RAPPORT 2022 SUR LE COÛT DES MENACES INTERNES À L'ÉCHELLE MONDIALE

Réalisé de manière indépendante par :

Ponemon INSTITUTE

proofpoint.

SOMMAIRE

INTRODUCTION

Le Ponemon Institute a le plaisir de vous présenter les conclusions de son *Rapport 2022 sur le coût des menaces internes à l'échelle mondiale*.

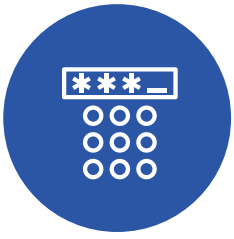
CETTE ÉTUDE DE RÉFÉRENCE EST LA QUATRIÈME DONT LE BUT EXPLICITE EST DE COMPRENDRE LES CONSÉQUENCES FINANCIÈRES DES MENACES INTERNES. ELLE PERMET PAR AILLEURS D'ÉVALUER L'EFFICACITÉ DES MESURES QUE PRENNENT LES ENTREPRISES POUR RÉDUIRE CES RISQUES.

Réalisée en 2016, la première étude sur le coût des menaces internes à l'échelle mondiale se concentrait exclusivement sur les entreprises basées en Amérique du Nord. Depuis lors, elle a été élargie afin d'inclure les entreprises d'Europe, du Moyen-Orient, d'Afrique et d'Asie-Pacifique comptant un effectif mondial de 500 à plus de 75 000 collaborateurs. Cette année, nous avons interrogé 1 004 professionnels de l'informatique et de la sécurité informatique travaillant dans 278 entreprises ayant subi un ou plusieurs incidents majeurs d'origine interne. Au total, 6 803 incidents d'origine interne sont représentés dans cette étude.

Dans le cadre de cette étude, les menaces internes sont divisées selon trois profils :

Collaborateur ou sous-traitant négligent

Utilisateur interne malintentionné



Voleur d'identifiants de connexion

RÉSUMÉ

CES DEUX DERNIÈRES ANNÉES, LA FRÉQUENCE ET LE COÛT DES MENACES INTERNES ONT AUGMENTÉ DE FAÇON SPECTACULAIRE. LE NOMBRE DE VOLS D'IDENTIFIANTS DE CONNEXION, PAR EXEMPLE, A PRESQUE DOUBLÉ DEPUIS 2020.

Même si le nombre de menaces internes a augmenté pour les trois profils, celles liées à la négligence d'un collaborateur sont les plus courantes.

D'après nos observations, 56 % des incidents subis par les entreprises ayant participé à l'étude étaient dus à la négligence d'un collaborateur, et le coût annuel moyen de la correction des incidents s'élevait à 6,6 millions de dollars.

L'étude révèle également que le coût des menaces internes varie considérablement selon le type d'incident. Ces variations s'expliquent principalement par les activités à entreprendre à la suite d'un incident d'origine interne, notamment la surveillance, les investigations, la remontée des problèmes, la réponse aux incidents, le confinement, l'analyse ex post et l'application de mesures correctives.

Voici quelques chiffres clés concernant le coût des incidents d'origine interne sur une période de 12 mois :

278 Nombre total d'entreprises interrogées	**6 803** Nombre total d'incidents d'origine interne	**15,4 Mio USD** Coût annuel moyen total
56 % Incidents dus à la négligence	**26 %** Incidents imputables à des utilisateurs internes malintentionnés	**18 %** Incidents liés au vol d'identifiants de connexion
6,6 Mio USD Coût annualisé pour la négligence	**4,1 Mio USD** Coût annualisé pour les utilisateurs internes malintentionnés	**4,6 Mio USD** Coût annualisé pour le vol d'identifiants de connexion

VOICI LES PRINCIPALES OBSERVATIONS DE L'ÉTUDE.

Le délai de confinement d'un incident d'origine interne a augmenté depuis la dernière étude.

Il a fallu en moyenne 85 jours pour confiner les incidents, contre 77 jours dans la dernière étude.

Seuls 12 % des incidents ont été endigués en moins de 30 jours.

Nombre moyen de jours pour confiner un incident

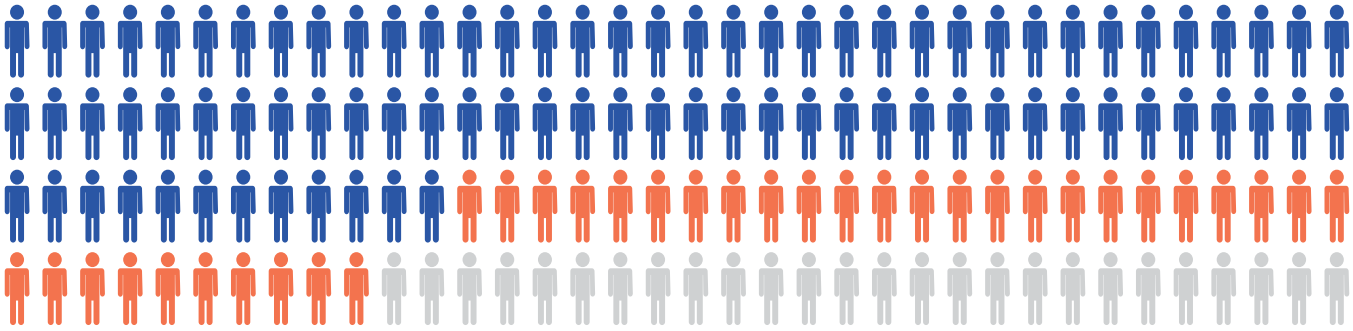
85 JOURS

12 % des incidents endigués en

≤ 30 JOURS

34 % des incidents endigués en

≥ 90 JOURS



La négligence des utilisateurs internes est la cause première de la plupart des incidents.

