de sécurité croissante sur l'ensemble des secteurs. Le gouvernement fédéral américain souhaite aussi la mise en œuvre de cette approche par les opérateurs d'infrastructures critiques et celle-ci a un rôle à jouer dans cette étape d'identification des systèmes stratégiques.

L'approche zéro confiance n'est pas un modèle de sécurité « tout ou rien ». Elle peut être abordée sous de nombreux angles et donner lieu à une application incrémentielle, même par petites étapes. L'identification et la priorisation des éléments les plus cruciaux pour l'entité constituent une étape clé dans cette démarche incrémentielle, et elles fournissent les connaissances permettant de placer les contrôles « zéro confiance » aux endroits où leur nécessité est maximale.

Les systèmes stratégiques sont-ils identifiés et priorisés ?

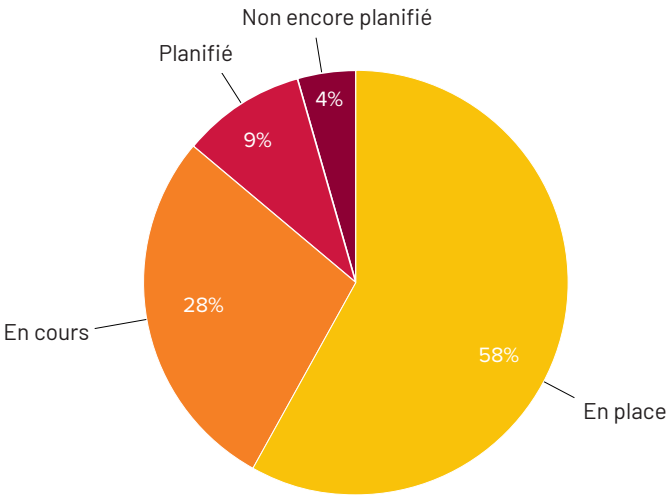


Figure 1

RECOMMANDATIONS

En vous inspirant de la stratégie zéro confiance, examinez tous les éléments DAAS de l'entité (à savoir les données, actifs, applications et services), et attribuez une priorité à chacun selon sa criticité. Il s'agit des « surfaces à protéger » de l'entité, chacune ayant les contrôles de cybersécurité appropriés en place par ordre de priorité.

Dans les infrastructures critiques, les systèmes de commande, ainsi que les données et applications de ligne de production sont des exemples de systèmes stratégiques probables. Demandez à vos équipes de gestion, de production, informatiques et de sécurité quelles seraient les conséquences d'un verrouillage de ces systèmes à la suite d'une attaque par rançonlogiciel. Interrogez-vous sur les systèmes permettant les opérations de production, la sécurité ou l'intégrité des données, les communications, la continuité de la chaîne logistique ou simplement la fourniture des services aux clients, afin de faciliter l'exercice de détermination des priorités.

SECTION 2

Protection et mises en œuvre des protections

La transformation numérique, la numérisation des processus et la technologie IoT, ainsi que la convergence OT/IT résultante, ont amélioré l'efficacité et la fiabilité des infrastructures critiques, en permettant aux prestataires d'offrir au public des services améliorés et plus rentables.

Ces évolutions sont certes positives, mais elles exposent les opérateurs d'infrastructures critiques à de nouvelles menaces et vulnérabilités, à travers l'exposition accrue à Internet via les capteurs et dispositifs, le télétravail, les API tierce partie, ainsi que de nombreux composants non sécurisés (notamment les automates programmables, les passerelles et les actionneurs).

Les contrôles de sécurité des systèmes OT diffèrent des pratiques pour l'informatique, car de nombreux composants OT sont dépourvus des protections de base. Les systèmes existants pilotant la production ne peuvent, bien souvent, pas faire l'objet de correctifs. Pour ceux qui le peuvent, l'application des correctifs est plus lente que pour l'informatique et ce ne sont pas les seules réalités de l'atelier.

D'autre part, la sécurité des technologies de la production devient de plus en plus la propriété des CISO, même si nombre d'entre eux ne comprennent pas pleinement les implications de la gestion de la sécurité OT et, par extension, de la sécurité de l'IoT. Côté face, les responsables de l'ingénierie des usines doivent préserver de manière fiable la durée de fonctionnement et n'ont pas le loisir d'arrêter des réseaux de production complets sur de longues périodes pour corriger des failles de sécurité, encore moins à la volée.

Cela explique peut-être les résultats de l'enquête, à savoir seulement 28 % des personnes interrogées ont aujourd'hui une feuille de route pour la convergence de la sécurité IT/OT et 35 % autres indiquent que le processus est en cours. Les entités des secteurs des infrastructures critiques doivent suivre la voie ouverte par le secteur de la fabrication et des machines, où 84 % des personnes interrogées ont indiqué avoir déjà réalisé cette convergence ou l'avoir inscrite sur leur feuille de route. Il est clair que les autres secteurs ont beaucoup de retard à rattraper.

Néanmoins, la marche vers la convergence continuera. Pour élaborer une feuille de route de convergence robuste, les responsables IT et OT doivent s'atteler à un véritable processus de planification conjoint. Rockwell Automation recommande généralement à nos clients de réserver une semaine complète, au cours de laquelle un expert des processus peut guider les deux équipes, afin qu'elles identifient l'ensemble des éléments, obstacles et exigences touchant à la sécurité. Cette approche suscite l'adhésion de toutes les parties prenantes pour la prise des décisions importantes.

Certains clients créent aussi un centre d'excellence de la cybersécurité, au sein duquel différents groupes d'acteurs de l'informatique, de la production et de la gestion collaborent en continu à la création de systèmes opérationnels et résolvent ensemble tout nouveau problème.

Accès à distance sécurisé

Les acteurs malveillants exploiteront n'importe quel biais leur permettant de prendre pied dans une entité. Alors que la pandémie provoque une évolution vers le télétravail intégral ou hybride et une mobilité globale accrue du personnel, les accès distants mal sécurisés sont devenus une cible facile.

La sécurité des systèmes d'accès à distance est souvent obsolète et utilise fréquemment uniquement des mots de passe et non une authentification multi-facteurs (MFA). Dans les secteurs des services publics, de l'extraction pétrolière/gazière et de l'exploitation minière, les informations d'identification utilisées pour la connexion sont le type de données bien souvent le plus exposé aux violations[3], et la profusion d'informations d'identification disponibles sur le Dark Web (suite à un vol ou une fuite) permet aux pirates mal intentionnés d'infiltrer aisément les systèmes d'accès à distance. Par conséquent, même si 69 % des personnes interrogées indiquent avoir des accès à distance sécurisés, le résultat peut être trompeur concernant l'adéquation de la protection des accès en question.

Dans ce domaine, la pandémie de la COVID-19 a constitué un défi et un atout. Une personne interrogée a fait remarquer que les modèles de travail hybride ont compliqué les accès à distance consolidés et une autre a déclaré que « le modèle de télétravail », qui est devenu la norme pendant la pandémie, a forcé les entités à être attentives à ces questions.

RECOMMANDATIONS

Un programme fiable de gestion des identités et des accès (IAM) est essentiel dans une stratégie zéro confiance. La solution IAM permet de savoir qui demande un accès, à quelles applications et données, à partir de quel emplacement, avec quel équipement et à quelle heure, et elle contrôle d'autres normes comportementales approuvées. Elle permet la surveillance et l'application de politiques et contrôles d'accès. Une solution IAM qui intègre une authentification multi-facteurs peut réduire sensiblement la menaces de mots de passe compromis.

Zone démilitarisée industrielle (IDMZ)

La création d'une zone tampon entre les systèmes de commande, les systèmes de production et l'informatique au moyen d'une IDMZ constitue une base de la conception de la cybersécurité des réseaux. En effet, elle contribue à empêcher les mouvements latéraux vers les réseaux de production et les automates, lorsque les acteurs malveillants accèdent aux systèmes informatiques, et inversement. Selon les réponses à l'enquête, près de 50 % des entités ont une zone démilitarisée industrielle dans leur architecture OT et 25 % supplémentaires travaillent à en établir une (figure 2).

Les établissements de soins, ainsi que les secteurs de la santé publique et des services d'urgence sont particulièrement en retard. En effet, 38 % des personnes interrogées n'ont pas encore planifié de zone démilitarisée industrielle, contre 16,5 % tous secteurs confondus. Ces conclusions sont conformes aux observations de Rockwell Automation sur le marché dans son ensemble.

