RAPPORT

État des lieux 2022 des technologies OT et de leur cybersécurité

TABLE DES MATIÈRES

Infographie : l'essentiel des résultats

Collaborateurs

33% des entreprises confient leur sécurité OT au VP/directeur de l'ingénierie/des opérations réseau

67% des responsables de la sécurité OT ont un profil d'ingénieur OT

43% des personnes interrogées considèrent le délai de réponse aux incidents de sécurité comme un des trois principaux indicateurs de performance

Posture de sécurité

56% des entreprises déclarent disposer d'une maturité de niveau 3 ou 4 en matière de sécurité OT

50% déclarent que la posture de sécurité OT est un facteur important pour définir le score de risque global

13% des entreprises disposent d'une visibilité centralisée sur leurs environnements OT

Pratiques de sécurité

48% signalent les incidents de sécurité à leur Direction générale

32% ont déployé un contrôle d'accès au réseau basé sur le rôle

52% déclarent que toutes les activités OT sont contrôlées et suivies par leur SOC

Résultats en matière de sécurité

93% des entreprises ont subi au moins une intrusion au cours de l'année écoulée, **78%** en ont subi plus que 3

61% des intrusions ont impacté les systèmes OT

90% des intrusions ont nécessité plusieurs heures pour restaurer les services

Bonnes pratiques

Les entreprises les mieux sécurisées sont plus susceptibles de

- Disposer d'une visibilité centralisée
- Être évaluées selon le critère du délai de réponse à une vulnérabilité
- Déployer un contrôle d'accès au réseau
- Signaler les incidents de sécurité
- Faire appel à un seul constructeur de dispositifs OT

Synthèse

L'état de lieux 2022 des technologies OT et de leur cybersécurité, qui en est cette année à sa quatrième édition annuelle, souligne que les entreprises progressent trop lentement vers une protection complète de leurs ressources et technologies industrielles (OT). Le rôle des systèmes OT a gagné en importance dans le bon fonctionnement de nombreuses entreprises. Celles-ci subissent des événements géopolitiques qui favorisent des attaques plus fréquentes. Les systèmes OT sont davantage connectés à Internet tandis que les menaces basées sur IP deviennent plus sophistiquées et perturbatrices. Ces différents facteurs font de la sécurité OT une préoccupation plus importante pour les entreprises.

Basé une enquête mondiale menée auprès de plus de 500 professionnels de la sécurité OT, le rapport de cette année révèle que si ce sujet capte l'attention des dirigeants d'entreprise, il continue à être de la responsabilité de collaborateurs d'un niveau plutôt bas d'un point de vue hiérarchique. Depuis des années, la sécurité des technologies OT est attendue être du ressort du DSSI/RSSI, mais rien n'indique que les choses évoluent dans ce sens. Et si la sécurité compte parmi les indicateurs de performance utilisés par la plupart des répondants à l'enquête, nombre d'entre eux sont davantage évalués sur des critères de productivité, ce qui pourrait les inciter à prendre quelques raccourcis en matière de sécurité.

Sur la base d'une enquête mondiale menée auprès de plus de 500 professionnels de la sécurité des technologies OT, le rapport de cette année révèle que si la sécurité OT retient l'attention des dirigeants d'entreprise, elle continue d'être du ressort de professionnels de rang hiérarchique relativement bas.

Les entreprises font de modestes progrès dans la maturité globale de leur posture de sécurité OT, avec seulement un peu plus de la moitié d'entre elles ayant atteint un niveau 3. Cependant, l'examen de certaines bonnes pratiques apporte des nuances à cette problématique. Seuls 13% des répondants disposent d'une visibilité centralisée sur toutes leurs activités OT, tandis que 52% sont en mesure de suivre toutes les activités OT à partir de leur centre opérationnel de sécurité (SOC). Seule la moitié des répondants affirme assurer le suivi et le reporting des indicateurs de sécurité de base, et moins de la moitié d'entre eux utilise une douzaine de technologies et de pratiques de sécurité. Ce dernier point souligne la diversité des façons dont les entreprises abordent la sécurité OT et reflète un marché qui continue à évoluer.

Sur l'année écoulée, les performances des entreprises en matière de sécurité se sont certes améliorées, mais trop timidement. 93% des entreprises ont subi une intrusion au cours des 12 derniers mois et 78% en ont subi plus de trois. Les conséquences sont lourdes : arrêt des opérations, pertes financières ou de données, image de marque ternie, voire une sécurité physique moindre. Il est clair que la plupart des entreprises ont du pain sur la planche. Heureusement, une minorité des répondants a su déjouer les intrusions au cours de l'année écoulée, sans doute en capitalisant sur des pratiques efficaces décrites dans ce rapport.

Introduction

Bien que les technologies industrielles OT soient moins visibles que leurs homologues IT dans la plupart des entreprises, et certainement peu connues du grand public, elles n'en sont pas moins importantes pour l'économie et la vie quotidienne des gens. Après tout, les systèmes OT contrôlent des infrastructures critiques dont nous dépendons tous : réseaux électriques, systèmes d'eau et d'égouts, pipelines de carburant, centrales électriques ou encore réseaux de transport. L'OT est également essentiel à la fabrication de tous les types de biens.

L'OT est une composante importante de la transformation digitale des entreprises industrielles. L'évolution rapide des conditions du marché a imposé l'adoption des méthodologies et technologies de type Industrie 4.0. La pandémie de Covid-19 a accéléré ces tendances, laissant les « démunis » en matière de technologie se démener pour actualiser et simplifier leurs opérations.[1]

Des menaces croissantes sur la sécurité

Cette tendance n'a pas échappé aux cybercriminels. L'année dernière, le rapport de sécurité Global Threat Landscape Report de FortiGuard Labs pointait une recrudescence majeure des menaces détectées par les systèmes de prévention des intrusions (IPS) pour les systèmes OT.[2] Cette observation a coïncidé avec plusieurs événements de sécurité très médiatisés au sein d'environnements OT, notamment les attaques par ransomware contre Colonial Pipeline et JBS qui ont perturbé, respectivement, l'approvisionnement en essence et la distribution de viande en Amérique du Nord, en mai et juin derniers.[3]

Les cyberattaques sur les systèmes OT ont progressé au cours de la dernière décennie, ces systèmes étant devenus plus vulnérables aux attaques provenant de l'extérieur. Alors que l'OT était traditionnellement isolé de l'IT, ces deux infrastructures sont aujourd'hui bien plus intégrées. Les systèmes OT sont connectés à l'Internet et théoriquement accessibles de partout. En soi, ceci représente une extension significative de la surface d'attaque pour les industriels et la prolifération des objets connectés industriels (IIoT) étend encore plus cette surface d'attaque. Dans le même temps, les systèmes OT connectés sont vulnérables à des menaces IT de plus en plus sophistiquées.

L'invasion de l'Ukraine par la Russie et les conséquences qui en découlent apportent une nouvelle perspective sur la sécurité OT. En avril 2022, l'agence américaine de cybersécurité et de sécurité des infrastructures (CISA), ainsi que ses homologues en Australie, au Canada, en Nouvelle-Zélande et au Royaume-Uni, ont averti que des acteurs affiliés à la Russie intensifiaient leurs efforts en réponse aux sanctions imposées par l'Occident. Les agences ont ainsi exhorté les responsables des réseaux d'infrastructures critiques à se préparer à des cybermenaces potentielles et à en maîtriser les effets - y compris les logiciels malveillants destructeurs, les rançongiciels, les attaques par déni de service et le cyberespionnage - en renforçant leurs cyberdéfenses et en s'investissant pour identifier les indicateurs d'activités malveillantes.[4]

En effet, les attaques attribuées à la Russie ont progressé et nombre d'entreprises ukrainiennes en ont fait les frais.[5] Mais le reste du monde est loin d'être à l'abri, puisque sept organisations d'intérêt vital sur dix au Royaume-Uni ont signalé une augmentation des cyberattaques depuis le début de la guerre.[6]

La sécurité OT sous les projecteurs

En conséquence, les entreprises de nombreux secteurs se démènent pour protéger des systèmes OT de plus en plus vulnérables. Une étude réalisée pour Fortinet par Westlands Advisory[7] révèle que les investissements en technologies de sécurité IT/OT et spécifiques à l'OT ont atteint 6,9 milliards de dollars sur l'année 2022. Et ces investissements progressent plus rapidement que ceux alloués exclusivement à l'IT, avec un taux de croissance annuel moyen estimé à 21% pour la sécurité OT et à 16% pour la cybersécurité OT/IT d'ici 2027.

Si la progression des investissements est un très bon signe, ce rapport constate que, dans l'ensemble, les entreprises ayant participé à l'enquête de cette année ont encore beaucoup de chemin à parcourir pour protéger leurs systèmes OT de manière pertinente. Cependant, un petit sous-ensemble de répondants a traversé les 12 derniers mois sans subir d'intrusion, et ce rapport tente de mettre en lumière certaines des bonnes pratiques mises en œuvre par ces entreprises.

Méthodologie de l'étude

Le rapport de cette année sur l'état des lieux des technologies OT et de leur cybersécurité est basé sur une enquête menée auprès de plus de 500 professionnels de l'OT entre le 14 et le 18 mars 2022. Les questions de l'enquête sont proches des celles posées lors des enquêtes similaires en 2019, 2020 et 2021, décrites dans les versions précédentes de ce rapport. Les personnes interrogées ont répondu à 40 questions sur leur environnement OT, leur infrastructure de sécurité, les meilleures pratiques de sécurité et le processus de sélection des fournisseurs technologiques.

Diversité des zones géographiques, des fonctions professionnelles, des secteurs d'activité et des dispositifs

Le panel de l'enquête de cette année est différent de celui des années précédentes : le périmètre est mondial plutôt que centré sur l'Amérique du Nord (schéma 1). Dans l'ensemble, 28 pays sont représentés, avec 150 répondants en Amérique du Nord (NA), 70 en Amérique latine (LATAM), 130 en Europe, Moyen-Orient et Afrique (EMEA) et 170 en Asie-Pacifique (APAC).

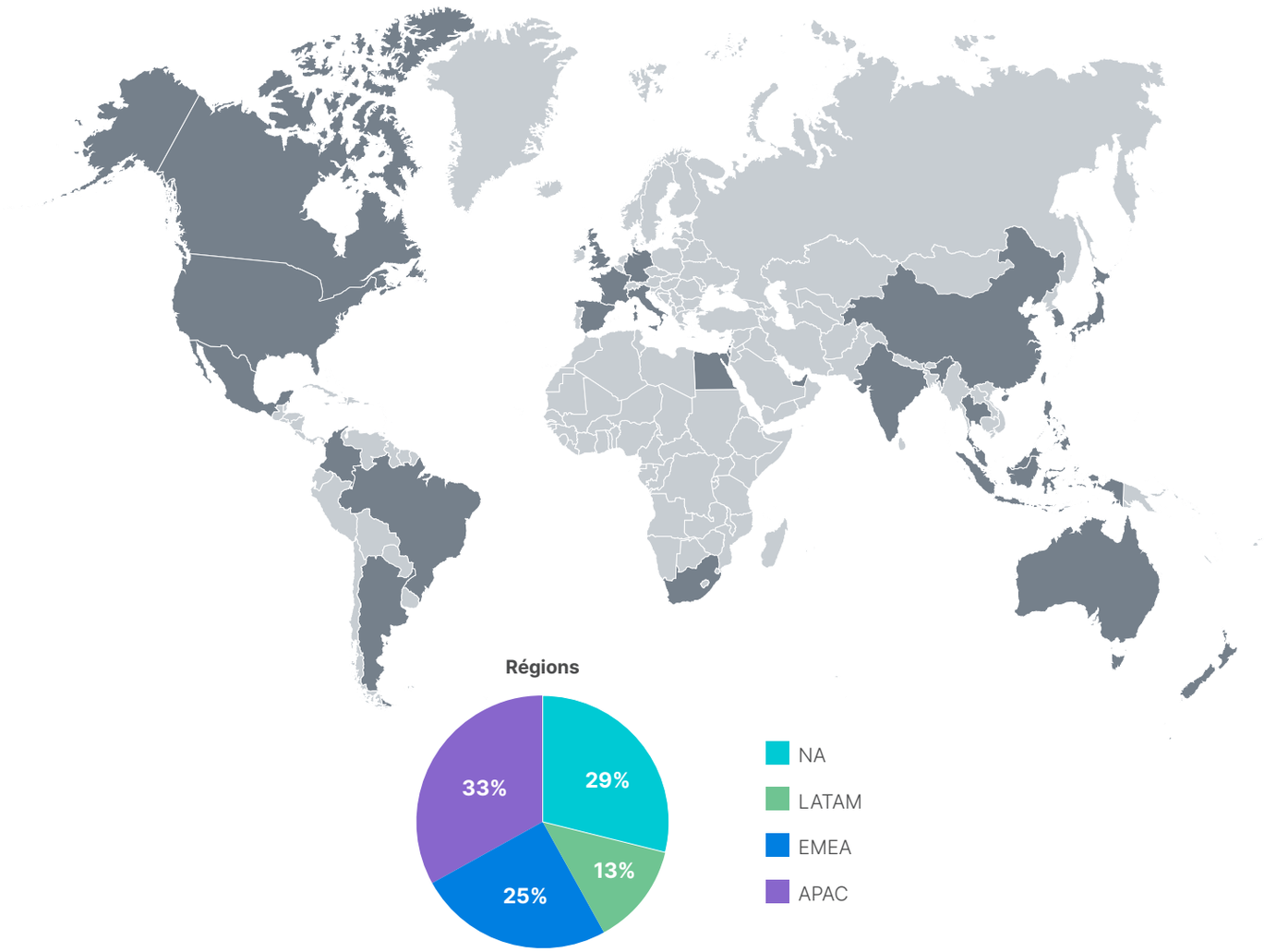


Schéma 1 : pays et régions représentés dans l'enquête.