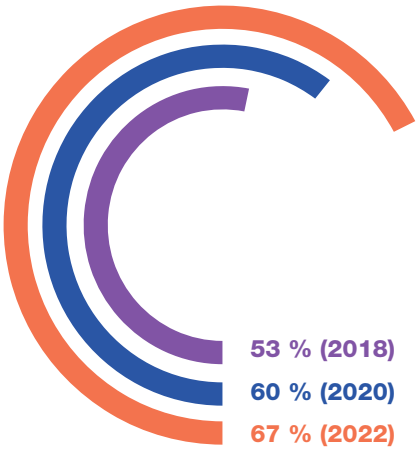
Au total, 3 807 attaques (56 %) ont été provoquées par la négligence d'un collaborateur ou d'un sous-traitant, avec un coût moyen de 484 931 dollars par incident. Divers comportements peuvent en être à l'origine : oubli de vérifier que les terminaux sont sécurisés, non-respect des politiques de sécurité de l'entreprise, correctifs et mises à niveau disponibles non installés, etc.

1 749 incidents (26 %) sont imputables à des utilisateurs internes malintentionnés, avec un coût moyen de 648 062 dollars par incident.

Les utilisateurs internes malintentionnés sont des collaborateurs ou des personnes autorisées qui tirent parti de leur accès aux données pour se livrer à des activités préjudiciables, illégales ou contraires à l'éthique. Étant donné que les collaborateurs ont accès à de plus en plus d'informations afin d'améliorer leur productivité dans le contexte de télétravail actuel, les utilisateurs internes malintentionnés sont plus difficiles à détecter que les cybercriminels externes.

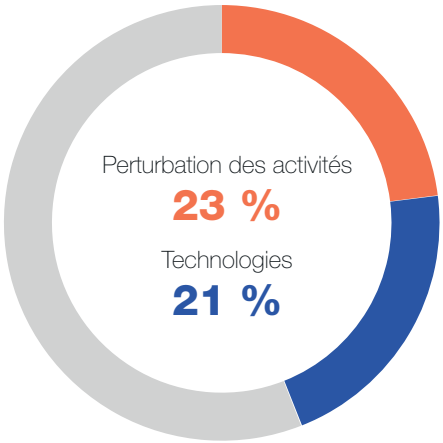
Le nombre de vols d'identifiants de connexion a presque doublé depuis la dernière étude.

Les vols d'identifiants de connexion sont le type d'incident dont la correction coûte le plus cher (en moyenne 804 997 dollars par incident). L'objectif des voleurs d'identifiants de connexion est de dérober des identifiants qui leur permettront d'accéder à des données stratégiques. L'ingénierie sociale, en particulier le phishing, est une technique d'attaque prisée par bon nombre d'entre eux. Cette année, 1 247 incidents (18 %) au total étaient liés au vol d'identifiants de connexion.



La fréquence des incidents a bondi.

Selon l'étude 2022, 67 % des entreprises subissent entre 21 et plus de 40 incidents par an, contre 60 % en 2020 et 53 % en 2018.



Les perturbations et les temps d'arrêt, ainsi que les investissements dans les technologies, représentent les coûts les plus élevés en matière de gestion des menaces internes.

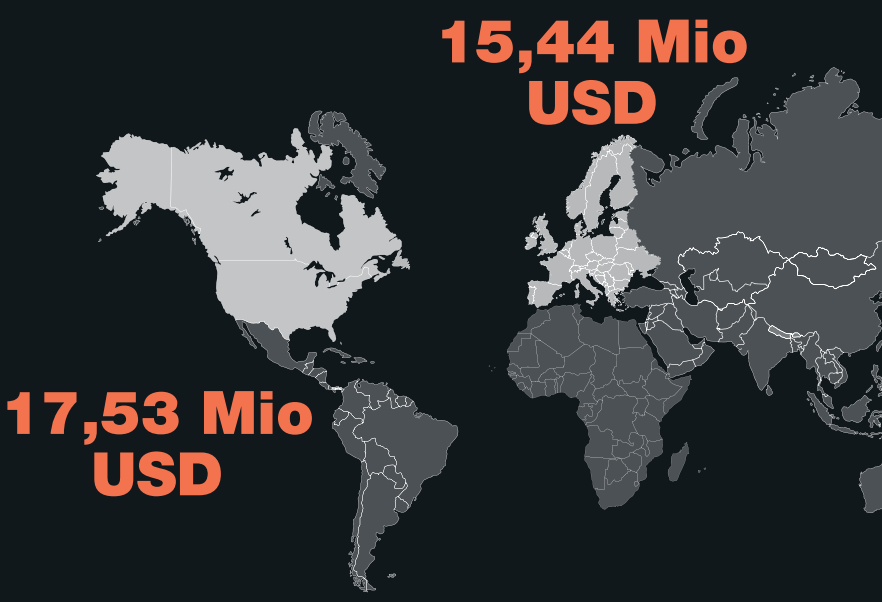
Les deux catégories de coûts les plus importantes sont les conséquences de la perturbation des activités en raison de la baisse de productivité des collaborateurs (23 % du coût total) et les technologies, qui comprennent la valeur amortie et les licences pour le matériel et les logiciels déployés en réponse à des incidents d'origine interne (21 %).