Les zones démilitarisées industrielles ne sont pas la panacée pour la cybersécurité, en particulier dans la mesure où les systèmes OT et les dispositifs IoT peuvent se connecter directement à Internet via les réseaux informatiques. Des mesures doivent être mises en œuvre pour une défense robuste.

Quel est le statut de la mise en œuvre d'une zone démilitarisée industrielle (IDMZ) dans l'architecture de sécurité OT ?

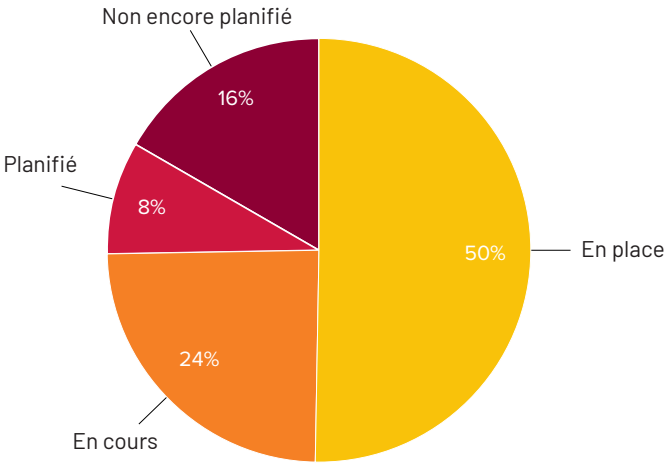


Figure 2

RECOMMANDATIONS

Pour une architecture sécurisée, la mise en œuvre d'IDMZ constitue une bonne pratique de base. En séparant les réseaux et actifs informatiques et de production, des acteurs malveillants ne pourront pas passer d'un système à l'autre. Il convient toutefois d'avoir à l'esprit qu'une architecture de sécurité moderne d'infrastructure critique doit inclure des défenses supplémentaires, en particulier autour des surfaces stratégiques à protéger et pour tous les actifs reliés à Internet.

[3] Verizon, « 2021 Data Breach Investigations Report », mai 2021

Gestion des correctifs

Les correctifs pour les technologies de la production constituent une zone sensible. L'enquête à confirmé une réalité constatée régulièrement sur le terrain : la gestion des correctifs n'est pas considérée comme une pratique importante, elle n'est pas financée ou sa mise en œuvre est simplement trop complexe. Parmi les personnes interrogées, 37 % seulement ont implémenté une gestion efficace des correctifs OT et 13 % n'ont pas encore planifié une approche en la matière (figure 3).

Dans le secteur de la fabrication et des machines, 42 % des entreprises interrogées n'ont pas de gestion efficace des correctifs ou n'ont rien en cours à ce sujet. Les principaux secteurs en avance sur les autres dans leur progression rapide sont le secteur manufacturier aux États-Unis et au Royaume-Uni/Irlande, et le secteur de la finance au Moyen-Orient et dans la région Asie-Pacifique.

Ces constatations sont alarmantes pour tous les secteurs, au vu du nombre de vulnérabilités découvertes et du risque de logiciels malveillants insidieux en embuscade.

De nombreux systèmes OT ne peuvent être corrigés par la voie normale, en raison de fonctionnalités limitées et/ou de structures existantes qui n'autorisent pas les composants de sécurité intégrés. L'application de correctifs peut aussi durer [à chaque fois] une journée entière lorsque vous avez des dizaines ou des centaines de serveurs réseau. Le coût résultant en termes de temps d'arrêt étant considérable, de nombreux opérateurs d'installations ont toujours résisté aux approches informatiques en matière de correctifs.

Quel est le statut de la gestion efficace des correctifs OT ?

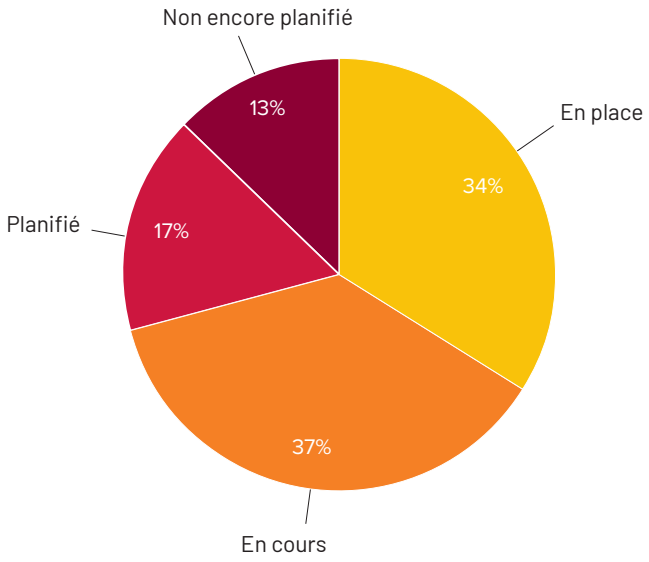


Figure 3

Des lacunes de sécurité supplémentaires

- **Supports amovibles.** À peine plus de la moitié des entités ont indiqué avoir des procédures de sécurité efficaces concernant les supports amovibles. Pour les autres, n'importe qui peut sortir des données à tout moment ou pénétrer dans les locaux et insérer un logiciel malveillant sur les réseaux. Il suffit d'examiner les affaires internes Snowden et Manning pour comprendre les implications potentielles. Une personne interrogée, dont l'entreprise travaille à une solution, a apporté cet excellent éclairage : « Configurez votre prochaine génération d'outils de détection et de réponse de terminaux (EDR) afin d'interdire les clés USB. »
- **Segmentation du réseau.** Dans un cas similaire, 49 % des entités ont mis en œuvre une segmentation ou une micro-segmentation pour protéger les systèmes stratégiques. Cette meilleure pratique essentielle est exigée par de nombreuses politiques publiques et est une composante clé de l'approche zéro confiance. Étant donné l'efficacité de cette approche, il va falloir probablement plus de décrets pour que les opérateurs d'infrastructures critiques segmentent efficacement les réseaux.
- **Sensibilisation du personnel.** 69 % des entités ont mis en place, à l'attention du personnel, des programmes de sensibilisation, de formation et de test sur le sujet de la sécurité. Le secteur financier et bancaire au Moyen-Orient et en Asie-Pacifique est pionnier dans ce domaine, alors que le secteur des transports et du tourisme aux États-Unis indique n'avoir aucune formation en la matière. Près d'un tiers des entités, globalement, n'ont pas mis en œuvre de formation à la sécurité, alors qu'il s'agit d'une bonne pratique fortement recommandée du cadre NIST. Les formations à la sensibilisation sont une mesure de protection éprouvée pour prévenir et bloquer les attaques initiées par un hameçonnage (celles-ci représentent une proportion énorme de 86 % des intrusions confirmées). Que vos programmes soient entre les mains des ressources humaines ou de l'informatique, veillez à ce qu'ils couvrent les cybermenaces et meilleures pratiques spécifiques aux technologies de la production. Nous recommandons aussi d'effectuer des tests de pénétration, afin d'identifier les domaines dans lesquels une formation supplémentaire du personnel s'impose.

RECOMMANDATIONS

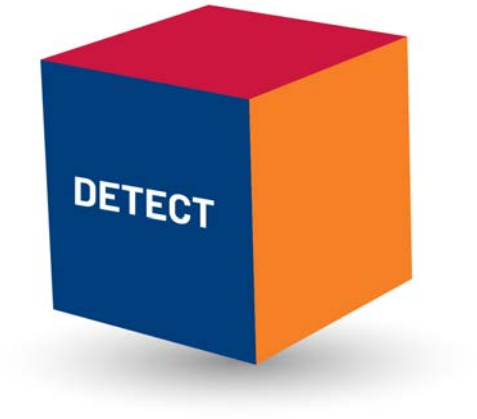
Les acteurs malveillants sont constamment à la recherche de vulnérabilités. Aucune entité, en particulier dans les secteurs des infrastructures critiques, ne peut continuer 'comme si de rien n'était'. Avec le risque accru de temps d'arrêt découlant de cyberattaques, l'équilibre risque/bénéfice entre ne rien faire et, au final, traiter la complexité des correctifs OT doit pencher naturellement vers la prévention, au vu des pertes et dommages potentiellement élevés.

Une gestion efficace et efficiente des correctifs OT commence par une expérience approfondie de l'industrie et une expertise de la cybersécurité des technologies de la production. Cette expertise contribue à éviter les pièges courants et à exploiter les meilleures pratiques découlant de nombreuses implémentations réussies. Le fait de travailler avec un partenaire qui comprend la dynamique des environnements de production et les graves implications de temps d'arrêt liés à des cyber-incidents peut rationaliser ce processus complexe mais indispensable, et permettre une application des correctifs OT avec un minimum de perturbations.