L'enquête a ciblé des profils occupant des postes à responsabilité et en charge de l'OT et de la sécurité OT, de manager à cadre dirigeant (schéma 2). Ces personnes sont issues d'un large éventail de secteurs d'activité qui utilisent les technologies OT de manière importante : production industrielle, transports et logistique, soins de santé... Six personnes interrogées sur dix sont des décideurs finaux en matière d'achats OT, et 85% disent être régulièrement consultées sur les investissements en cybersécurité (schéma 3).

Les personnes interrogées sont des utilisateurs de systèmes de contrôle industriel (ICS) et de systèmes de contrôle et d'acquisition de données (SCADA) conçus par 15 fournisseurs différents (schéma 4). Comme les années précédentes, Honeywell et Siemens restent les marques les plus utilisées par les répondants, avec davantage d'utilisateurs de Honeywell et Schneider que les années précédentes. L'utilisation de Siemens et de Yokogawa a considérablement diminué au cours de la même période. Certains de ces changements reflètent le périmètre géographique plus large de l'enquête de cette année.

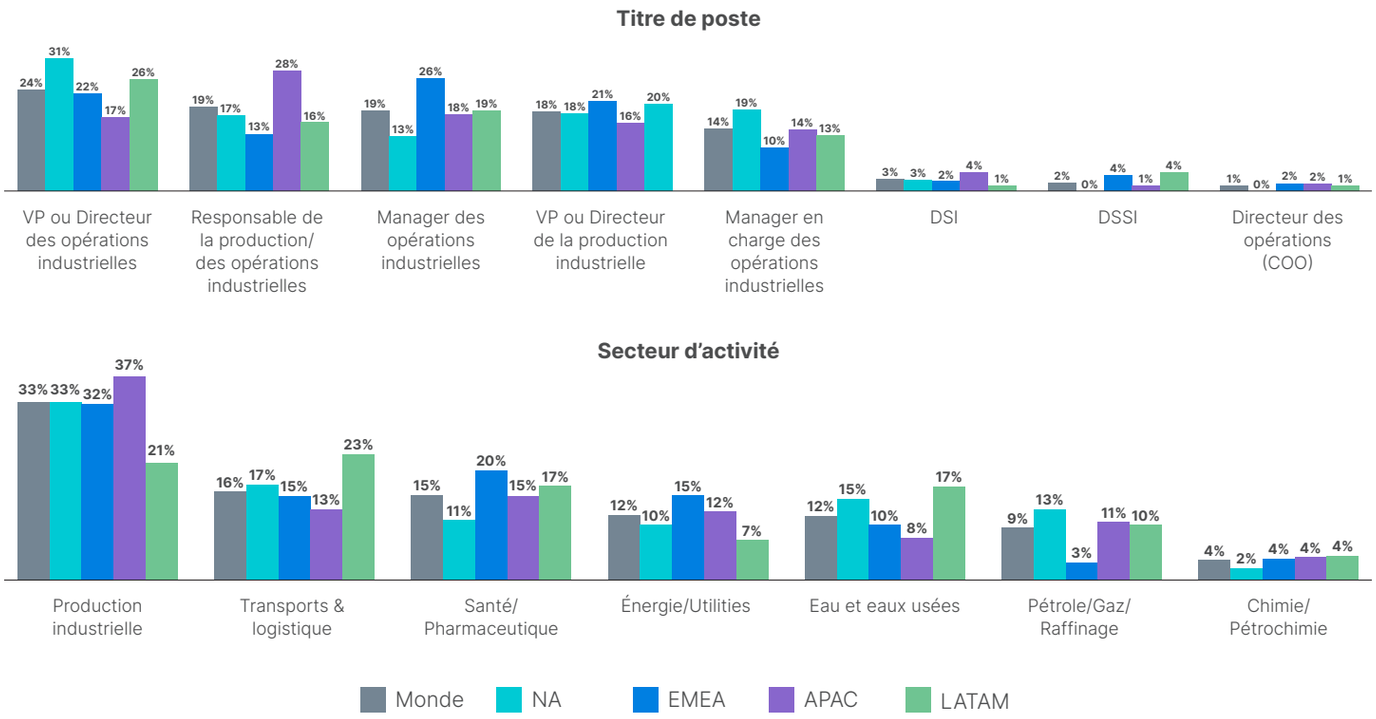


Schéma 2 : Titres de poste et secteurs d'activité par région.

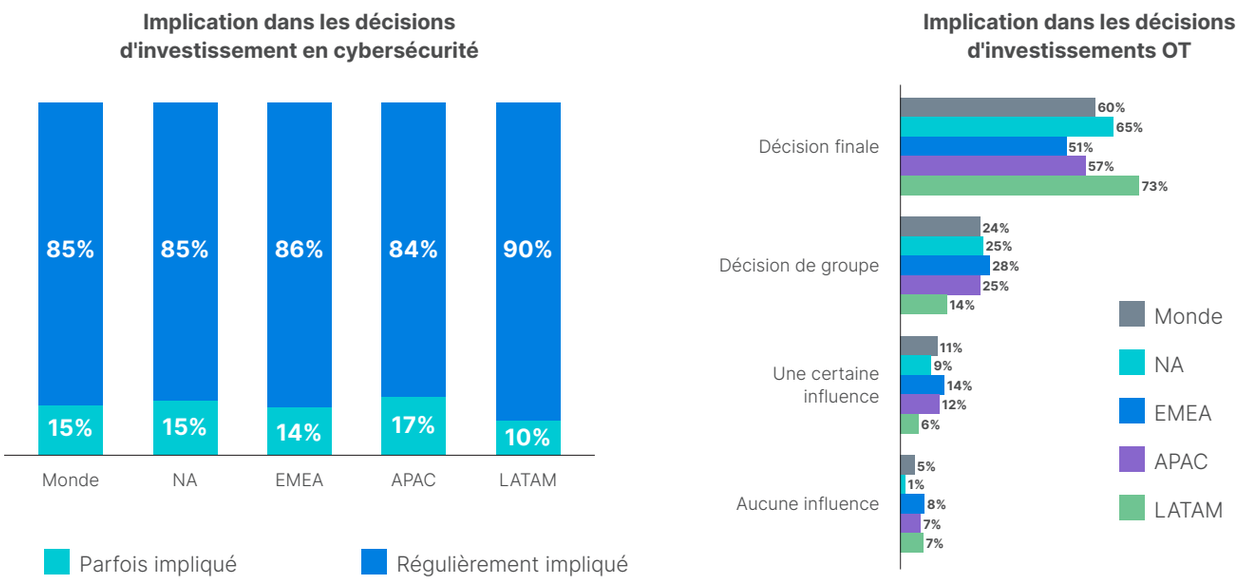


Schéma 3 : rôle des répondants en matière d'investissement en cybersécurité et OT.

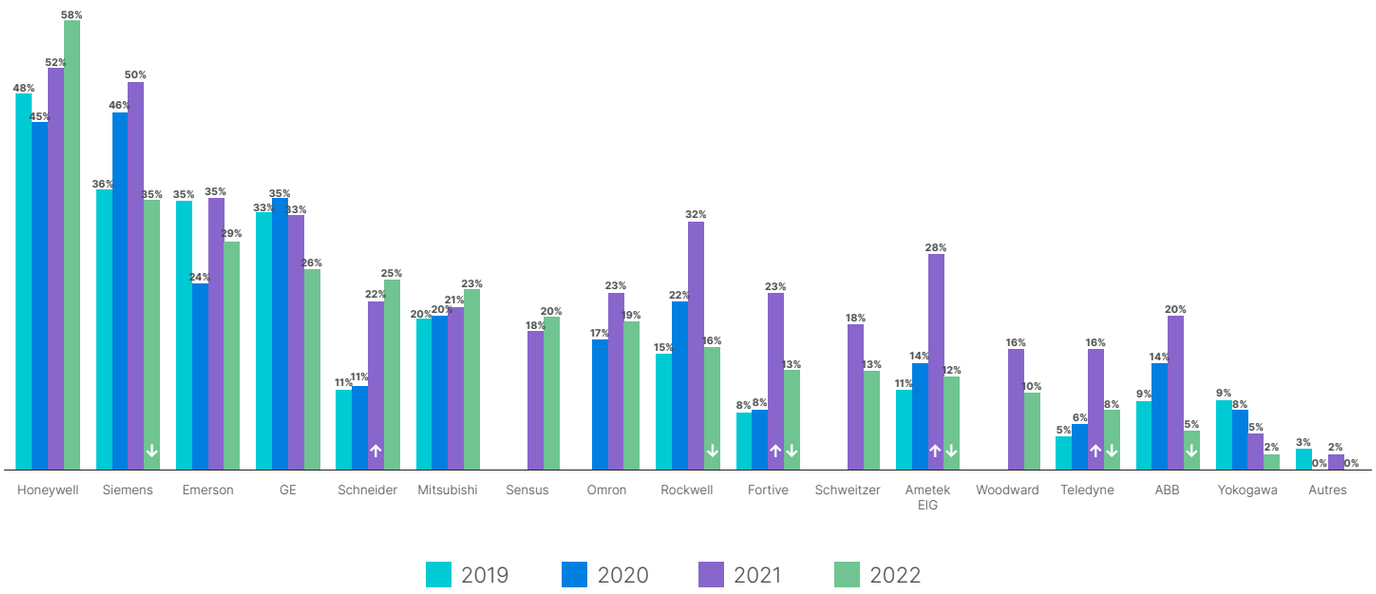


Schéma 4 : constructeurs des dispositifs OT existants.

Perspectives et bonnes pratiques

Ce rapport dresse un état des lieux pour l'ensemble du panel, mais également par région géographique ou secteur d'activité. D'autre part, nous comparons les résultats de l'enquête de cette année sur la zone nord-américaine avec ceux des enquêtes menées en Amérique du Nord en 2019, 2020 et 2021. À partir de cette analyse, nous avons dressé cinq constats clés sur l'état de la cybersécurité OT aujourd'hui.

Dans la dernière section de ce rapport, nous analysons les réponses à l'enquête en fonction des résultats concrets en matière de cybersécurité. Sont ainsi comparées les entreprises n'ayant subi aucune intrusion au cours de l'année écoulée à celles qui en ont subi plus de 10. Cette comparaison permet d'identifier plusieurs bonnes pratiques que les entreprises les mieux sécurisées auront davantage tendance à appliquer.

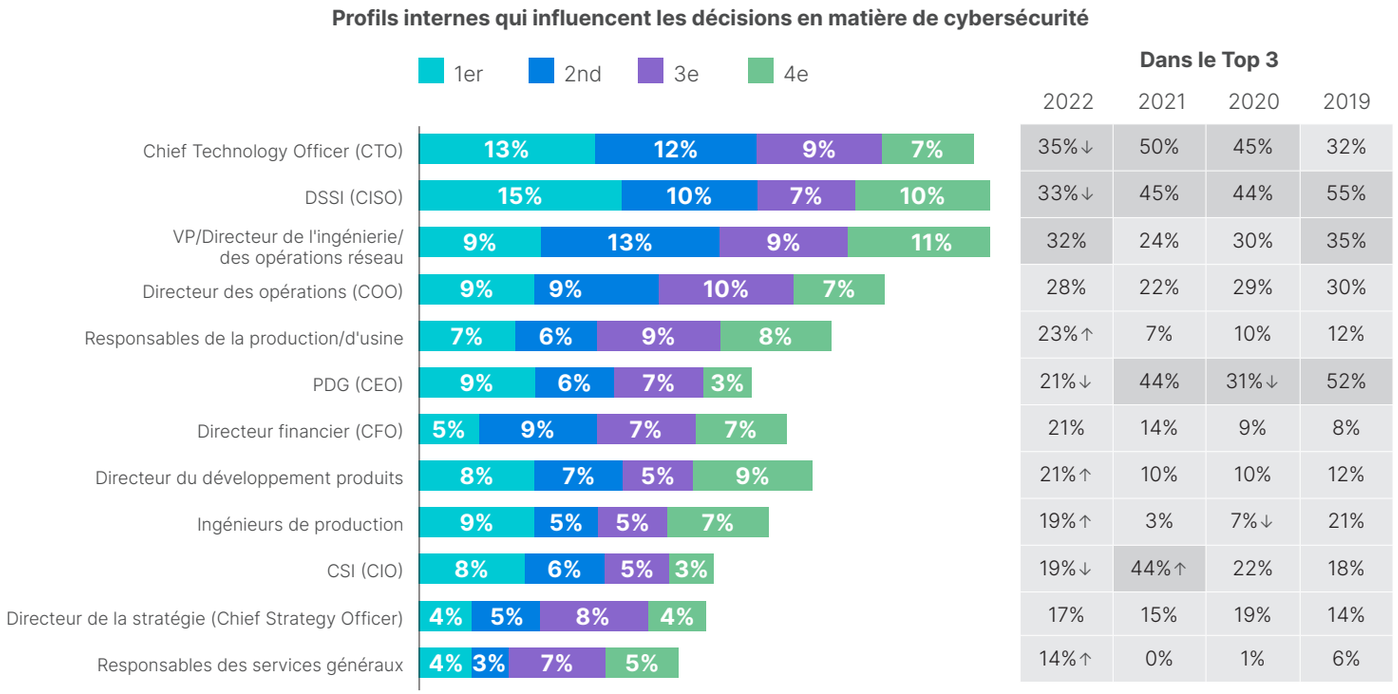
« Les récentes cyber-opérations sponsorisées par l'état russe ont donné lieu à des attaques par déni de service (DDoS). Les opérations plus anciennes ont porté sur le déploiement de logiciels malveillants destructeurs contre des administrations ukrainiennes et des infrastructures critiques du pays. »[8]

Perspectives sur la sécurité OT

Les résultats de l'enquête révèlent que les entreprises se préoccupent de plus en plus de la sécurité de leur infrastructure OT, mais qu'elles ne sont que partiellement préparées aux menaces. Voici cinq constats clés qui ressortent de notre étude :

Constat 1 : la sécurité OT est une priorité d'entreprise dont la responsabilité relève de différents groupes

Il n'est pas surprenant que la sécurité des systèmes OT retienne l'attention des dirigeants de nombreuses organisations, le CTO et le CISO/CSO (DSSI/RSSI) étant les plus souvent cités parmi les trois principales fonctions dirigeantes influençant les décisions en matière de cybersécurité. Toutefois, les réponses à l'enquête indiquent que ces dirigeants ont perdu de leur influence au cours de l'année écoulée (schéma 5). L'année dernière, 50% des entreprises comptaient le CTO parmi les trois principaux influenceurs en matière de sécurité, et 45% en faisaient de même pour le CISO/CSO. Ces chiffres dévissent à 35% et 33%, respectivement en 2022. La nature mondiale de l'enquête n'explique pas ces évolutions, car les chiffres sont identiques pour les répondants nord-américains et pour le panel global.