Le confinement des incidents de sécurité d'origine interne est un poste de dépenses conséquent pour les entreprises.

En moyenne, les entreprises dépensent 184 548 dollars pour limiter les conséquences d'une menace interne. La remontée des problèmes et la surveillance sont les activités dont le coût moyen est le moins élevé (32 228 et 35 080 dollars, respectivement). Les incidents endigués en moins de 30 jours ont affiché le coût annuel moyen le plus faible (11,23 millions de dollars). En revanche, le coût annuel moyen des incidents dont le confinement a pris plus de 90 jours s'élève à 17,19 millions de dollars.

Les entreprises nord-américaines dépensent plus que le coût moyen pour la gestion des menaces internes.

Le coût moyen total de la résolution des menaces internes sur une période de 12 mois s'élève à 15,38 millions de dollars. Les entreprises nord-américaines ont enregistré le coût total le plus élevé, à savoir 17,53 millions de dollars. Elles sont suivies par les entreprises européennes, avec 15,44 millions de dollars.



Les entreprises de services financiers et les sociétés de services enregistrent le coût moyen le plus élevé.

Celui-ci s'élève respectivement à 21,25 et 18,65 millions de dollars. Les sociétés de services représentent un large éventail d'entreprises, notamment des cabinets comptables, des cabinets de conseil et des sociétés de services professionnels.

La taille de l'entreprise influe sur le coût par incident.

Le coût annuel des incidents varie selon la taille de l'entreprise. Au cours de l'année écoulée, les grandes entreprises comptant plus de 75 000 collaborateurs ont dépensé en moyenne 22,68 millions de dollars pour résoudre des incidents d'origine interne. Pour faire face aux conséquences des incidents d'origine interne, les entreprises de plus petite taille, comptant moins de 500 collaborateurs, ont dépensé en moyenne 8,13 millions de dollars.

Les entretiens que nous avons réalisés avec les participants à l'étude nous ont permis de tirer les conclusions suivantes sur les menaces internes.

En plus de déterminer le coût des menaces internes pour les entreprises dans le cadre de l'étude, nous avons interrogé les participants au sujet de leurs expériences de ce type de menaces et des mesures qu'ils prennent pour réduire les risques.

Parmi tous les types de menaces internes couverts dans cette étude, c'est le vol d'identifiants de connexion qui préoccupe le plus les entreprises. Le nombre de vols d'identifiants de connexion a presque doublé depuis la dernière étude. Il s'agit en outre du type d'incident d'origine interne dont la correction coûte le plus cher. 55 % des sondés craignent avant tout qu'un cyberpirate vole les identifiants de connexion d'un collaborateur. Ils sont bien moins nombreux (21 %) à être préoccupés par la négligence des utilisateurs internes.

La plupart des incidents d'origine interne sont causés par des collaborateurs négligents et des voleurs d'identifiants de connexion. 57 % des sondés indiquent que les incidents d'origine interne qu'ils ont subis étaient dus à la négligence d'un collaborateur, tandis que 51 % affirment qu'un cybercriminel externe a volé des données en compromettant les identifiants ou les comptes d'utilisateurs internes.

Les terminaux IoT vulnérables présentent le risque le plus élevé de fuite de données. 63 % des sondés admettent craindre la fuite de données sensibles via des terminaux IoT non gérés. D'autres redoutent que la même chose se produise via le cloud (52 %) et le réseau (51 %).

La plupart des données sensibles se trouvent dans les emails des collaborateurs. 65 % des sondés affirment que les collaborateurs stockent les données les plus sensibles de leur entreprise, comme les données personnelles, la propriété intellectuelle et autres informations métier stratégiques, dans leurs emails.

Les utilisateurs internes malintentionnés se servent de la messagerie d'entreprise pour voler des données sensibles. 74 % des sondés déclarent que des utilisateurs internes malintentionnés ont envoyé des données sensibles à des tiers par email, 62 % qu'ils ont recherché des ports ouverts et des vulnérabilités, et 60 % qu'ils ont accédé à des données sensibles sans lien avec leur rôle ou fonction.

Face à la multiplication des menaces internes et à l'allongement du délai de confinement, des technologies avancées telles que l'analyse du comportement des utilisateurs et l'automatisation sont essentielles pour s'en prémunir. Les outils de détection des menaces internes grâce à l'analyse du comportement des utilisateurs sont considérés comme indispensables ou très importants pour réduire les menaces internes (62 % des sondés). Ils sont suivis par l'automatisation (55 % des sondés) et par l'intelligence artificielle et l'apprentissage automatique (54 %) pour la prévention, les investigations, la remontée des problèmes, le confinement et la correction des incidents d'origine interne.