[4] Verizon, « 2021 Data Breach Investigations Report », mai 2021

SECTION 3

Détection des menaces et identifications des événements de cybersécurité



Un principe fondamental de la sécurité zéro confiance consiste à supposer qu'une intrusion a déjà eu lieu. Il ne faut faire confiance à aucune demande de connexion ou d'accès tant qu'elle n'est pas vérifiée et authentifiée systématiquement et de manière dynamique, ce en toutes circonstances. Ce principe repose sur une surveillance constante et en temps réel des activités malveillantes, afin de détecter et d'atténuer les menaces.

Malheureusement, les réponses à l'enquête montrent que la détection des menaces est un angle mort dans les secteurs des infrastructures critiques. Autrement dit, les attaques contre les systèmes OT peuvent passer inaperçues et les entités ne traitent pas les risques d'attaques fréquentes tels que les rançonlogiciels susceptibles de paralyser les opérations, les acteurs étatiques qui mènent des activités d'espionnage à long terme et les attaquants susceptibles d'infiltrer les systèmes et chaînes logistiques en vue d'une attaque d'envergure.

Détection des menaces et anomalies via un SOC OT

Un centre de sécurité des opérations (SOC) OT regroupe les technologies, les outils, les talents et d'autres ressources afin de surveiller les menaces 24 h/24 et 7 jours/7, et de pouvoir répondre à celles-ci. Un SOC OT est indispensable pour détecter rapidement les menaces et anomalies, et pour réduire l'impact sur les systèmes stratégiques. Selon notre enquête, 43 % des entités n'ont actuellement pas de détection en temps réel des menaces et anomalies via un SOC OT en place (figure 4), ce qui révèle une lacune généralisée dans la préparation en matière de cybersécurité.

La région Asie-Pacifique, l'Australie et la Nouvelle-Zélande sont en retard en matière d'implémentation de SOC OT, la première réponse étant « Non encore planifié ». Parmi les personnes interrogées de cette région, 31 % n'ont aucun SOC OT planifié, contre 16 % à l'échelle du globe. Une exploration approfondie des données montre qu'aucune entité de cette partie du monde travaillant dans les secteurs de l'énergie, de l'électricité et du nucléaire n'a de SOC ou n'en prévoit un. À titre de comparaison, 74 % des entités au Moyen-Orient et en Afrique ont mis en œuvre un SOC automatisé ou y travaillent, avec deux secteurs ouvrant la voie : la finance et la banque, d'une part, et d'autre part, l'énergie, l'électricité et le nucléaire.

D'autre part, 47 % des personnes interrogées n'ont pas mis en place de plate-forme de gestion des événements et informations de sécurité (SIEM) pour analyser les alertes de sécurité des applications et des équipements réseau. Alors que la majorité des systèmes SIEM ne génèrent pas de véritables alertes en « temps réel », certains en sont très proches, ce qui en fait un élément incontournable dans votre panoplie d'outils de SOC et un composant critique d'une défense efficace des infrastructures critiques.

Quel est le statut de la mise en œuvre d'une détection en temps réel des menaces et anomalies via un SOC OT (interne ou via des services administrés) pour les logiciels malveillants, les rançonlogiciels et les vulnérabilités ?

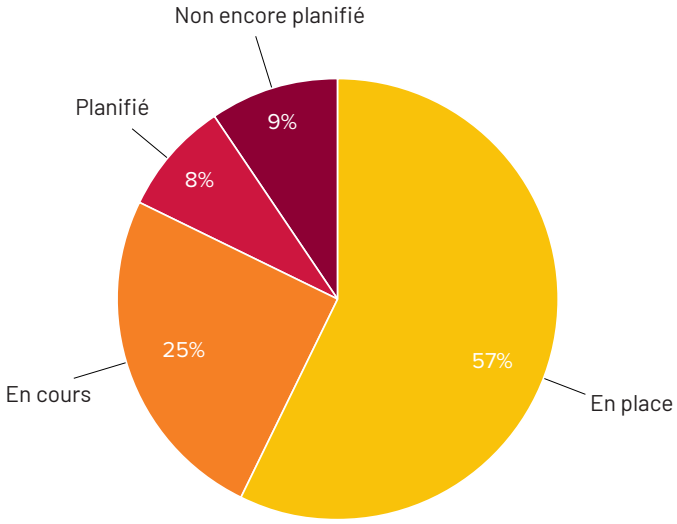


Figure 4

RECOMMANDATIONS

Les contraintes liées aux ressources, notamment le manque de compétences en interne, peuvent créer des obstacles insurmontables pour la capacité de nombreuses entités à surveiller et détecter les menaces. Néanmoins, il s'agit d'une pierre angulaire incontournable dans l'environnement actuel en pleine évolution des menaces pour les technologies de la production. Recourez à des solutions de SOC OT tierce partie, qui incluent des services tels que la surveillance continue des menaces et la réponse aux incidents.

Lorsque vous travaillez avec un partenaire fiable spécialiste des SOC OT, vous bénéficiez de l'expertise concrète d'une équipe de sécurité de haut vol, mais aussi des informations en temps réel obtenues auprès de tous les clients desservis par le SOC. Un SOC OT administré évite aussi des dépenses d'investissement élevées et garantit le déploiement à votre service du nec-plus-ultra en matière d'outils, de techniques et de connaissances du renseignement sur les menaces. Cette approche est avantageuse au vu de la pénurie mondiale de professionnels de la sécurité, qui est estimée à 2,72 millions de personnes ((ISC)² 2021 Cybersecurity Workforce Study).

Sécurisation des terminaux

Des capteurs IoT industriels et des équipements personnels des employés aux automates, la prolifération des terminaux étend considérablement la surface d'attaque des technologies de la production. La protection des opérations dans cet environnement constitue un problème croissant. Parmi les responsables de la sécurité interrogés, 46 % ne surveillent et ne contrôlent aujourd'hui pas en temps réel les terminaux 24 h/24, 7 jours/7 (figure 5). Autrement dit, une grande proportion de dispositifs connectés aux systèmes OT ne sont pas configurés correctement ou contiennent des failles de sécurité. Les entités peuvent avoir de la chance mais, dans la majorité des cas, c'est juste une question de temps avant que des acteurs malveillants exploitent ces terminaux non sécurisés et non surveillés lors de cyberattaques.

Quel est le statut concernant le contrôle des accès de tous les terminaux et leur surveillance en temps réel 24 h/24, 7 jours/7 ?

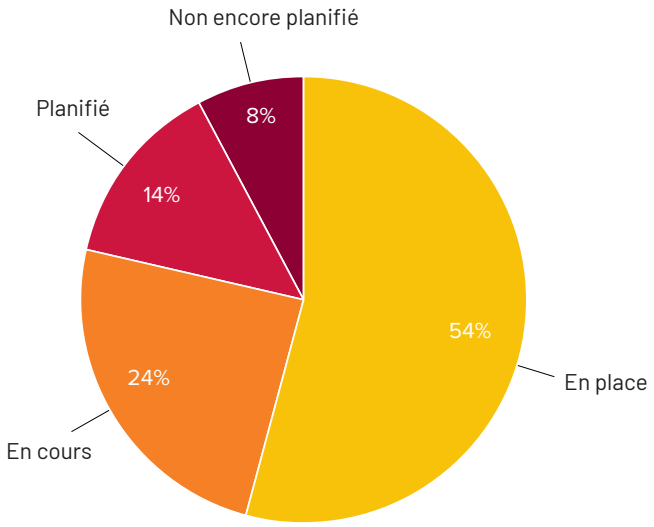


Figure 5

RECOMMANDATIONS

Les terminaux sont un domaine à consolider rapidement. Commencez par réaliser l'évaluation de l'inventaire des actifs de réseau mentionnée précédemment, afin d'identifier tous les terminaux connectés à votre réseau. Une fois les terminaux identifiés et évalués en termes de risques pour la sécurité, vous pouvez élaborer un plan, basé sur vos systèmes stratégiques identifiés et vos priorités en matière de sécurité, afin de déterminer les outils, le personnel et les services requis pour durcir les périmètres autour de ces points d'entrée.