	Dans le Top 3			
	2022	2021	2020	2019
Chief Technology Officer (CTO)	35%↓	50%	45%	32%
DSSI (CISO)	33%↓	45%	44%	55%
VP/Directeur de l'ingénierie/ des opérations réseau	32%	24%	30%	35%
Directeur des opérations (COO)	28%	22%	29%	30%
Responsables de la production/d'usine	23%↑	7%	10%	12%
PDG (CEO)	21%↓	44%	31%↓	52%
Directeur financier (CFO)	21%	14%	9%	8%
Directeur du développement produits	21%↑	10%	10%	12%
Ingénieurs de production	19%↑	3%	7%↓	21%
CSI (CIO)	19%↓	44%↑	22%	18%
Directeur de la stratégie (Chief Strategy Officer)	17%	15%	19%	14%
Responsables des services généraux	14%↑	0%	1%	6%

Schéma 5 : profils internes influençant les décisions en matière de sécurité.

Qui pilote la sécurité OT ?

Lorsqu'on interroge le panel sur qui est responsable en dernier ressort de la sécurité OT au sein de leur entreprise, un tiers des répondants cite le vice-président ou directeur de l'ingénierie ou des opérations réseau (schéma 6). Ce chiffre, en progrès sensible sur un an, se veut le plus élevé depuis quatre ans que l'enquête est menée. Ainsi, la responsabilité de la sécurité des technologies OT se serait déplacée un peu vers le haut de l'organigramme par rapport aux années précédentes, lorsqu'une personne de hiérarchie moindre (directeur ou manager) était responsable de la sécurité des technologies OT au sein de nombre d'entreprises.

Les répondants pensent que ce mouvement ascendant dans l'organigramme va se poursuivre. Si seuls 15% des répondants affirment que le DSSI (CISO) est responsable de la sécurité OT aujourd'hui, 79% déclarent s'attendre à ce que cette fonction soit rattachée au DSSI au cours des 12 prochains mois (schéma 7). Cependant, on peut être sceptique quant à cette affirmation : une majorité des répondants a fait cette même prédiction pour chacune des années de l'enquête, et le pourcentage d'organisations où le DSSI est actuellement en charge de la sécurité OT a en fait légèrement diminué en 2022 par rapport à 2021. L'influence moindre du DSSI sur les décisions de sécurité, mentionnée ci-dessus, ajoute du poids à ce scepticisme.

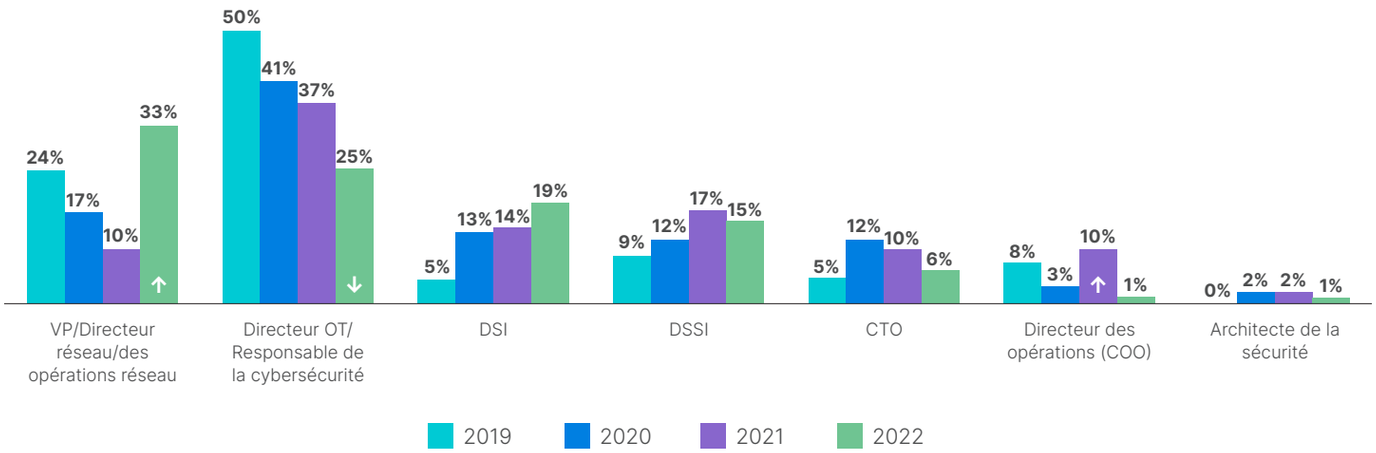


Schéma 6 : responsable actuel de la cybersécurité OT.

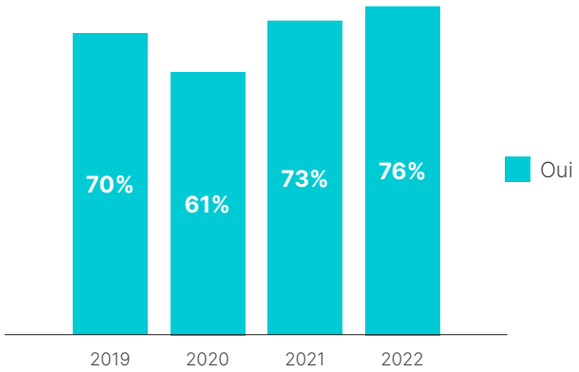


Schéma 7 : les répondants qui s'attendent à ce que la sécurité OT soit placée sous la responsabilité du DSSI dans les 12 prochains mois.

Parcours professionnels dans la sécurité OT

Pour participer à l'enquête, les répondants devaient avoir une responsabilité importante en matière d'OT. 85% d'entre eux consacrent plus de la moitié de leur temps à cette discipline tandis de 28% y consacrent plus des trois quarts de leur temps de travail (schéma 8). Deux tiers des personnes interrogées dans le monde ont une expérience professionnelle dans l'OT, soit au sein d'une entreprise industrielle, soit chez un fournisseur de solutions technologiques industrielles OT (schéma 9). Le tiers restant est issu de la sécurité IT (plus de la moitié du panel en Amérique latine).

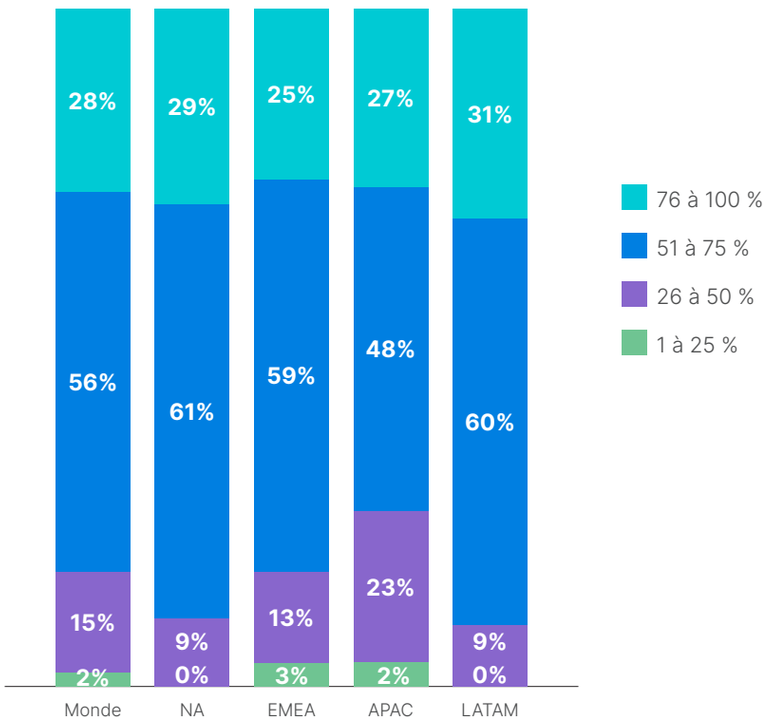


Schéma 8 : pourcentage du temps consacré au support et la gestion de la sécurité OT.

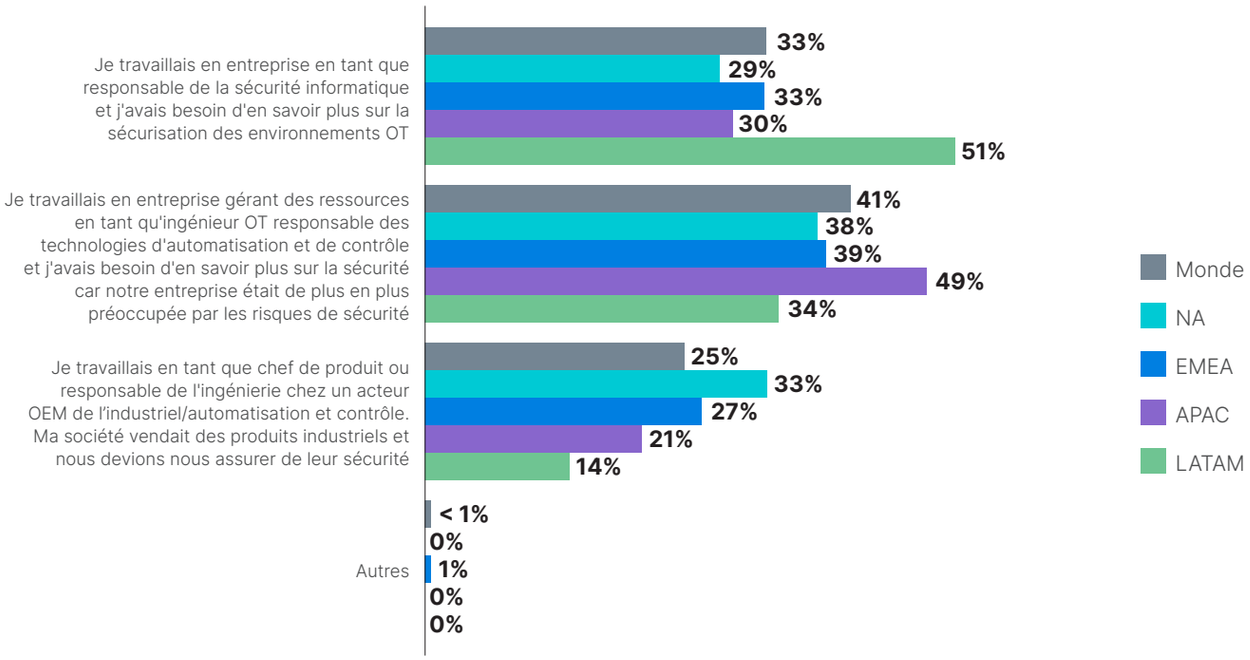
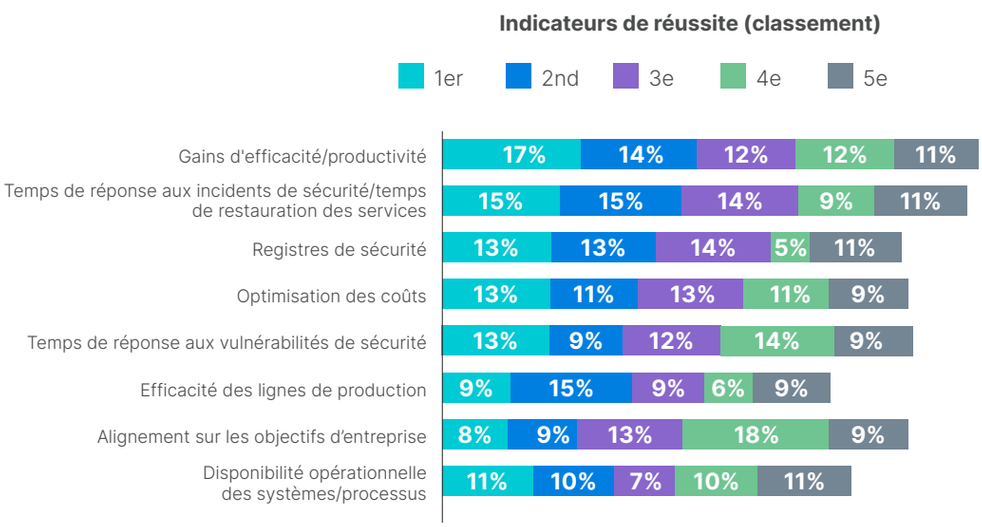


Schéma 9 : parcours professionnel ayant conduit à la sécurité OT.