05

signes que votre entreprise est en danger

01 Les collaborateurs ne reçoivent aucune formation leur permettant de comprendre et d'appliquer pleinement les lois ou exigences réglementaires liées à leur travail et qui affectent la sécurité de l'entreprise.

02 Les collaborateurs ignorent les mesures à prendre de manière systématique pour assurer en permanence la protection des terminaux qu'ils utilisent (qu'ils soient fournis par l'entreprise ou BYOD).

03 Les collaborateurs envoient des données hautement confidentielles vers des emplacements non sécurisés dans le cloud, ce qui expose l'entreprise à des risques.

04 Les collaborateurs enfreignent les politiques de sécurité de l'entreprise pour simplifier leurs tâches.

05 Les collaborateurs exposent l'entreprise à des risques dès lors qu'ils n'installent pas systématiquement les derniers correctifs et mises à niveau disponibles pour les terminaux et les services.

À PROPOS DE L'ÉTUDE :

L'ÉTUDE SE CONCENTRE SUR LES INCIDENTS D'ORIGINE INTERNE AYANT GÉNÉRÉ DES COÛTS POUR LES ENTREPRISES AU COURS DES 12 DERNIERS MOIS.

Les méthodes que nous employons s'efforcent de prendre en compte les coûts directs et indirects, y compris, sans s'y limiter, les menaces suivantes :

- Vol ou fuite de données stratégiques ou de propriété intellectuelle
- Impact des temps d'arrêt sur la productivité
- Dommages causés aux équipements et autres ressources
- Coût de la détection et de la correction des systèmes et des processus métier fondamentaux
- Conséquences juridiques et réglementaires (p. ex., frais de défense en cas de litige)
- Perte de confiance des principales parties prenantes
- Préjudice porté à la marque et à sa réputation sur le marché

Cette étude emploie une méthode de comptabilisation des coûts par activité. Notre enquête sur le terrain s'est déroulée sur une période de deux mois et a pris fin en septembre 2021. Notre échantillon de référence final est constitué de 278 entreprises. Au total, 1 004 entretiens ont été menés avec des collaborateurs clés de ces entreprises. Les coûts des activités mentionnés dans ce rapport ont été calculés à partir d'informations recueillies dans la plus stricte confidentialité auprès des participants lors de réunions ou de visites sur site. Les entreprises ciblées remplissaient les critères suivants :

- Entreprise commerciale ou du secteur public
- Présence dans les régions suivantes : Amérique du Nord, Europe, Moyen-Orient et Afrique, et Asie-Pacifique
- Rôle informatique central avec contrôle sur l'environnement sur site et/ou dans le cloud
- Victime d'un ou de plusieurs incidents majeurs liés à des utilisateurs internes négligents ou malintentionnés

Ce rapport propose un cadre objectif pour mesurer l'impact total des coûts engendrés par les incidents d'origine interne. Trois profils ont été utilisés pour catégoriser et analyser les coûts associés aux incidents d'origine interne de 278 entreprises :

- Collaborateur ou sous-traitant négligent
- Utilisateur interne (y compris collaborateur ou sous-traitant) malintentionné
- Voleur d'identifiants de connexion (ou « usurpateur »)

La première étape de cette étude a consisté à recruter des entreprises internationales. Les chercheurs ont utilisé des entretiens de diagnostic et une méthode de comptabilisation des coûts par activité pour recueillir et extrapoler les données relatives aux coûts. Le Ponemon Institute s'est chargé de toutes les phases de ce projet de recherche, qui incluaient les étapes suivantes :

01 Sessions de travail afin de définir les domaines de recherche

02 Recrutement des entreprises de référence

03 Mise au point d'une méthode de comptabilisation des coûts par activité

04 Administration du programme de recherche

05 Analyse des résultats à l'aide de contrôles de fiabilité appropriés

06 Préparation d'un rapport résumant les principales observations de l'étude

ÉCHANTILLON DE RÉFÉRENCE

L'UNITÉ D'ANALYSE DE CETTE ÉTUDE DE RÉFÉRENCE EST L'ENTREPRISE.

FIGURE 1.

Secteurs d'activité des entreprises participantes

La figure 1 montre la répartition en % des entreprises dans 13 secteurs d'activité. Les trois principaux secteurs sont les services financiers, les services et l'industrie et la fabrication. Les entreprises de services financiers incluent des banques, des compagnies d'assurance, ainsi que des sociétés de gestion d'investissements et de courtage. Les sociétés de services représentent un large éventail d'entreprises, notamment des cabinets comptables, des cabinets de conseil et des sociétés de services professionnels.