SECTION 4

Réponse aux cyber-incidents

La planification et la préparation de la réponse aux incidents sont cruciales. Les préparatifs appropriés réduiront au minimum les temps d'arrêt, les pertes financières, les perturbations pour les clients et d'autres répercussions négatives des cyber-incidents. Pour les opérateurs d'infrastructures critiques, la rapidité de la réponse est cruciale, en raison de l'étendue possible des dommages, notamment en termes de service public et de sûreté, avec, dans certains cas, des conséquences pour des millions de personnes.

Les opérateurs d'infrastructures critiques réalisent des progrès, avec 57 % des personnes interrogées faisant état de capacités pour analyser, contenir et atténuer les cybermenaces (figure 6). Toutefois, nous avons aussi constaté que cet aspect est source d'inquiétude, peut-être en raison de l'évolution constante et rapide du paysage des menaces. Une personne interrogée a émis la remarque suivante : « Quelqu'un a-t-il trouvé une solution ? » Une autre personne pose aussi la question suivante : « Comment les opérateurs d'infrastructures critiques prévoient-ils d'aborder la continuité et la résilience de l'activité, alors qu'ils en sont encore à comprendre comment élaborer une stratégie basique de réponse aux incidents ? »

Quel est le statut concernant les capacités d'analyse, de confinement et d'atténuation des cybermenaces ?

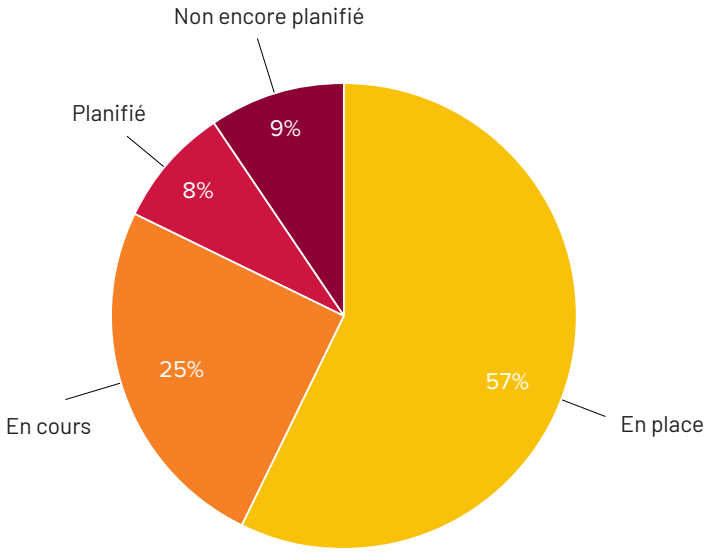


Figure 6

RECOMMANDATIONS

Si les ressources et l'expertise posent problème dans l'élaboration de votre stratégie de réponse aux incidents, envisagez de faire appel à un prestataire de services administrés, notamment un partenaire spécialiste des SOC OT, pour aller rapidement de l'avant et éviter les difficultés liées à l'embauche directe de talents expérimentés dans la cybersécurité, au vu de la pénurie mondiale en la matière. Un partenaire tel que Rockwell Automation, qui a une grande expertise des SOC OT et s'appuie sur un riche héritage industriel, peut vous apporter l'assurance d'avoir un plan efficace et opérationnel de réponse aux incidents. Il peut aussi réagir instantanément pour votre compte, afin de bloquer et d'atténuer si nécessaire les attaques. Les équipes d'experts réalisent aussi des formations continues et testent différents scénarios pour valider l'aptitude à répondre rapidement. Par ailleurs, un partenaire d'excellence en matière de SOC OT vous apportera une connaissance approfondie des exigences de conformité et de reporting dans le domaine des technologies de la production.

SECTION 5

Reprise après un incident

46 % des personnes participant à l'enquête ont déclaré qu'elles sont, aujourd'hui, prêtes avec des processus de reprise et qu'elles ont des systèmes, données et procédures opérationnelles pour restaurer rapidement les opérations après une cyberattaque.

En matière de récupération après une cyberattaque, qu'est-ce qui est considéré comme « rapide » ? Dans certains cas, une semaine peut sembler appropriée. Dans d'autres, chaque minute compte.

Par exemple, lorsque des compagnies d'électricité ont connu des pannes pendant la grande tempête de neige au Texas en 2021, un arrêt d'une semaine s'est soldé par des centaines de morts. Dans le cas de l'attaque par rançonlogiciel contre Colonial Pipeline, l'arrêt de seulement 24 heures s'est chiffré en millions de dollars, du fait des coûts et de l'impact économique considérable découlant de l'absence d'approvisionnement en essence sur la côte Est des États-Unis.

Même si le retour du fonctionnement à la normale est l'objectif clé de votre étape de reprise après incident, c'est aussi l'occasion d'identifier les domaines nécessitant des améliorations. La mise en œuvre de changements significatifs basés sur les enseignements des incidents instaure une culture de l'amélioration permanente de la cybersécurité, pour des systèmes encore plus résilients et plus protégés.

Utilisation des financements fédéraux

En novembre 2021, le Congrès des États-Unis a adopté une loi sur les infrastructures (H.R. 3684, Infrastructure Investment and Job Act) et alloué près de 2 milliards de dollars pour des mises à niveau et améliorations de la cybersécurité dans les infrastructures critiques. Sur cette somme, 1 milliard de dollars est prévu au titre de subventions pour des entités au niveau des États et au plan local, pour des organisations tribales et pour certaines organisations à but non lucratif. Les directives de demande de subventions sont en cours d'élaboration, mais Rockwell Automation s'attend à ce que les subventions soient alignées sur le cadre de cybersécurité du NIST (NIST Cybersecurity Framework), dans la mesure où il est utilisé par l'agence fédérale CISA (Cybersecurity and Infrastructure Security Agency).

Près d'un tiers des personnes ayant répondu à l'enquête (29 %) disposent d'un plan de cybersécurité adaptable pour la demande de subventions. 25 % supplémentaires ont un plan en cours d'élaboration. Cela laisse environ 40 % d'entités sans ce niveau de préparation.

Un plan de cybersécurité permet non seulement aux entités visées de demander rapidement des subventions, lorsque celles-ci sont disponibles, mais contribue aussi à lancer le type approprié de programme de cybersécurité systématique qui mettra au jour les lacunes, réduira les risques et aidera à prioriser les efforts, afin de protéger l'entité et ses clients vis-à-vis des impacts dommageables.

Rockwell Automation encourage tous les responsables d'entités des secteurs des infrastructures critiques à se familiariser avec cette législation, à préparer un plan de référence et à rechercher des financements si leur entité est éligible aux subventions. N'attendez pas la publication des critères d'éligibilité aux subventions. Agissez dès maintenant pour commencer à préparer et élaborer votre plan. Rockwell Automation a créé un modèle de planification de la cybersécurité et une liste de contrôle s'appuyant sur le cadre du NIST : **Télécharger le modèle de planification**

RECOMMANDATIONS

La planification de la reprise et de la restauration doit être une pratique aussi courante que la gestion des actifs, et elle est cruciale pour la fiabilité des durées de fonctionnement. Les coûts financiers et humains de temps d'arrêt continuent d'augmenter et vous ne pouvez pas escompter transférer la charge du risque à votre compagnie d'assurance. À mesure que la responsabilité augmente et que l'assurabilité devient plus limitée, la charge sera répercutée sur l'assuré pour couvrir la majeure partie des pertes et coûts de reprise.

ÉTAPES SUIVANTES

Préparation de l'avenir

Chaque opérateur d'infrastructure critique doit agir maintenant afin d'éviter la paralysie totale. Les vies, le bien-être, la sûreté et les moyens de subsistance en dépendent.

La cybersécurité OT n'est pas une chose aisée. D'un autre côté, la majorité des intrusions ont des défenses connues. Les opérateurs d'infrastructures critiques ont énormément progressé en matière d'efficacité et de fiabilité, à travers la transformation numérique et l'automatisation. Maintenant, ils doivent s'atteler à la cybersécurité avec la même ténacité. Il ressort de notre enquête que les secteurs des infrastructures critiques ont pris conscience du besoin d'une cybersécurité moderne et ciblée. Néanmoins, cette prise de conscience est lente, des lacunes importantes demeurent, certaines priorités sont mal définies et il manque une certaine clarté concernant les risques et les meilleures pratiques.

Néanmoins, les responsables des infrastructures critiques commencent à s'intéresser de près à ces questions. De nombreuses personnes interrogées ont indiqué planifier ou mettre en place des protections importantes. Les opérateurs d'infrastructures critiques passent d'un faible niveau de sensibilisation à une attitude réactive après des attaques importantes relayées dans les médias et la réponse associée des autorités. Leur question maintenant est de savoir comment accélérer leur démarche de cybersécurité.