Constat 2 : certaines entreprises ont encore tendance à privilégier la productivité par rapport à la sécurité OT

Alors que toutes les entreprises déclarent être préoccupées par la sécurité OT, une façon de mesurer l'importance de la sécurité consiste à regarder comment les acteurs majeurs de l'OT sont évalués. Dans l'enquête de cette année, les gains d'efficacité et de productivité restent le plus souvent cités comme le premier indicateur de performance, et ils figurent parmi les trois premiers indicateurs pour 43% des entreprises (schéma 10). Lors de chaque enquête annuelle, ce critère reste le plus souvent cité dans le Top 3 des indicateurs de réussite. Cependant, sa prévalence fléchit de 14% entre 2021 et 2022.

Le CISO est l'un des principaux influenceurs des décisions en matière de sécurité OT dans seulement 33% des entreprises, contre 45% en 2021.



	Dans le Top 3			
	2022	2021	2020	2019
Gains d'efficacité/productivité	43↓	57%	46%	55%
Temps de réponse aux incidents de sécurité/temps de restauration des services	43%	N.A.	N.A.	N.A.
Registres de sécurité	40%	34%	44%	41%
Optimisation des coûts	37%	41%	40%	53%
Temps de réponse aux vulnérabilités de sécurité	34%↓	47%↑	32%	44%
Efficacité des lignes de production	32%	42%	41%↓	42%
Alignement sur les objectifs d'entreprise	29%	33%	24%	29%
Disponibilité opérationnelle des systèmes/processus	29%↓	41%	40%	35%

Schéma 10 : classement des indicateurs de réussite.

Notons qu'un indicateur de sécurité (temps de réponse aux incidents ou de restauration post-incident) a également été cité par 43% du panel comme comptant parmi les trois principaux indicateurs, ce qui constitue une bonne nouvelle. Le temps de réponse aux vulnérabilités de sécurité et le taux de disponibilité des systèmes/processus connaissent un déclin important, ce qui s'expliquerait par le fait que l'indicateur de réponse aux incidents est nouveau lors de l'enquête 2022, ce qui entraînerait une baisse des autres indicateurs de sécurité.

Préoccupation vis-à-vis des ransomwares

Depuis plusieurs années, les ransomwares font la une des médias dans le domaine de la cybersécurité et les entreprises se disent très préoccupées par cette menace, même si elle est moins courante que d'autres types d'attaques. Plus des deux tiers des personnes interrogées dans le monde - et les trois quarts en Amérique du Nord - déclarent être plus préoccupés par les ransomwares que par d'autres intrusions (schéma 11). Les ransomwares ont causé des dommages et des coûts économiques considérables au fil des ans, et leur prévalence visible a eu pour effet de susciter l'inquiétude des entreprises. Cependant, d'autres types d'attaques dommageables peuvent ne pas recevoir l'attention qu'elles méritent en raison de leur moindre visibilité.

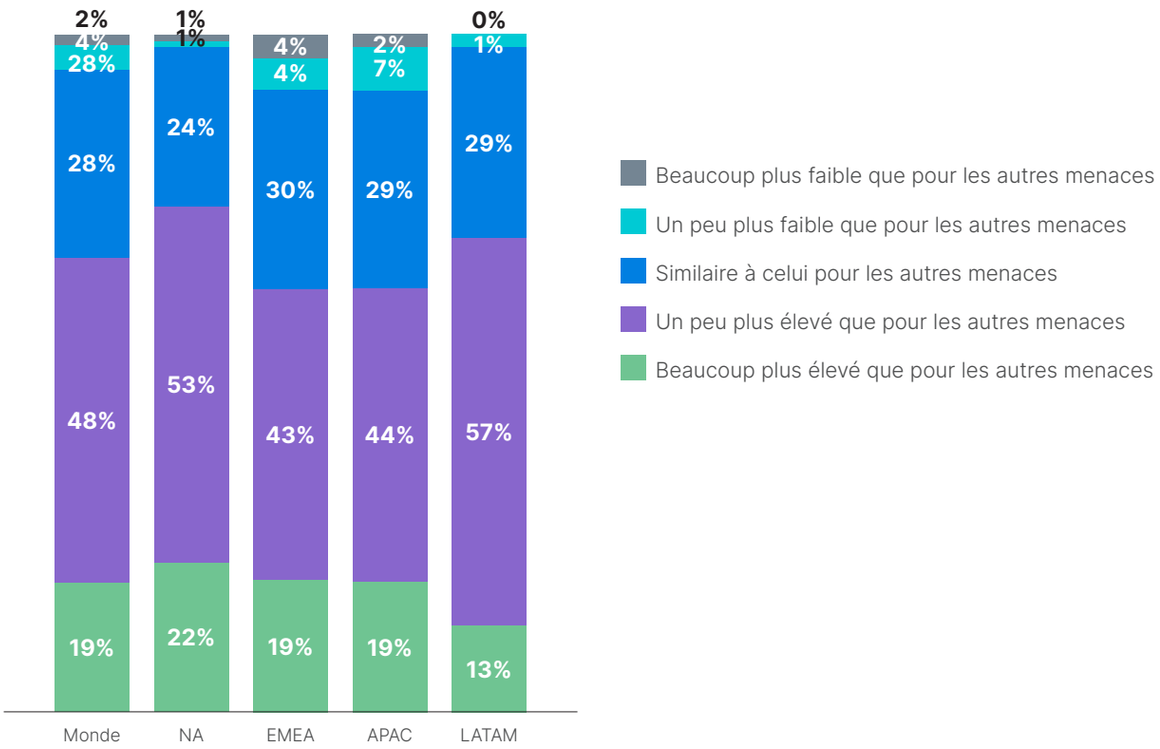
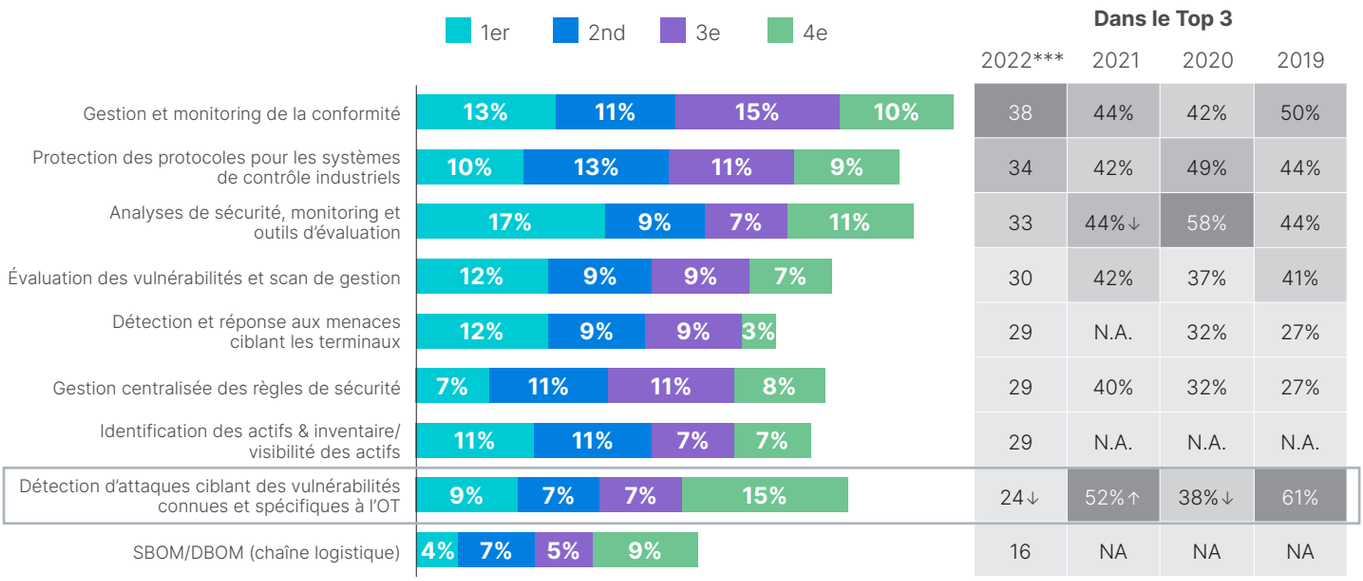


Schéma 11 : niveau de préoccupation face aux ransomwares.

Hiérarchie des outils de cybersécurité par ordre d'importance

Les personnes interrogées étaient très partagées quant aux fonctionnalités des solutions de cybersécurité les plus importantes pour leur entreprise. Les outils d'analyse, de surveillance et d'évaluation de la sécurité ont été le plus souvent cités comme étant les plus importants, mais seulement par 17% des répondants (schéma 12). Dans l'ensemble, les solutions de gestion et de surveillance de la conformité ont été le plus souvent citées dans le trio de tête, tandis que les fonctions de protection des protocoles OT se sont classées en deuxième position.

Fonctionnalités les plus importantes des solutions de cybersécurité (classement)



	Dans le Top 3			
	2022***	2021	2020	2019
Gestion et monitoring de la conformité	38	44%	42%	50%
Protection des protocoles pour les systèmes de contrôle industriels	34	42%	49%	44%
Analyses de sécurité, monitoring et outils d'évaluation	33	44%↓	58%	44%
Évaluation des vulnérabilités et scan de gestion	30	42%	37%	41%
Détection et réponse aux menaces ciblant les terminaux	29	N.A.	32%	27%
Gestion centralisée des règles de sécurité	29	40%	32%	27%
Identification des actifs & inventaire/ visibilité des actifs	29	N.A.	N.A.	N.A.
Détection d'attaques ciblant des vulnérabilités connues et spécifiques à l'OT	24↓	52%↑	38%↓	61%
SBOM/DBOM (chaîne logistique)	16	NA	NA	NA

Schéma 12 : classement des fonctions les plus importantes pour les solutions de cybersécurité.

Constat 3 : les entreprises font état d'un renforcement progressif de leur posture de sécurité OT, mais cette amélioration reste limitée

Comme pour les années précédentes, notre enquête demandait aux répondants d'indiquer eux-mêmes le niveau de maturité de la sécurité OT de leur entreprise. Une brève description de chaque niveau de maturité était proposée. 84% des répondants ont atteint au moins le niveau 2, avec mise en œuvre des accès contrôlés et d'un profiling (schéma 13). La moitié du panel a atteint au moins le niveau 3 (comportement prédictif), et 21% ont atteint le niveau 4 (orchestration et automatisation de la sécurité).

L'amélioration est marginale par rapport à 2021 et résulte essentiellement des entreprises qui ont progressé du niveau 2 au niveau 3. La part des entreprises ayant au moins atteint le niveau 3 est passée de 44% à 50% en un an.

Pour 43% des entreprises, le temps de réponse aux incidents de sécurité/ restauration des services est l'un des trois principaux indicateurs de réussite pour le télétravail.

Les résultats par zone géographique indiquent que les entreprises ayant atteint le niveau 4 sont plus nombreuses en Amérique latine et en APAC. En Amérique du Nord, les entreprises sont plus nombreuses à avoir dépassé le niveau 1, mais moins nombreuses à avoir atteint le niveau 4, ce qui laisse plus de 70% des entreprises positionnées sur des niveaux intermédiaires.

Malheureusement, seule la moitié des répondants déclare que la posture de sécurité OT de leur entreprise joue un rôle important dans son score de risque global (schéma 14). Pour la quasi-totalité des autres entreprises, ce facteur est estimé comme étant d'importance modérée.

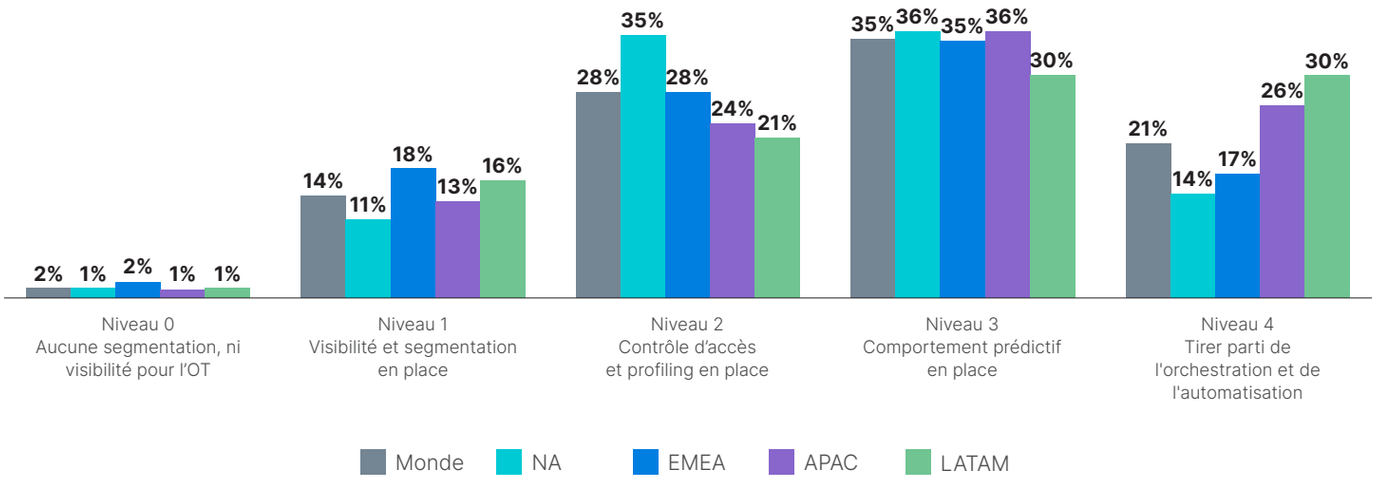


Schéma 13 : niveau de maturité de la posture de cybersécurité OT.