n = 278 entreprises

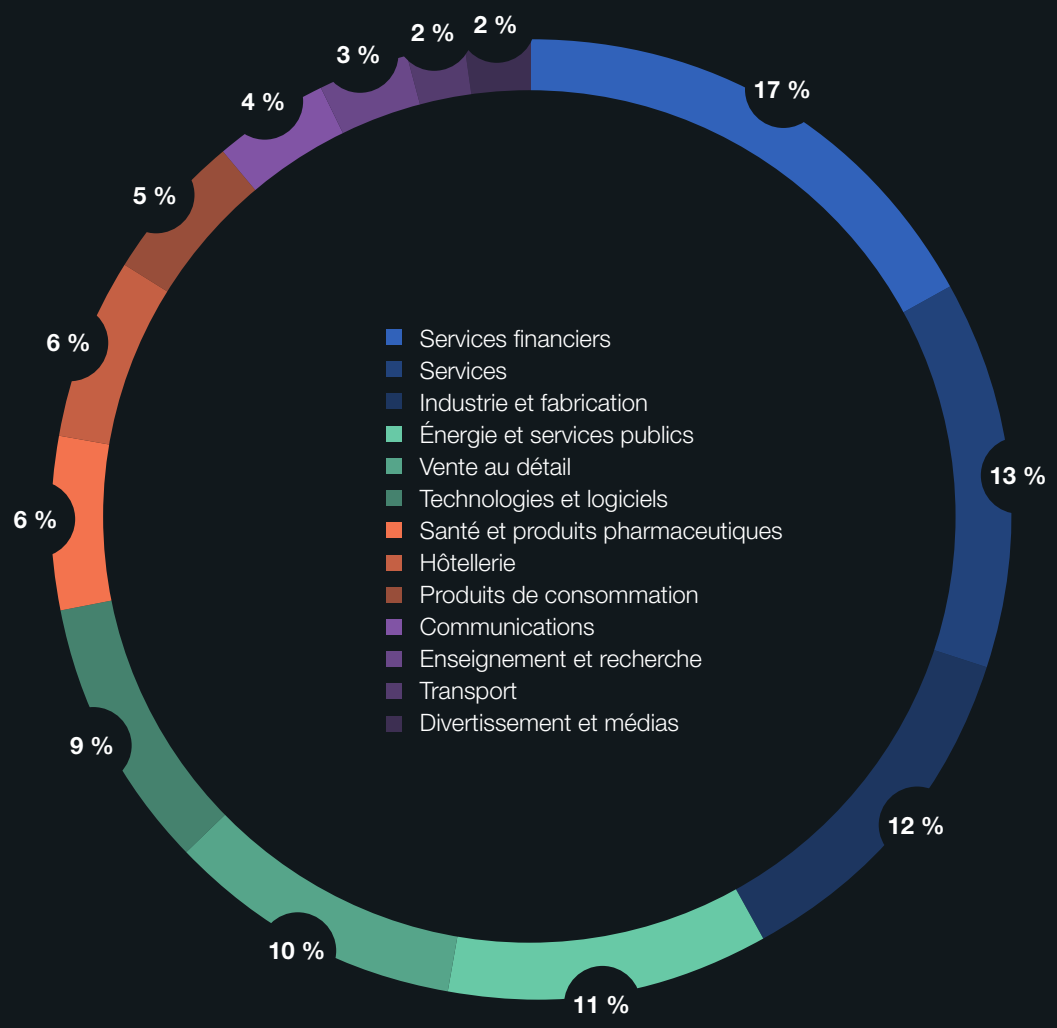


FIGURE 2.

Effectif (taille) des entreprises participantes

La figure 2 montre la répartition en % des entreprises selon leur effectif mondial, qui est un indicateur de la taille de l'entreprise. Comme vous pouvez le voir, l'échantillon est constitué à 43 % d'entreprises de plus grande taille comptant plus de 5 000 équivalents temps plein.