Rockwell Automation : Sécuriser ce sur quoi le monde est bâti.

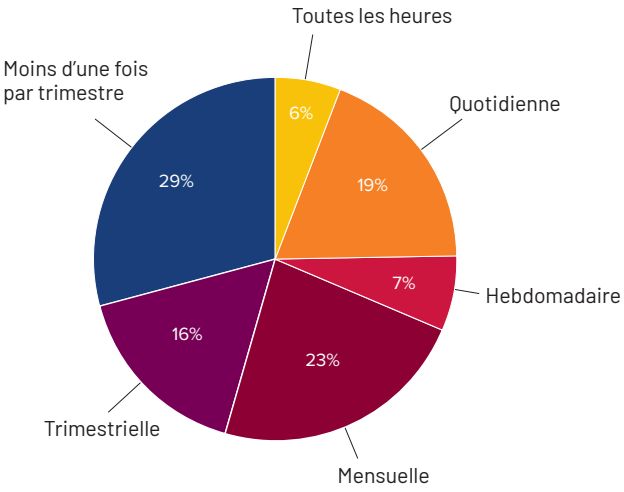
Rockwell Automation fournit une multitude de solutions et services de sécurité industrielle pour vous aider à gérer les menaces et à décupler la résilience de votre écosystème OT et IT. Nos experts peuvent vous aider à construire une infrastructure réseau robuste et sécurisée tout en renforçant votre protection contre les menaces et votre rapidité de réponse aux incidents. Outre notre expertise et notre connaissance approfondies des meilleures pratiques les plus récentes, nous apportons aux opérations de production une expérience s'appuyant sur plus de 100 ans au service de l'automatisation industrielle. Nos sites dans le monde entier permettent à nos clients d'appliquer des cyberprotections multisites à l'échelle mondiale, avec l'optimisation de la logistique que vous êtes en droit d'attendre du leader de l'automatisation industrielle.

RECOMMANDATIONS

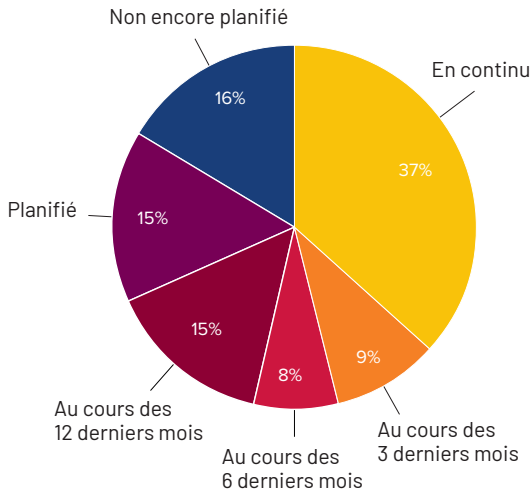
- Effectuez **l'évaluation Rockwell Automation de préparation en matière de cybersécurité** et recevez un rapport personnalisé, qui prend pour référence les participants à l'enquête originale. Découvrez le positionnement de votre entité selon son secteur, sa taille et sa région.
- Téléchargez notre **modèle de plan de cybersécurité OT** pour avoir un aperçu des outils, des services et du personnel nécessaires pour protéger efficacement vos opérations. Pour les entités des secteurs des infrastructures critiques aux États-Unis : utilisez le modèle de plan pour préparer votre demande de subvention, afin de vous aider à éliminer vos lacunes en matière de cybersécurité.
- **Contactez un professionnel Rockwell Automation** et découvrez comment nous pouvons vous aider à protéger au mieux vos opérations industrielles avec le programme de sécurité OT adapté.

ANNEXE

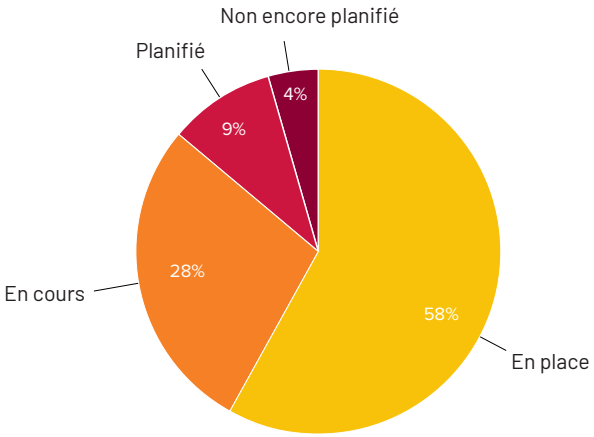
Quelle est la fréquence d'évaluation de l'inventaire du parc installé ?



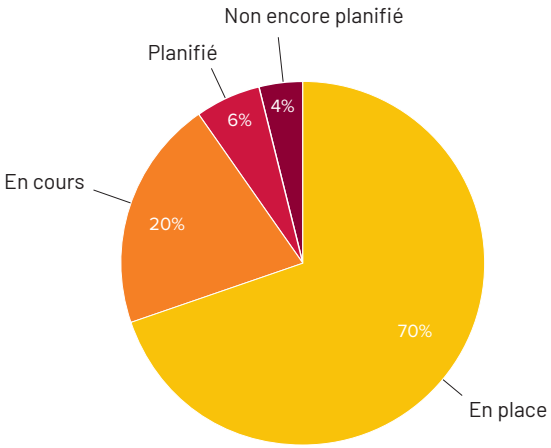
Quelle est la fréquence d'évaluation des risques de la chaîne logistique ?



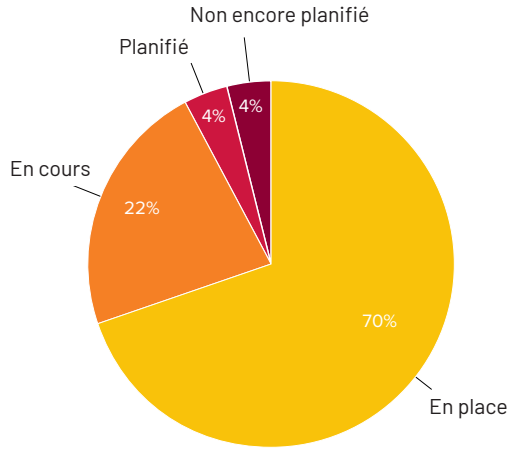
Les systèmes stratégiques sont-ils identifiés et priorisés ?



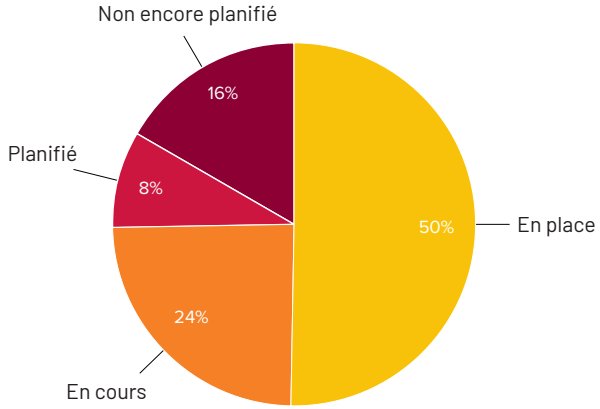
Quel est le statut concernant les contrôles des accès à distance pour la connexion sécurisée hors site ?



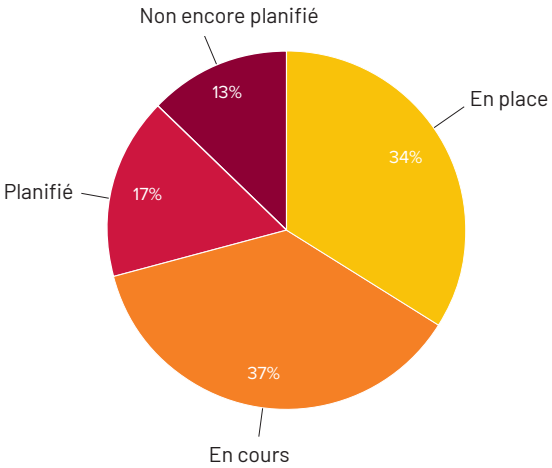
Quel est le statut des contrôles d'accès physiques qui identifient et empêchent les accès non autorisés aux systèmes ?