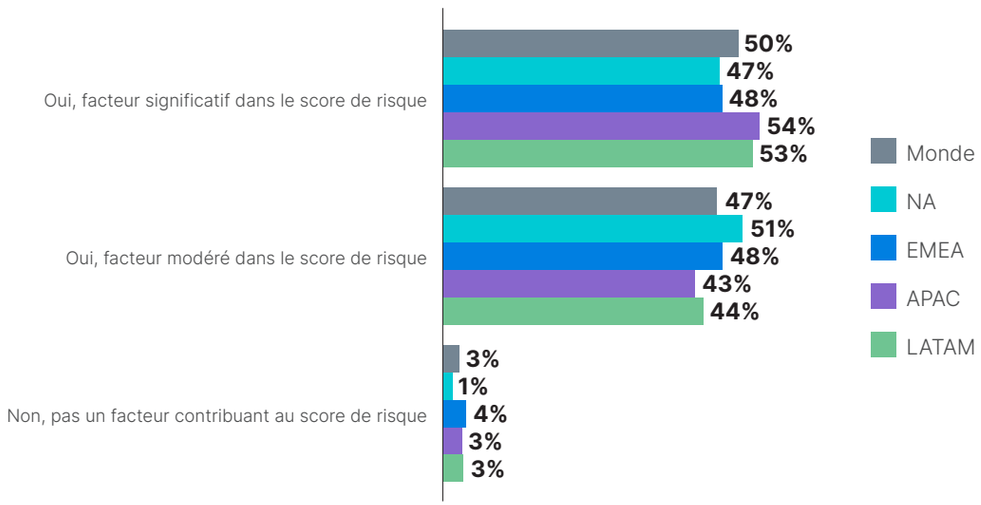


Schéma 14 : importance de la posture de sécurité OT dans le score de risque global.

Maturité globale de la cybersécurité

Les répondants ont également été invités à évaluer la maturité de leur programme global de cybersécurité IT et OT. Selon les réponses, les répondants étaient plus susceptibles d'avoir atteint le niveau 3 (59%) mais moins susceptibles d'avoir atteint le niveau 4 (16%, schéma 15). De nouveau, les entreprises d'Amérique latine et APAC affichent une plus grande maturité, tandis que celles d'Amérique du Nord sont globalement en retard. Les grandes entreprises et celles évoluant dans la production industrielle sont plus susceptibles de présenter une maturité plus élevée, tout comme les entreprises dans lesquelles les principaux responsables technologiques et de la sécurité ont une influence sur les décisions de cybersécurité (schéma 16).

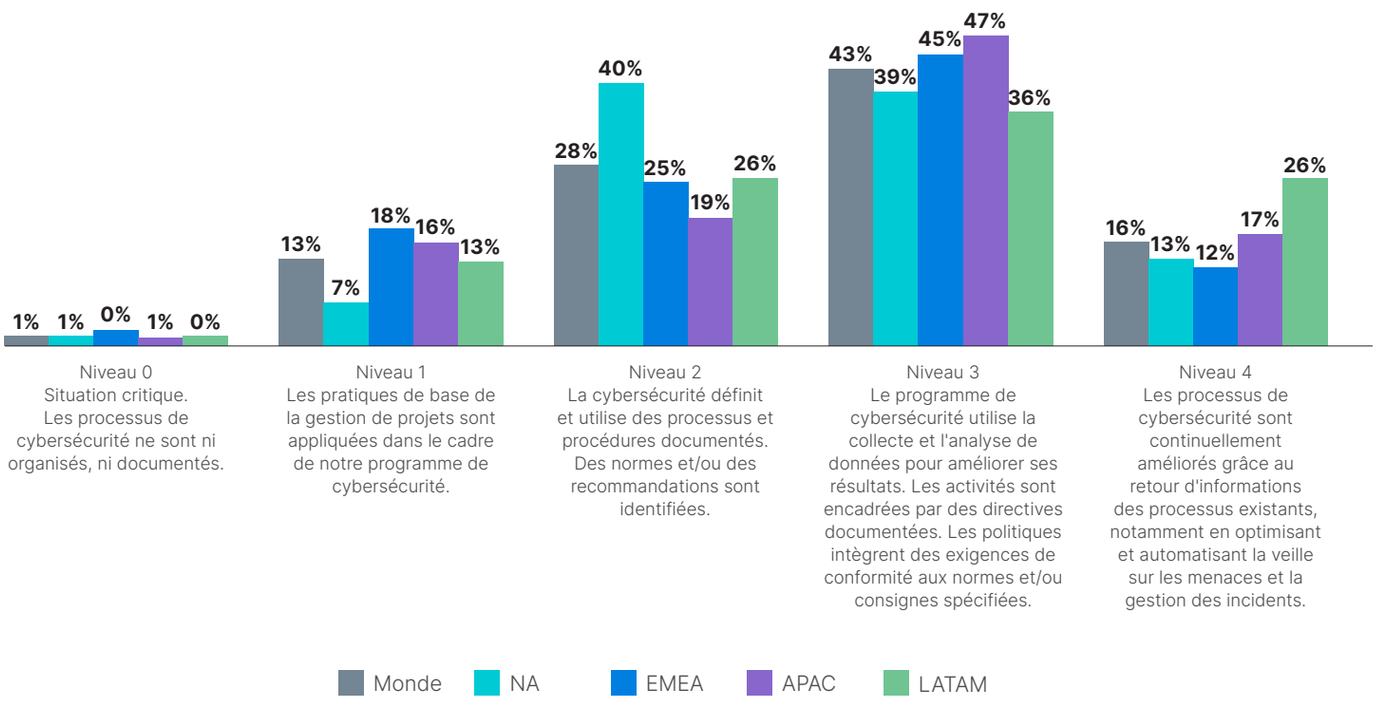
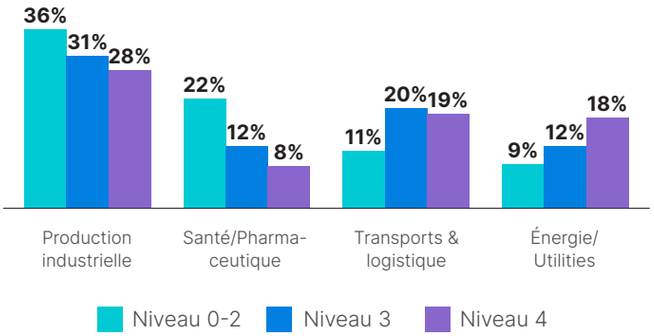
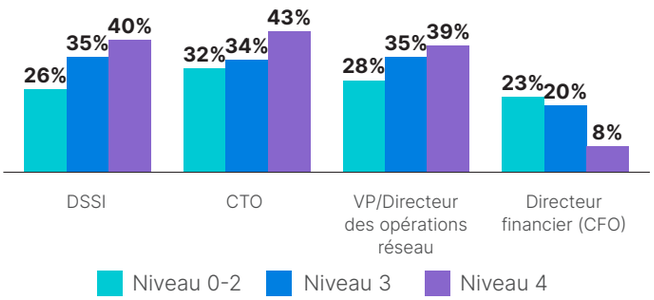


Schéma 15 : niveau de maturité du programme de cybersécurité global.





% Plus de 5 000 collaborateurs		
21%	28%	41%

% la cybersécurité contribue à / freine le succès		
65%-4%	82%-6%	83%-11%
% aide en facilitant l'application de normes de sécurité		
40%	46%	58%

Schéma 16 : données démographiques du panel par niveau de maturité du programme de cybersécurité.

Visibilité centralisée

La visibilité sur les processus OT fait partie du niveau 1 de notre matrice de maturité de la sécurité OT. Cependant, la précision de cette visibilité peut faire la différence. Alors que 98% des personnes interrogées revendiquent au moins une maturité de niveau 1, seuls 74% d'entre elles déclarent que les équipes opérationnelles de sécurité ont une visibilité sur leurs activités OT (schéma 17). Ce chiffre est de 77% en Amérique du Nord, en amélioration par rapport aux années précédentes (schéma 18). Cependant, le pourcentage de répondants nord-américains bénéficiant d'une visibilité intégrale (100%) semble reculer, de 23% en 2020 à 13% en 2022.

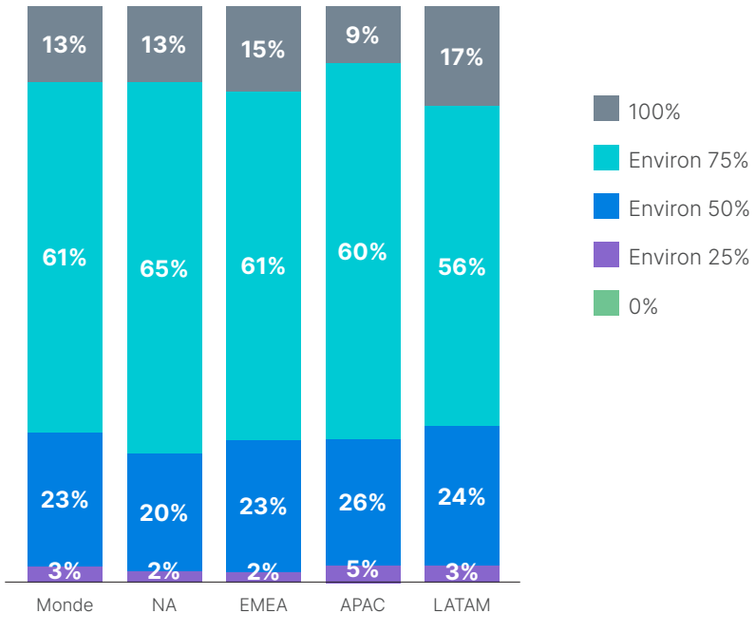


Schéma 17 : Visibilité des équipes de sécurité sur l'OT.

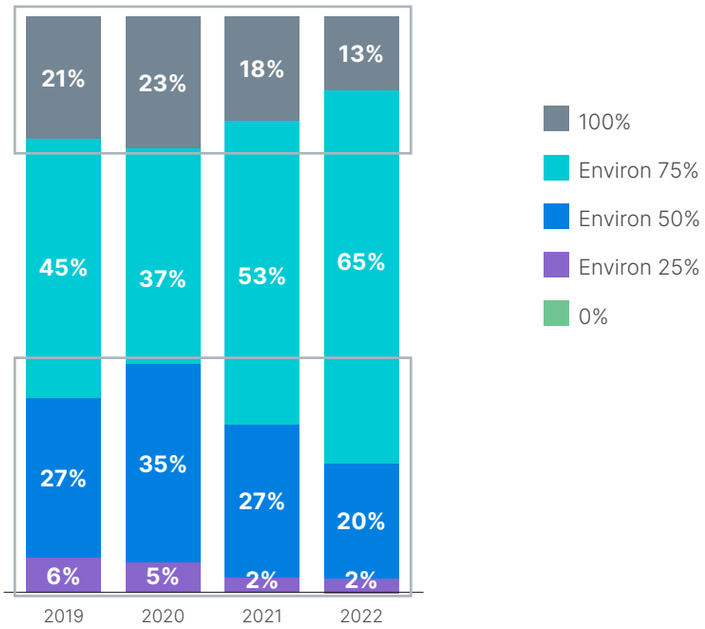


Schéma 18 : isibilité des équipes de sécurité sur l'OT, Amérique du Nord.

Constat 4 : les entreprises traitent la sécurité OT de différentes façons et subissent des carences en sécurité

Les systèmes OT ayant été historiquement déconnectés d'Internet, le besoin de sécuriser ces systèmes contre les menaces IT est relativement nouveau. Notre enquête révèle que les pratiques de sécurité n'ont pas encore été normalisées.

Comme nous l'avons évoqué, une approche consiste à confier la gestion de la sécurité OT au SOC, ce centre opérationnel de sécurité qui assure déjà cette fonction pour les systèmes IT. Presque tous les répondants à notre enquête sont dans cette démarche, pour au moins certaines activités OT. Cependant, seules 52% des entreprises confient la surveillance et le suivi de l'environnement OT *dans sa totalité à* l'équipe SOC (schéma 19). Ce chiffre n'a quasiment pas évolué depuis 4 ans que nous menons cette enquête. Les entreprises de la zone APAC font un peu mieux à cet égard, puisque 59% d'entre elles surveillent toutes les activités à partir du SOC.

50% des entreprises ont atteint une maturité de sécurité OT de niveau 3, contre 44% en 2021.