n = 278 entreprises

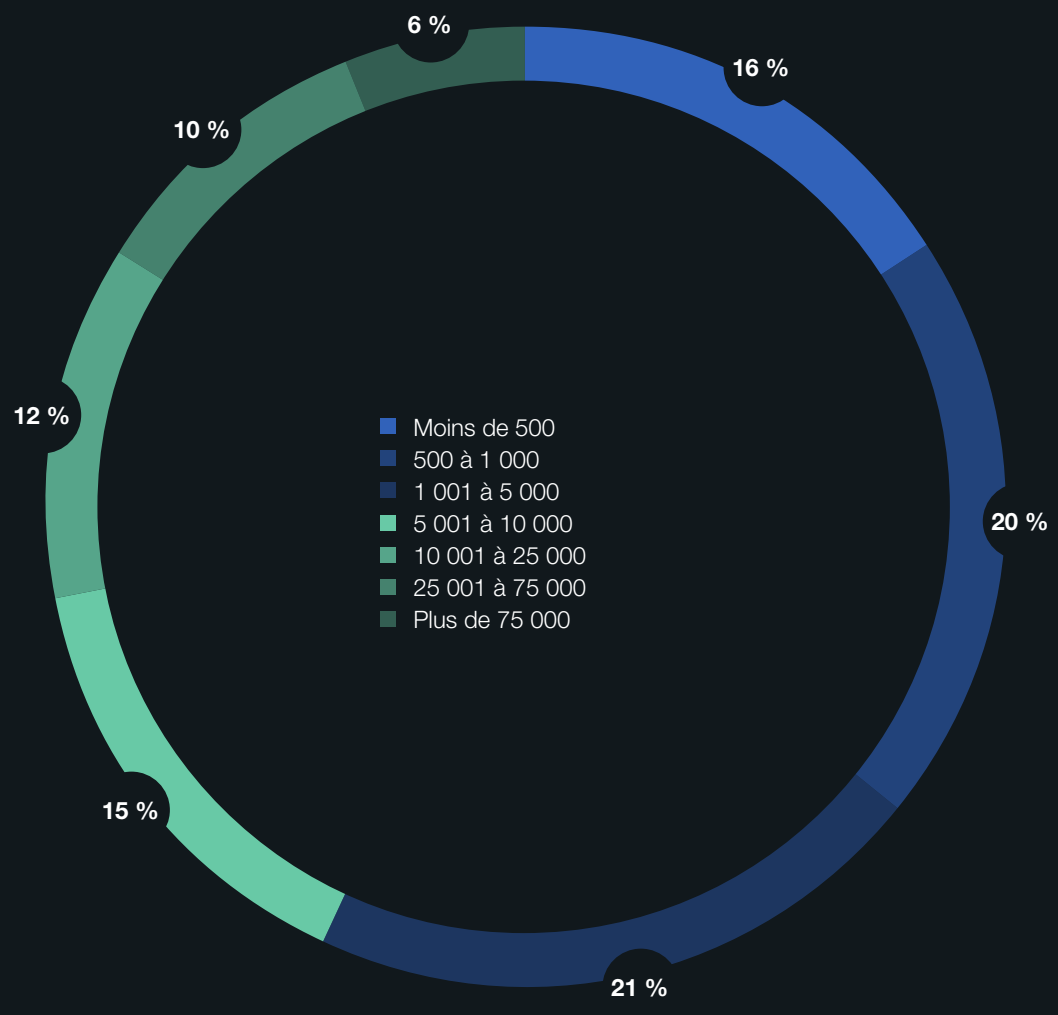


FIGURE 3.

Collaborateurs interrogés par poste ou fonction

D'après la figure 3, 1 004 collaborateurs ont participé à des entretiens sur site. Chaque étude de cas englobait 4,7 collaborateurs en moyenne. Les segments les plus importants sont les RSSI (15 %), les opérations informatiques (14 %), les DSI (12 %) et les techniciens informatiques (11 %).