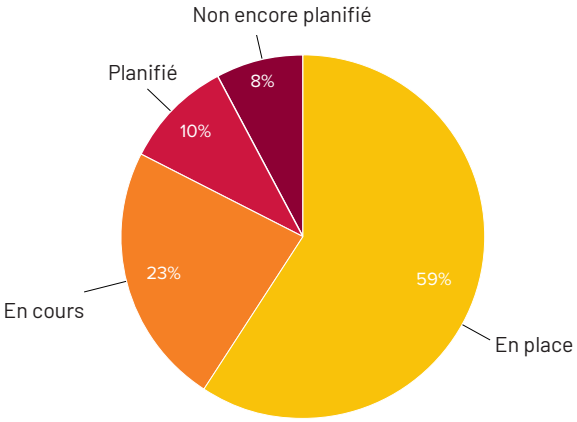
Quel est le statut de la mise en œuvre d'une zone démilitarisée industrielle (IDMZ) dans l'architecture de sécurité OT ?



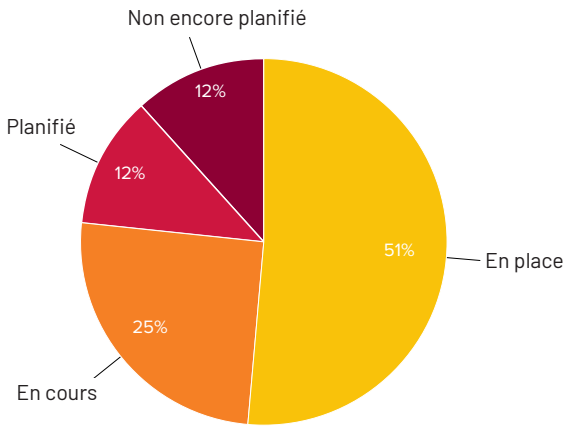
Quel est le statut de la gestion efficace des correctifs OT ?



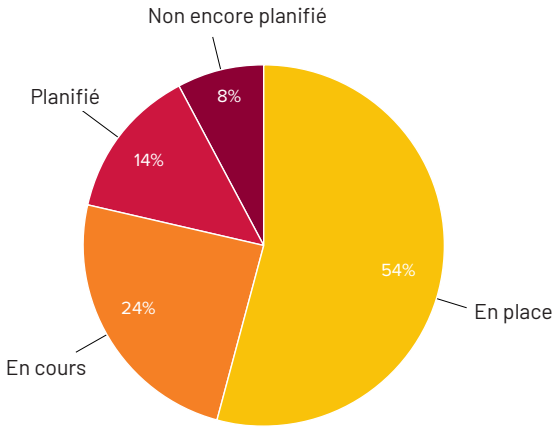
Des processus de sauvegarde des données des systèmes opérationnels sont-ils exécutés régulièrement ?



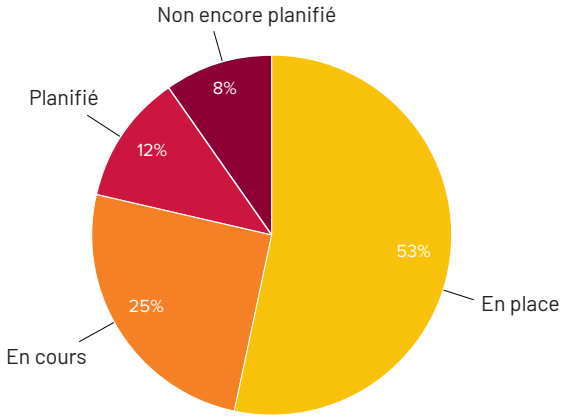
Technologie de protection : Quel est le statut des procédures efficaces de sécurité concernant les supports amovibles ?



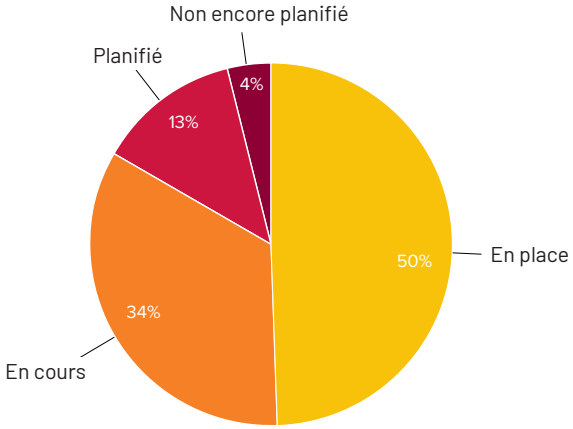
Quel est le statut concernant le contrôle des accès de tous les terminaux et leur surveillance en temps réel 24 h/24, 7 jours/7 ?



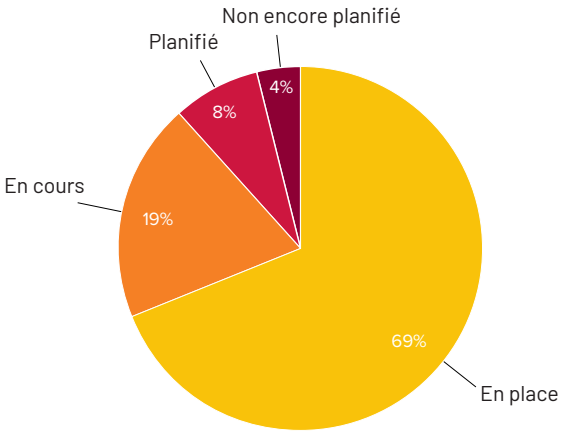
Quel est le statut du système de gestion des événements et informations de sécurité (SIEM), pour fournir des analyses en temps réel des alertes de sécurité générées par les applications et le matériel du réseau ?



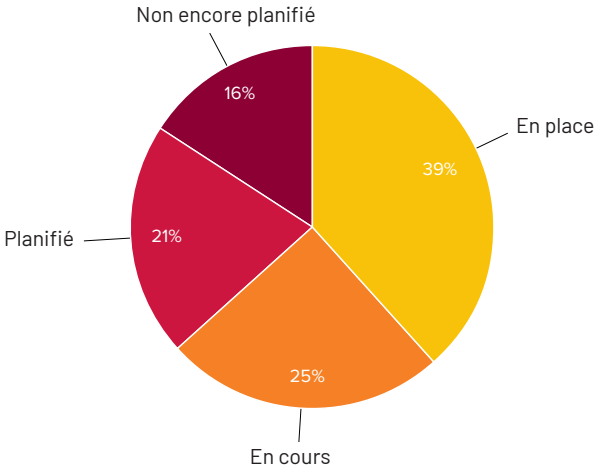
Quel est le statut de la mise en œuvre de l'architecture de segmentation/ micro-segmentation du réseau, afin d'instaurer des périmètres de sécurité autour des systèmes stratégiques ?



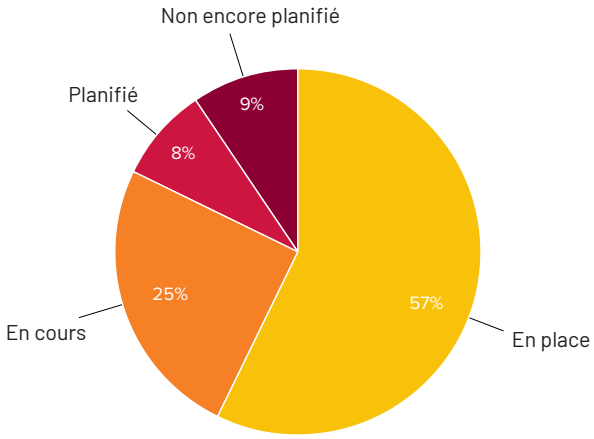
Avez-vous des formations de sensibilisation du personnel à la sécurité et des tests associés ?



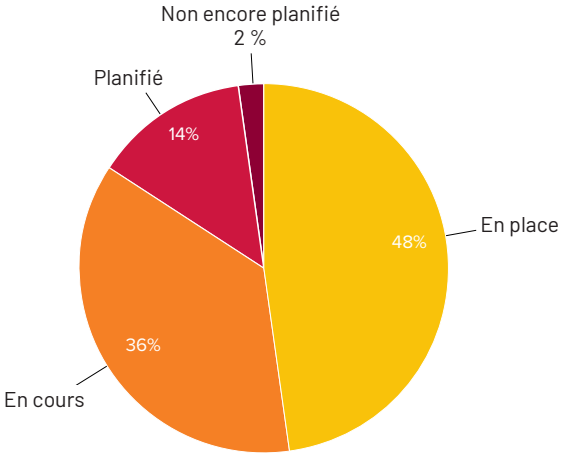
Quel est le statut de la mise en œuvre d'une détection en temps réel des menaces et anomalies via un SOC OT (interne ou via des services administrés) pour les logiciels malveillants, les rançonlogiciels et les vulnérabilités ?