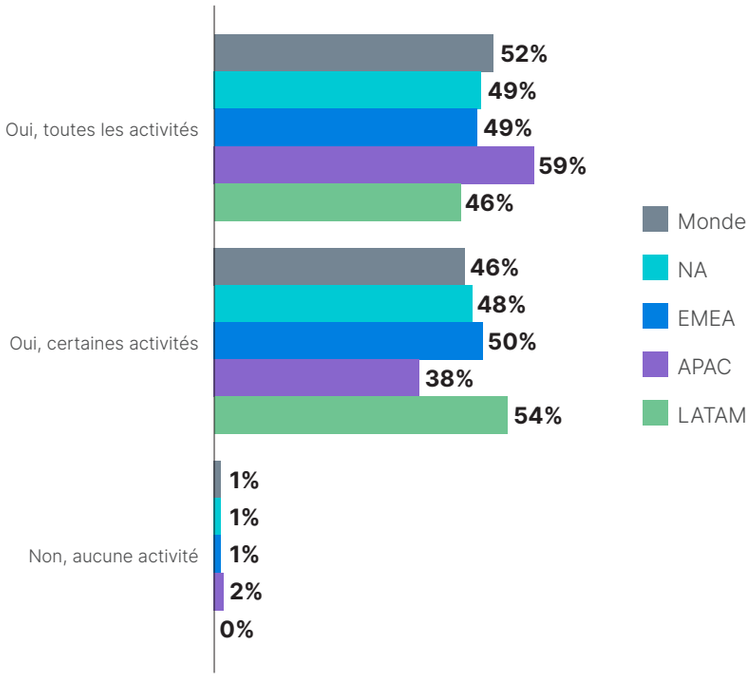


Schéma 19 : activités OT surveillées et suivies par le SOC.

Suivi et reporting des indicateurs

Les résultats sont mitigés sur le terrain du suivi et du reporting des indicateurs de sécurité. Nous avons présenté aux répondants une liste d'indicateurs de base de cybersécurité devant être suivis par toutes les entreprises. Seuls 52% des répondants déclarent en suivre au moins un (schéma 20).

En comparant les résultats sur l'Amérique du Nord d'année en année, la part de ceux qui suivent plusieurs indicateurs et en assurent le reporting a régressé par rapport à 2021 (schéma 21) - notamment pour l'indicateur de vulnérabilités identifiées et restaurées et celui des intrusions détectées et neutralisées.

Une proportion similaire de répondants communique régulièrement à leurs dirigeants des informations de base sur la sécurité de l'OT. Lorsqu'on leur présente une liste comprenant des éléments essentiels comme les rapports de conformité, les évaluations de sécurité et les incidents de sécurité, seuls 53% d'entre eux notifient au moins un de ces éléments à leur Direction générale (schéma 22).

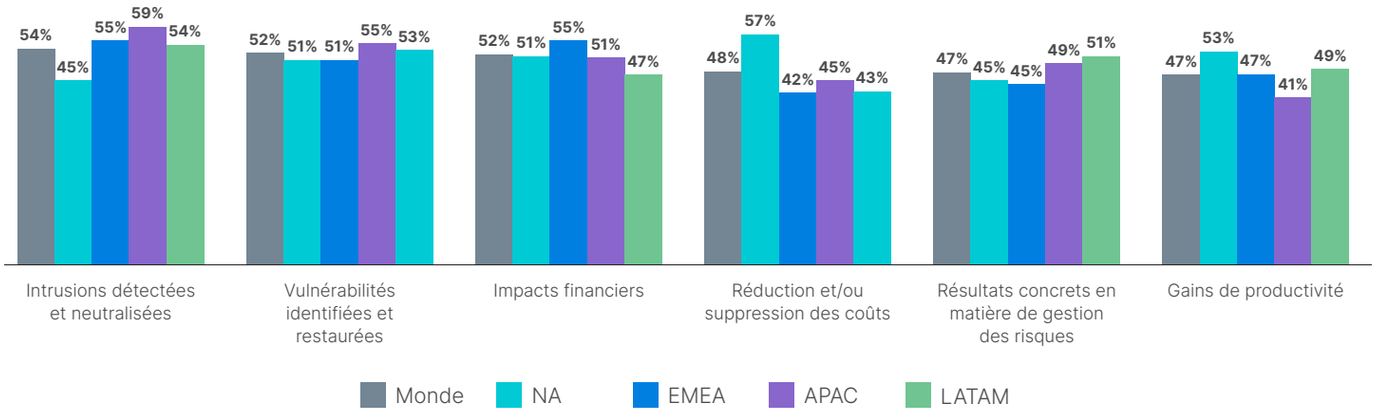


Schéma 20 : suivi/reporting des indicateurs de cybersécurité.

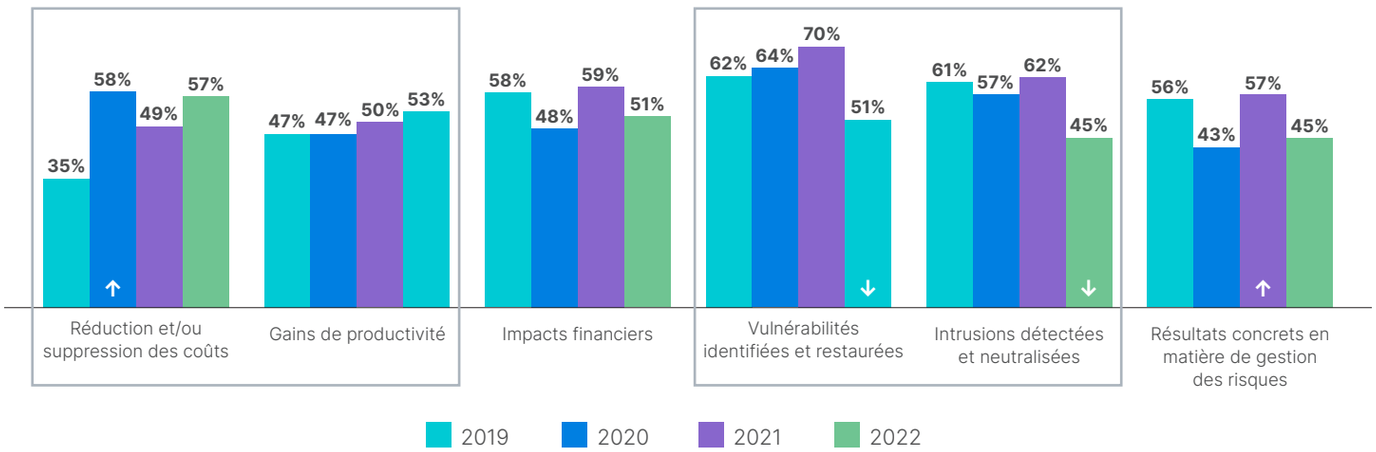


Schéma 21 : suivi/reporting des indicateurs de cybersécurité, Amérique du Nord.

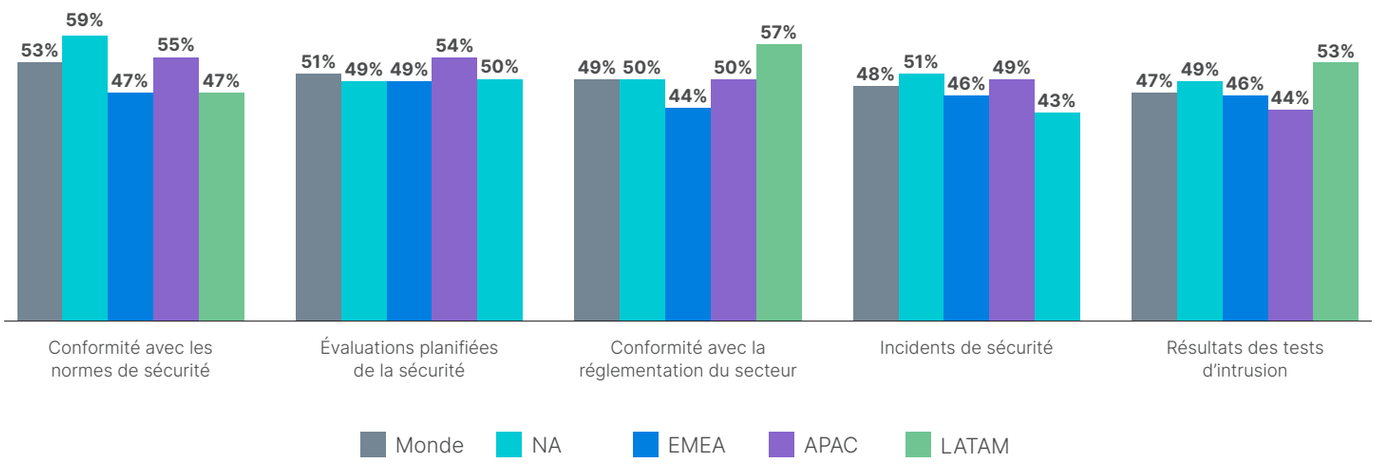


Schéma 22 : problématiques de cybersécurité OT notifiées à la direction générale.

Fonctions de sécurité en place

Les réponses se révèlent diverses et variées concernant les outils et fonctions de sécurité utilisés pour sécuriser les systèmes OT. Face à une liste assez complète d'outils et de processus, aucun d'entre eux n'est utilisé par plus de 47% du panel interrogé (schéma 23). Les outils mentionnés pour la première fois cette année sont l'accès distant sécurisé (41%), le SOAR (37%) et la veille sur les menaces (36%).

Ces chiffres reflètent un aspect de la sécurité qui, à bien des égards, est peu mature, avec différentes entreprises qui testent différentes approches. Une pratique devient clairement moins populaire, à savoir l'utilisation d'un centre d'opérations réseau (NOC) pour gérer la sécurité OT (schéma 24). Dans l'ensemble, il est intéressant de noter que les répondants nord-américains ont tendance à moins utiliser les fonctionnalités et pratiques répertoriées.

47% des entreprises utilisent un seul outil ou une seule approche pour la sécurité OT.

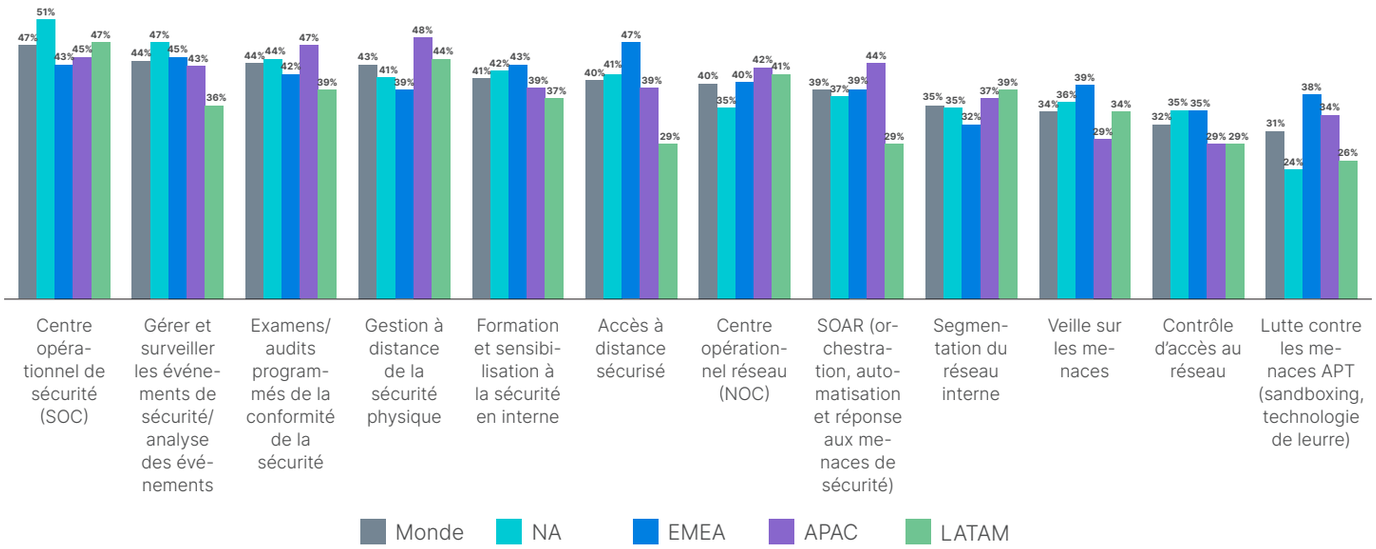


Schéma 23 : dispositifs de cybersécurité et de sécurité en place.

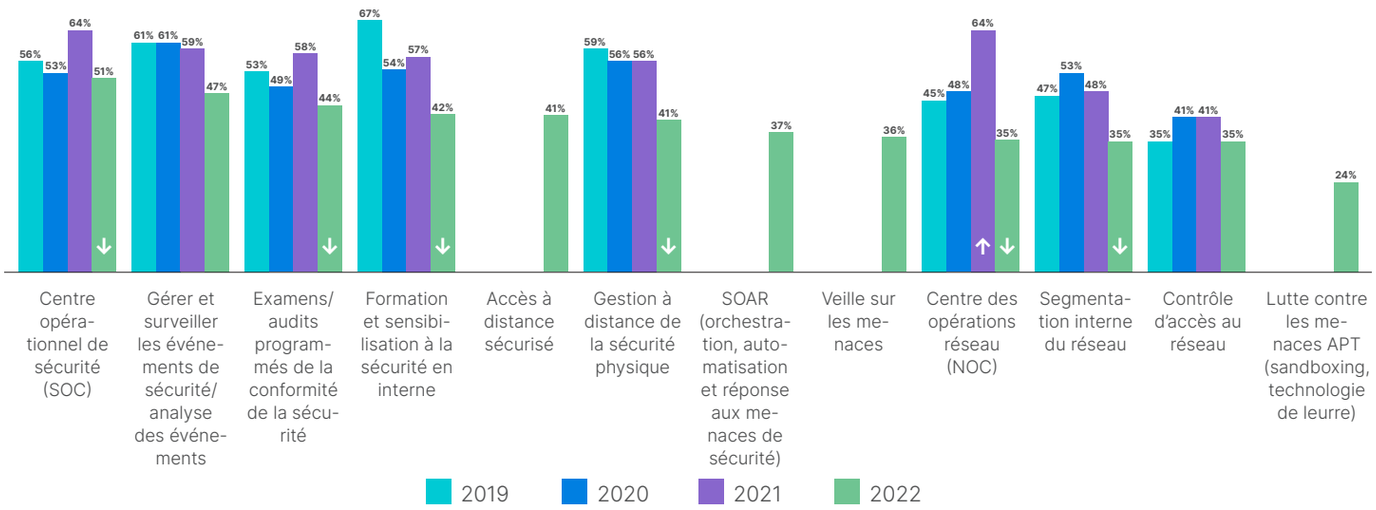


Schéma 24 : dispositifs de cybersécurité et de sécurité en place, Amérique du Nord.