n = 1 004 sondés

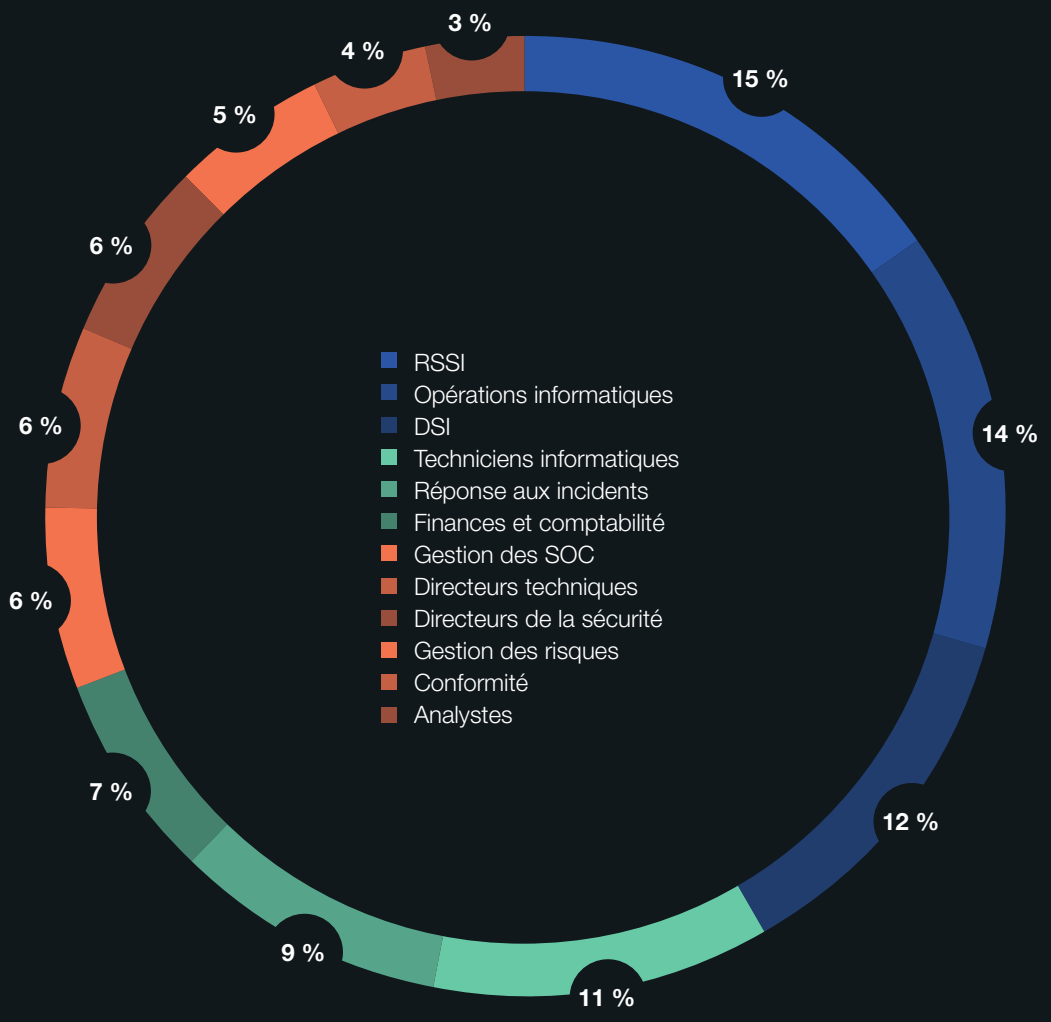
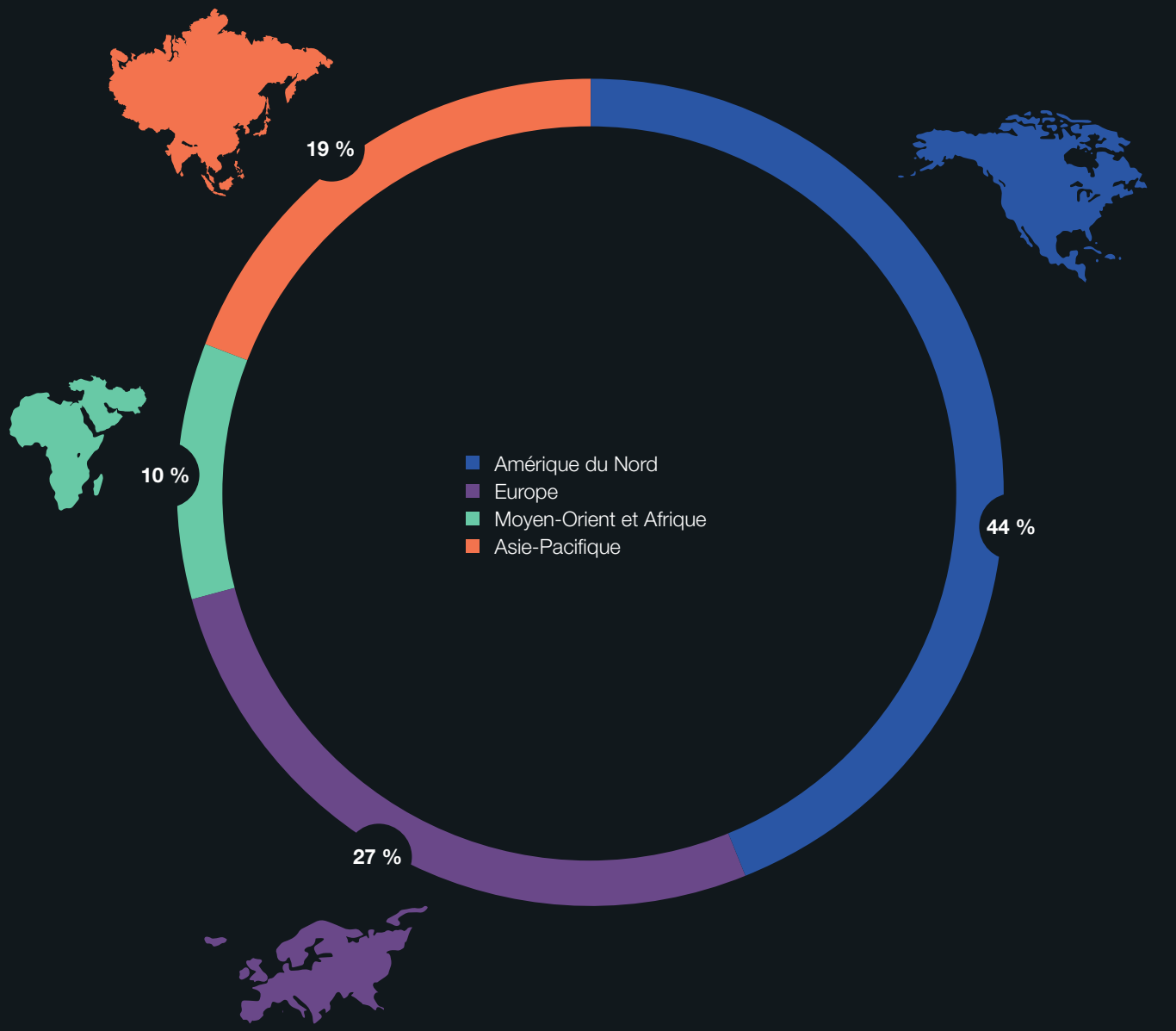


FIGURE 4.

Répartition régionale des entreprises internationales

La figure 4 montre les régions couvertes par l'étude. L'Amérique du Nord constitue le segment le plus important (44 % des entreprises), et le Moyen-Orient et l'Afrique le plus petit (10 %).

n = 278 entreprises



PRINCIPALES OBSERVATIONS

LE PLUS GRAND NOMBRE D'INCIDENTS SIGNALÉS PAR UNE ENTREPRISE DONNÉE EST DE 46, ET LE PLUS PETIT DE UN.

Collaborateurs ou sous-traitants négligents

3 807

Utilisateurs internes malintentionnés

1 749

Voleurs d'identifiants de connexion (usurpateurs)

1 247

FIGURE 5.