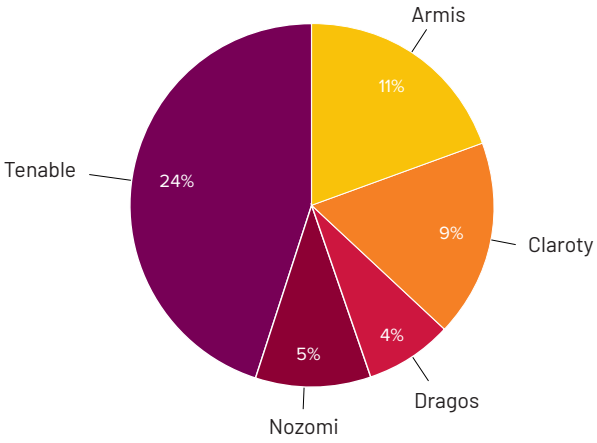
Quel est le statut concernant les capacités d'analyse, de confinement et d'atténuation des cybermenaces ?



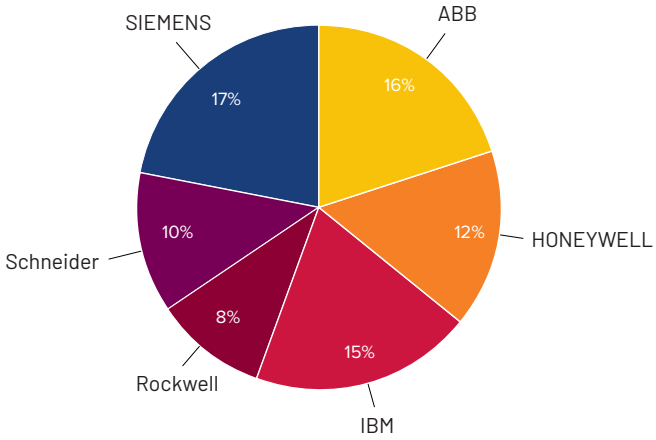
Quel est le statut des systèmes, données et procédures opérationnelles pour la restauration rapide des opérations en cas de cyberattaque ?



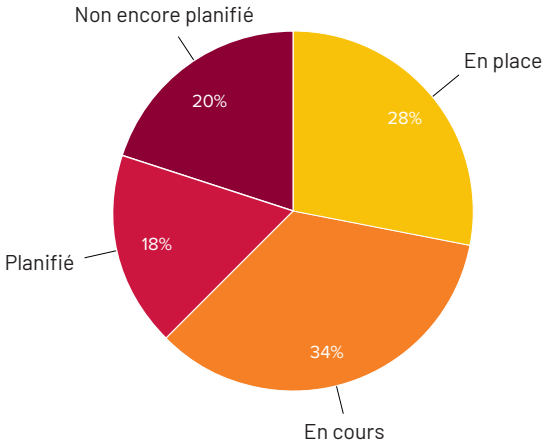
Des plates-formes ou services de détection des menaces OT sont-ils utilisés ?



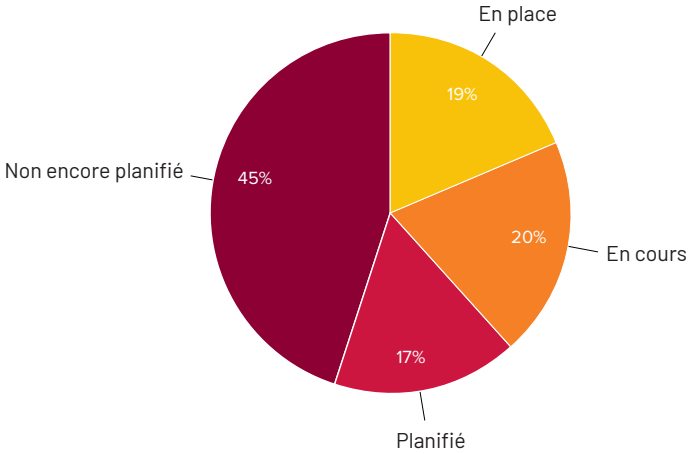
Quels sont les prestataires de services d'automatisation industrielle sollicités ?



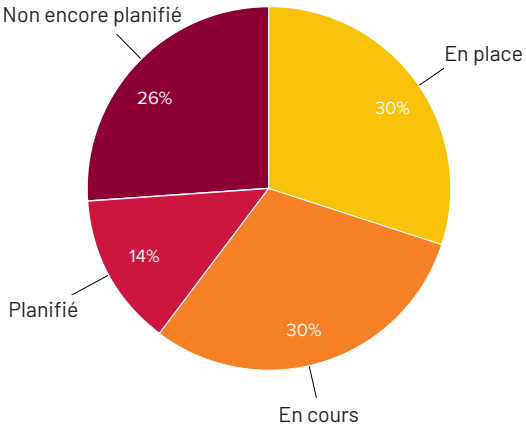
Quel est le statut de l'implémentation d'une feuille de route de cybersécurité pour la convergence IT/OT ?



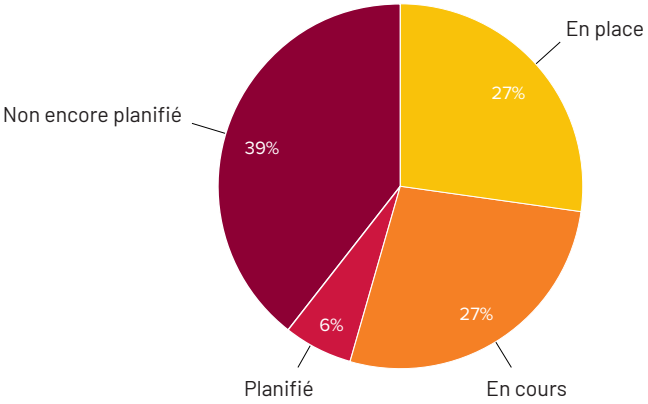
Quel est le statut de l'utilisation de produits certifiés CIP (Common Industrial Protocol) pour sécuriser et crypter les communications Ethernet ?



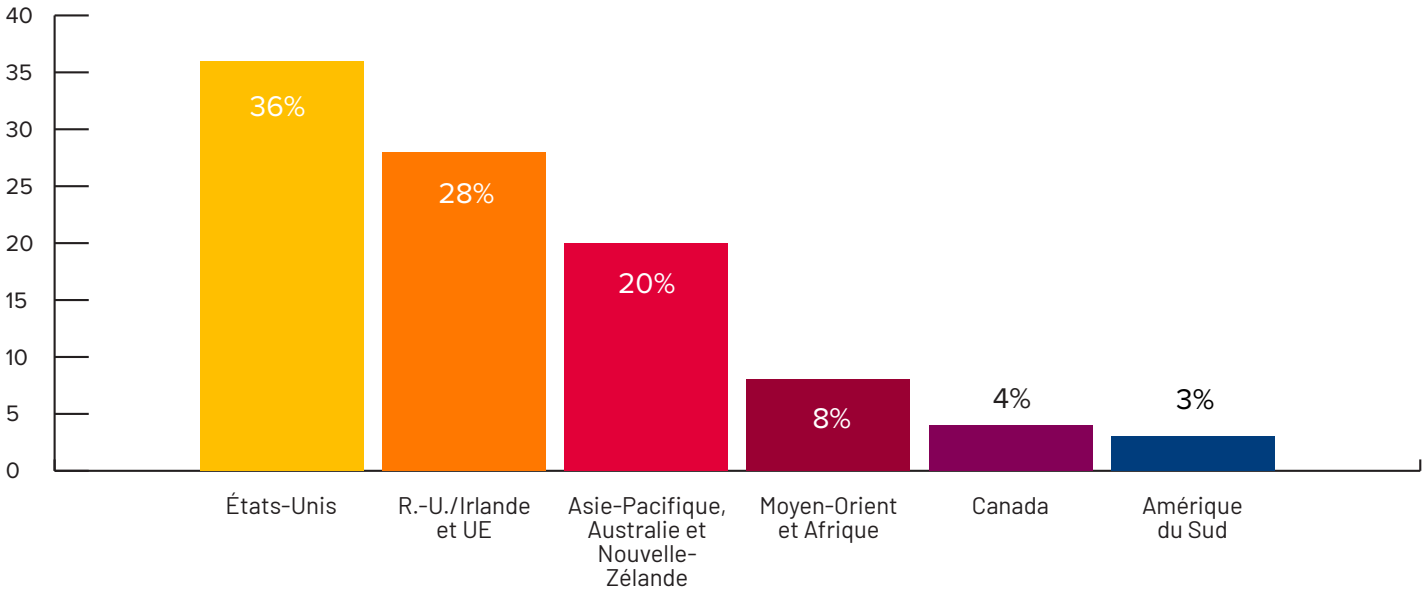
Votre entité travaille-t-elle avec un ou plusieurs partenaires spécialistes de la cybersécurité, lesquels proposent des services de SOC OT évolutifs et mis à jour de manière dynamique ?