Complexité des systèmes de sécurité et perception de leur efficacité

La complexité pèse souvent sur l'efficacité de la sécurité OT. Une grande majorité d'entreprises fait appel à entre deux et huit fournisseurs différents pour leurs équipements OT et disposent d'un parc de 100 à 10 000 dispositifs (schéma 25). Seuls 7% des entreprises ont réussi à consolider le nombre de constructeurs à un seul.

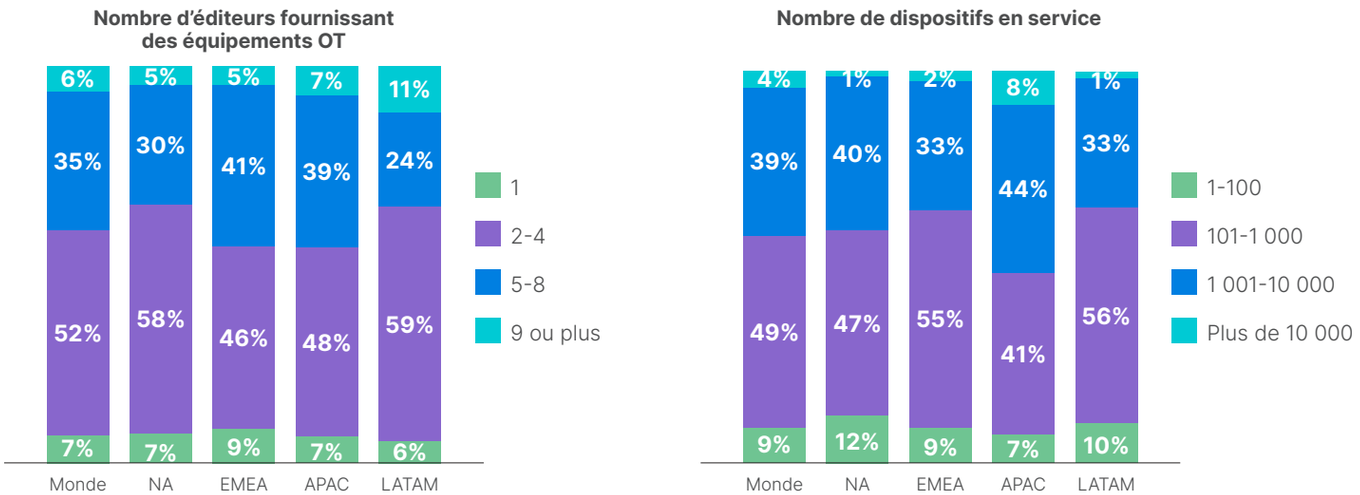


Schéma 25 : constructeurs OT et dispositifs OT utilisés.

Constat 5 : la majorité des entreprises subit encore plusieurs intrusions par an

Chaque année, nous demandons aux répondants de nous indiquer le nombre d'intrusions subies au cours des 12 derniers mois. En 2022, les trois-quarts ont reconnu avoir subi au moins trois intrusions, 19% en ont eu plus de six et 7% plus de 10 (schéma 26). Seuls 6% des répondants ont déclaré n'avoir subi aucune intrusion au cours des 12 derniers mois.

Les réponses sur la zone Amérique du Nord n'indiquent aucune amélioration sur quatre ans : la part des entreprises ayant subi trois intrusions ou plus depuis 2020 (schéma 27) est stable. Petite consolation : le pourcentage de répondants nord-américains ayant subi 10 intrusions est passé de 12% à 5% sur une année.

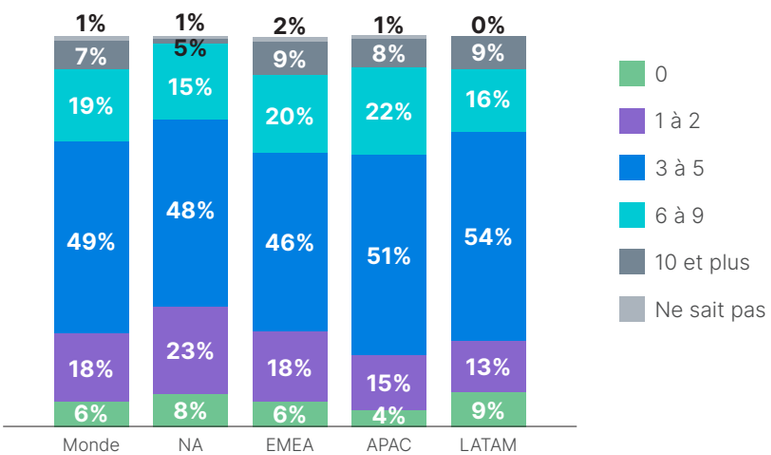


Schéma 26 : nombre d'intrusions sur l'année écoulée.

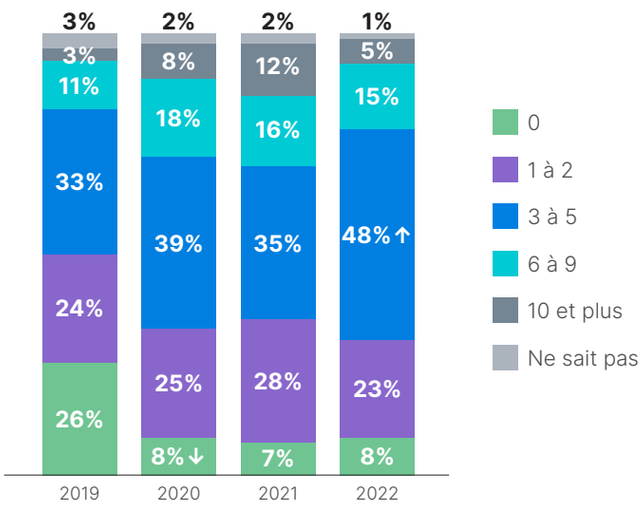


Schéma 27 : nombre d'intrusions sur l'année écoulée, Amérique du Nord.

Profils des attaques

Les entreprises interrogées ont été confrontées à une diversité de profils attaques, ce qui n'est pas surprenant compte tenu du nombre d'intrusions. Au total, huit profils d'attaque ont touché au moins un quart des personnes interrogées, les logiciels malveillants et le phishing arrivant en tête de liste avec plus de 40% des entreprises impactées (schéma 28). Les ransomwares ont touché moins d'un tiers des entreprises, sauf en Amérique latine (44%). Les répondants latino-américains sont moins nombreux à avoir été victimes de phishing par rapport à d'autres régions. L'examen des résultats sur quatre ans en Amérique du Nord démontre que les exactions perpétrées par les logiciels malveillants ou par des personnes internes malveillantes ont diminué cette année (schéma 29).

Le nombre global d'intrusions est à peu près similaire, quel que soit le niveau de maturité de sécurité déclaré, probablement parce que les entreprises plus matures sont capables de détecter une part plus importante des intrusions. Mais en examinant ce chiffre par profil d'attaque, il apparaît clairement que les entreprises les plus matures gèrent mieux les menaces internes et détectent davantage d'attaques provenant de l'extérieur (schéma 30).

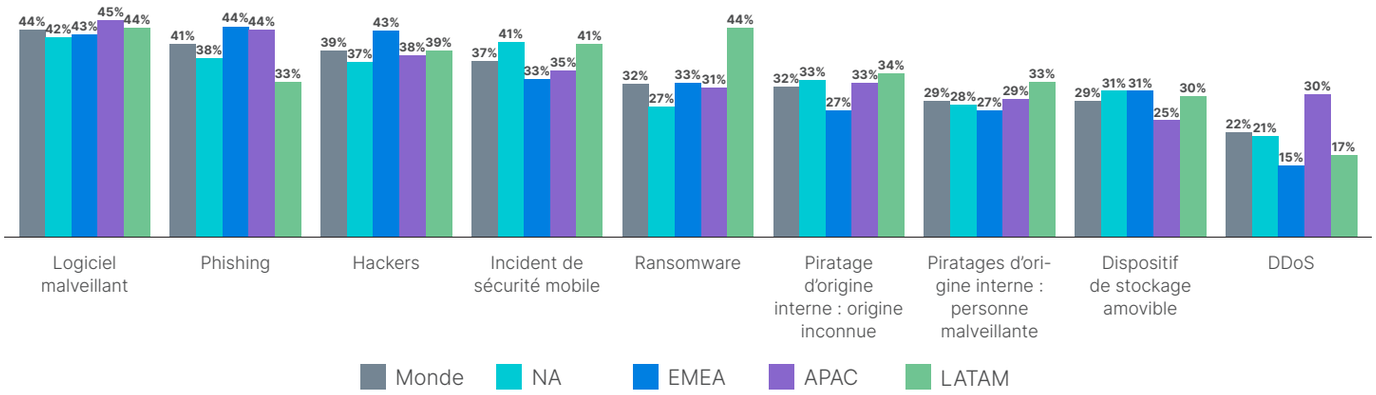


Schéma 28 : types d'intrusions subies.

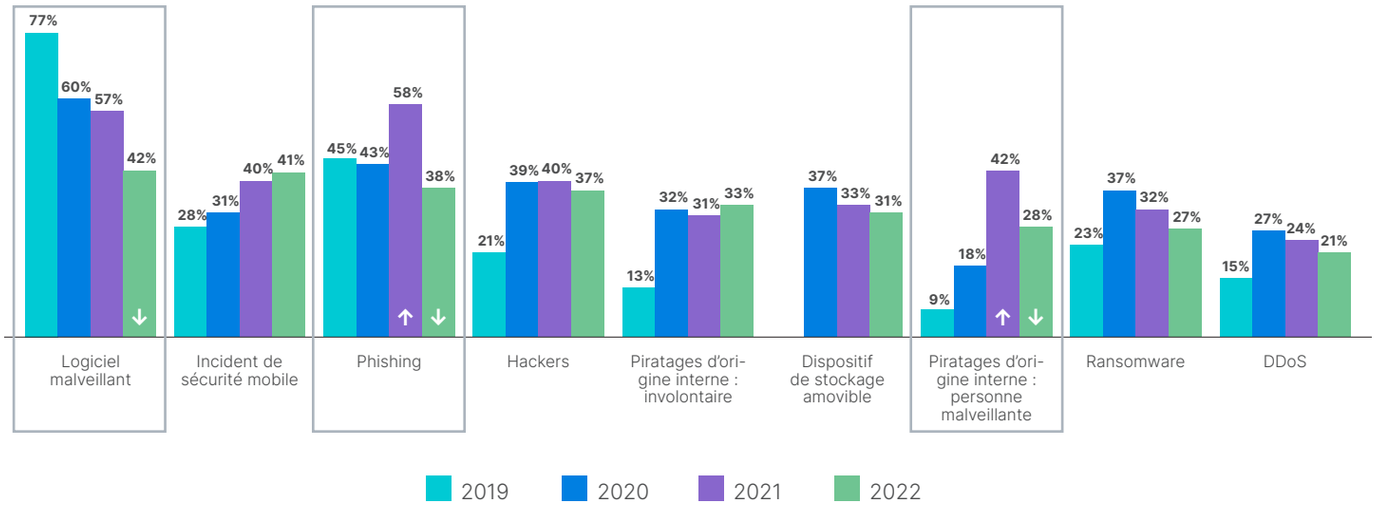


Schéma 29 : profils des intrusions subies, Amérique du Nord.

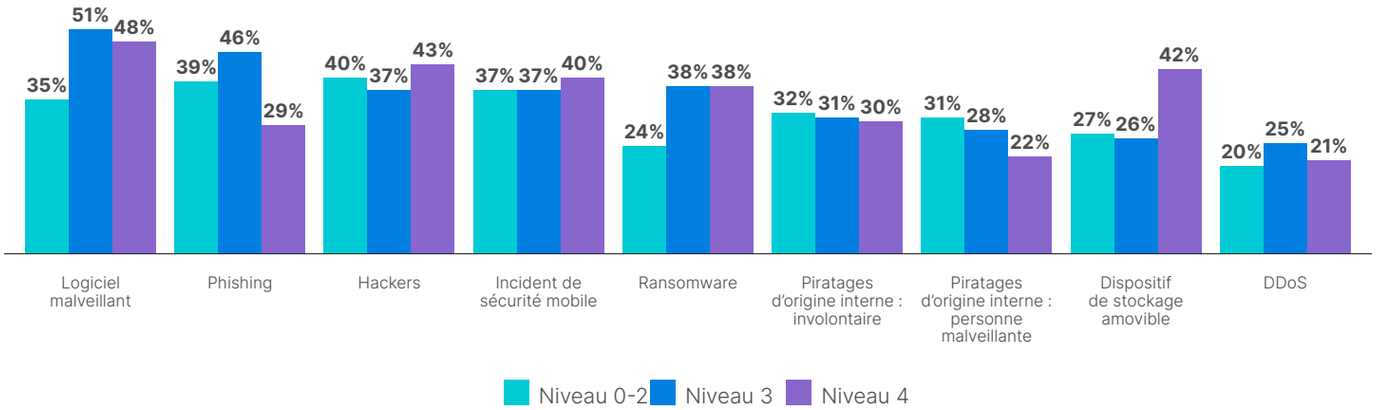


Schéma 30 : types d'intrusions par niveau de maturité de sécurité déclaré.