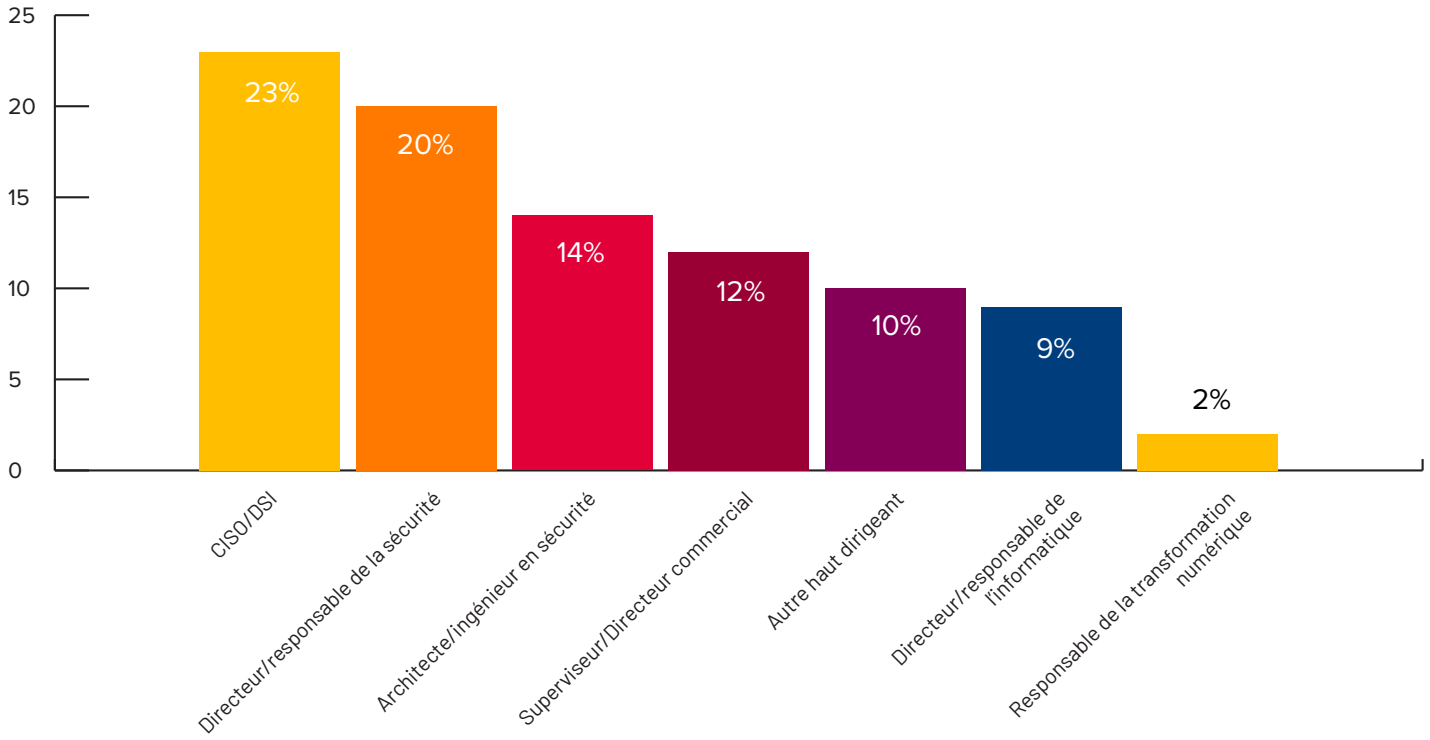
Votre entité a-t-elle un plan de cybersécurité adapté pour les demandes de subventions au titre de la loi américaine sur les infrastructures ?



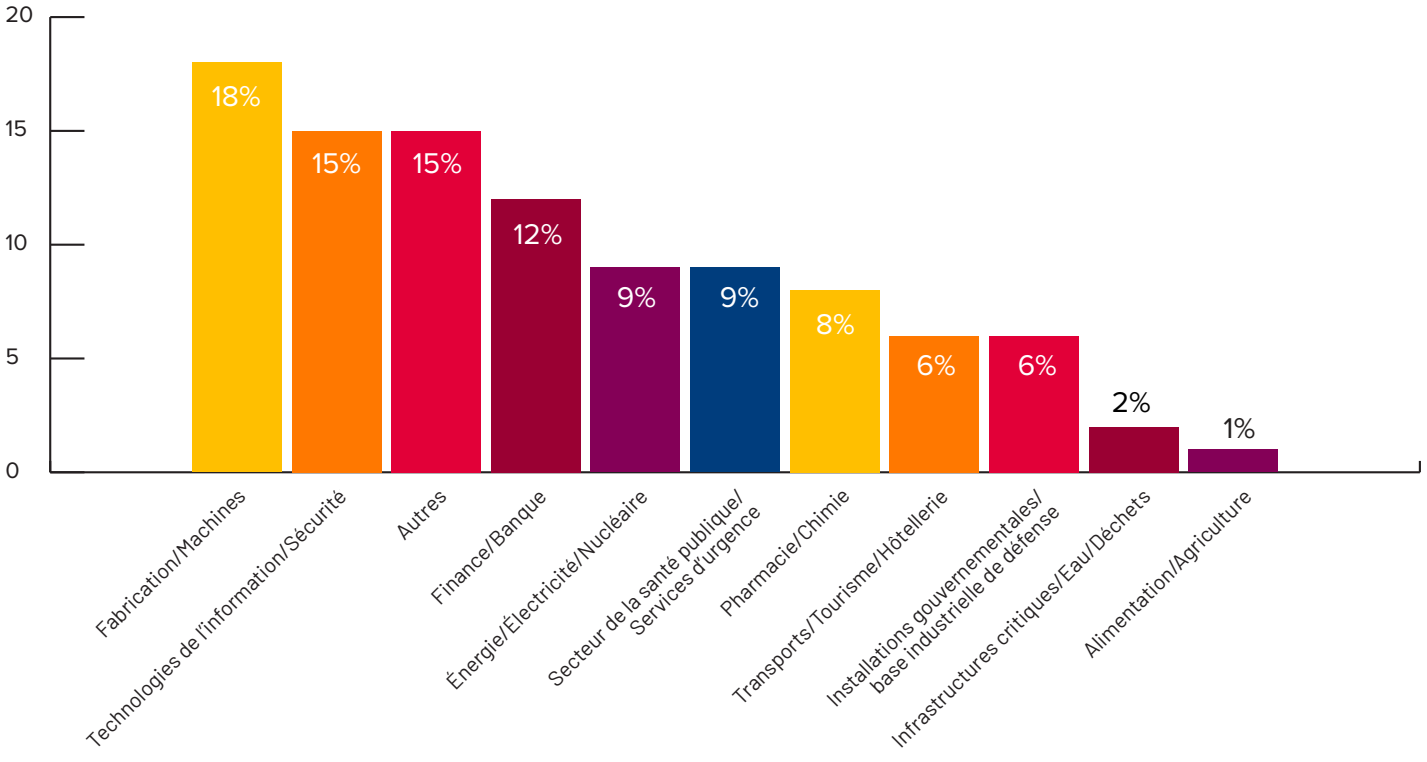
Participants à l'enquête par région



Participants à l'enquête par rôle



Participants à l'enquête par secteur d'activité



Suivez-nous.

rockwellautomation.com — expanding **human possibility**®

AMÉRIQUES : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 États-Unis, Tél. : +(1) 414.382.2000, Fax :+(1) 414.382.4444
EUROPE / MOYEN-ORIENT / AFRIQUE : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél. : +(32) 2 663 0600, Fax : +(32) 2 663 0640
ASIE PACIFIQUE : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél. : +(852) 2887 4788, Fax : +(852) 2508 1846
CANADA : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, Fax: +1 (450) 781-5101, www.rockwellautomation.ca
FRANCE : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00, Fax : +33 1 30 44 03 09
SUISSE : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Fax: 021 631 32 31, Customer Service Tél: 0848 000 278

Publication GMSN-SP016A-FR-P – Juin 2022