Impact des attaques

Il est intéressant de noter qu'une part légèrement plus élevée d'attaques a touché les systèmes OT par rapport aux systèmes IT (schéma 31), 61% des intrusions ayant eu un impact sur l'OT et 60% sur l'IT. L'impact des intrusions sur les entreprises est loin d'être négligeable. Près de la moitié des personnes interrogées a subi une interruption opérationnelle affectant leur productivité, tandis que plus d'un tiers d'entre elles ont vu leur chiffre d'affaires, leurs pertes de données, leur conformité et la valeur de leur marque impactés, voire des menaces pour la sécurité physique (schéma 32). Enfin, 90% des répondants admettent que la restauration des services a pris plusieurs heures ou plus (schéma 33).

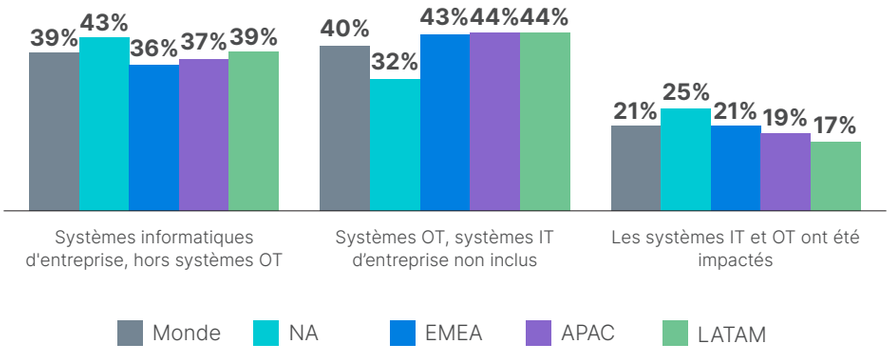


Schéma 31 : environnements impactés par les intrusions.

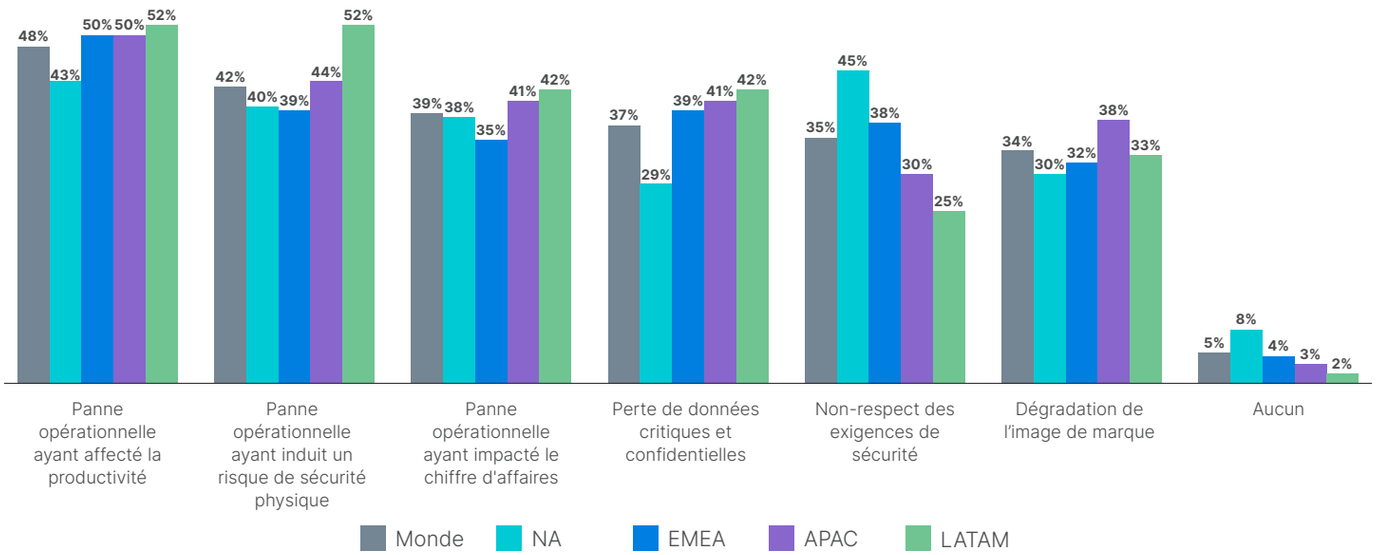


Schéma 32 : impacts organisationnels des intrusions.

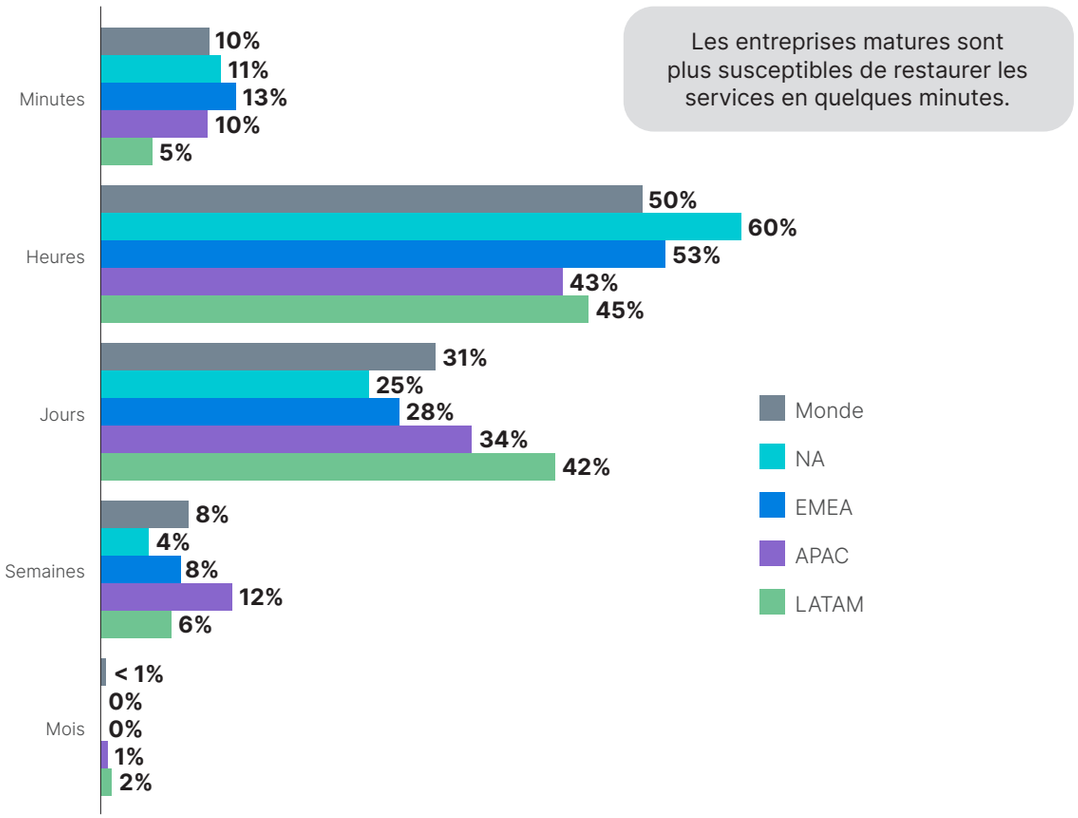


Schéma 33 : délai de restauration de service le plus long après une intrusion.

Les bonnes pratiques des entreprises les mieux sécurisées

Seules 6% des entreprises participant à l'enquête de cette année affirment n'avoir subi aucune intrusion au cours des 12 derniers mois, tandis que 5% ont signalé plus de *10 intrusions.* Nous avons comparé les pratiques.

Seules 6% des répondants peuvent affirmer n'avoir subi aucune intrusion sur l'année écoulée.

1. Les entreprises les mieux sécurisées ont 17% plus de chances de disposer d'une visibilité centralisée sur leur environnement OT.

La visibilité centralisée et de bout en bout sur toutes les activités OT est essentielle à leur sécurité. Ce travail a été entrepris par la plupart des entreprises. Les entreprises les mieux sécurisées sont plus de trois fois plus susceptibles de disposer de cette visibilité que leurs homologues moins performantes.

2. Les entreprises les mieux sécurisées sont 177% plus susceptibles de considérer le temps de réponse aux incidents de sécurité comme l'un de leurs trois principaux indicateurs de réussite.

Les processus ne peuvent être améliorés que s'ils sont mesurés. Réagir rapidement aux vulnérabilités OT est essentiel pour protéger ces systèmes. Les entreprises les plus performantes sont près de trois fois plus susceptibles de faire de cet indicateur un critère important de l'évaluation de leur performance globale.

3. Les entreprises les mieux sécurisées sont 37% plus susceptibles de disposer d'une technologie de contrôle d'accès au réseau.

S'assurer que seules les parties autorisées peuvent accéder à des systèmes spécifiques est essentiel pour sécuriser les ressources technologiques. En ce qui concerne l'OT, les personnes qui doivent accéder à ces systèmes sont représentatives d'un panel relativement étroit de titres de poste. Les entreprises qui ont évité les intrusions l'année dernière sont nettement plus susceptibles d'avoir mis en place de tels contrôles.

4. Les entreprises les mieux sécurisées sont 48% plus susceptibles de signaler les incidents de sécurité à la direction générale.

Les points qui sont régulièrement notifiés aux dirigeants ont tendance à rester une priorité sur l'année. Les entreprises qui tiennent les cadres dirigeants au courant des incidents de la sécurité ont tendance à en avoir moins. Les entreprises de premier plan ont tendance à être plus transparentes avec la direction générale.

5. Les entreprises les mieux sécurisées sont 32% plus susceptibles de demander à leur SOC de surveiller et suivre la sécurité des technologies OT.

Les centres opérationnels de sécurité (SOC) existent depuis des décennies et ont développé des pratiques éprouvées pour gérer la sécurité IT. Il est probable que les professionnels de l'OT qui ont su déjouer les intrusions ont confié leur sécurité OT au SOC.

6. Les entreprises les mieux sécurisées sont 44% plus susceptibles d'assurer le suivi et le reporting des intrusions.

La compréhension des attaques passées permet à une entreprise d'affûter ses compétences pour déjouer les attaques futures. Et il s'agit dans un premier temps de tenir à jour des registres de sécurité. Les entreprises qui n'ont pas subi d'intrusions sont plus susceptibles de les signaler systématiquement si nécessaire.

7. Les entreprises les mieux sécurisées sont nettement plus susceptibles de ne faire appel qu'à un seul constructeur pour fournir leurs dispositifs OT compatibles IP.

Éviter la complexité des réseaux et des systèmes est un bon moyen de réduire la surface d'attaque et d'améliorer la posture de sécurité. Aucune des entreprises ayant subi 10 intrusions ou plus ne faisait appel à un unique fournisseur pour ses dispositifs OT sur IP, ce qui est le cas pour plus d'un tiers des entreprises les mieux sécurisées.

Conclusion

L'état des lieux 2022 des technologies OT et leur cybersécurité révèle que les entreprises ne progressent pas au même rythme en matière de sécurité OT, pour une protection complète des systèmes ICS et SCADA dans le monde relativement nouveau des environnements OT connectés. Les progrès en matière de maturité de sécurité depuis l'année dernière n'ont que peu fait évoluer les résultats concrets sur le terrain : une majorité d'entreprises subit encore des intrusions trop fréquentes, plusieurs fois par an dans la plupart des cas.

Compte tenu du contexte géopolitique, les gouvernements du monde préviennent que les cyberattaques risquent de se multiplier contre les infrastructures critiques et les acteurs économiques clés. Les entreprises industrielles gagnaient à rendre rapidement leurs efforts de sécurité OT plus mature. Elles doivent tirer parti de technologies de comportement prédictif, d'orchestration et d'automatisation pour établir un véritable accès de type zero-trust et se défendre contre des menaces internes intentionnelles ou fortuites, des cybercriminels externes et des assaillants sponsorisés par des états.

Références

[1] Mayank Agrawal, et. al, "Industry 4.0: Reimagining Manufacturing Operations After COVID-19," McKinsey, 29 juillet 2020.

[2] "Global Threat Landscape Report, 1H 2021," Fortinet, août 2021.

[3] Clare Duffy, "Colonial Pipeline Attack: A 'Wake Up Call' about the Threat of Ransomware," CNN, 16 mai 2021; Liam Tung, "Ransomware: Meat Firm JBS Says It Paid Out $11m After Attack," ZDnet, 10 juin 2021.

[4] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, 20 avril 2022.

[5] Catherine Stupp, "Russian Cyberattacks Increase on Ukraine's Critical Infrastructure: Report," Wall Street Journal, 5 avril 2022.

[6] Phil Muncaster, "Critical Infrastructure Firms See Cyber-Attacks Surge," InfoSecurity, 10 mai 2022.

[7] Steven Webb, "IT/OT & OT Total Available Market Analysis," Westlands Advisory Research for Fortinet, Mars 2022.

[8] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, 20 avril 2022.

septembre 13, 2022 3:19 PM

1578659-0-0-FR