Répartition des 6 803 incidents entre les trois profils d'utilisateurs internes

Les collaborateurs et les sous-traitants demeurent la principale source de menaces internes. La figure 5 montre la répartition des 6 803 attaques signalées qui ont été analysées dans le cadre de notre échantillon. Au total, 3 807 attaques (56 %) étaient dues à la négligence d'un collaborateur ou d'un sous-traitant. Les utilisateurs internes malintentionnés ont causé 1 749 attaques (26 %), tandis que le vol d'identifiants de connexion concernait 1 247 attaques (18 %).

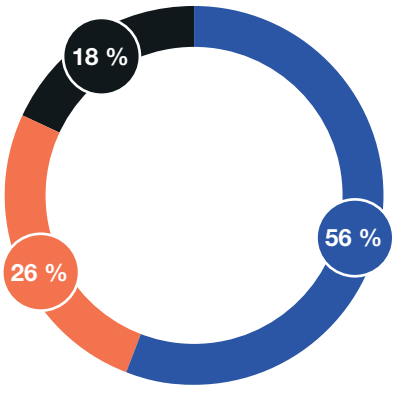
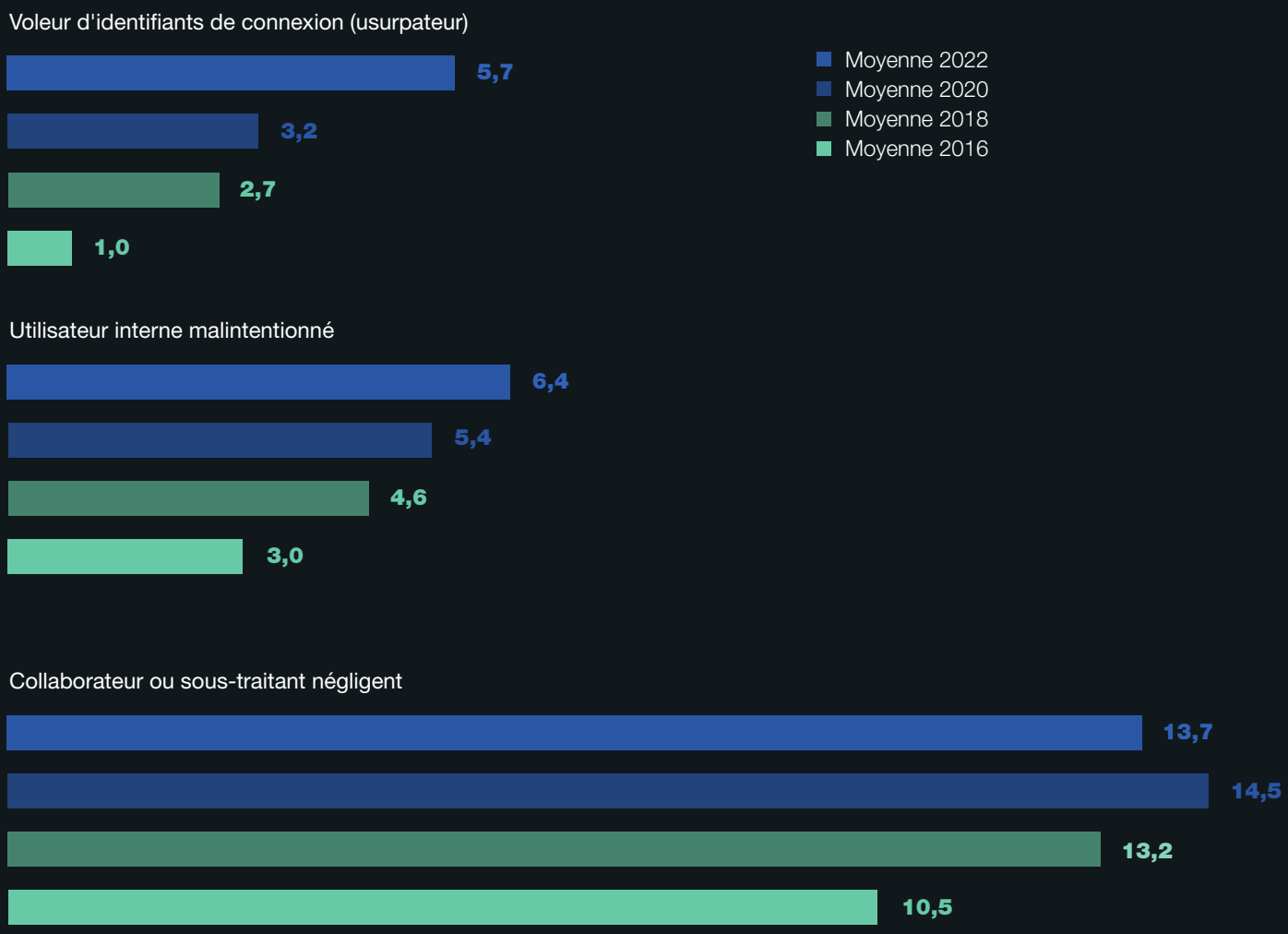


FIGURE 6.

Fréquence pour les trois profils d'utilisateurs internes

Le nombre moyen de vols d'identifiants de connexion a presque doublé. Comme le montre la figure 6, le nombre de vols d'identifiants de connexion est passé de 3,2 incidents en moyenne en 2020 à 5,7 incidents cette année. Le nombre d'incidents imputables aux utilisateurs internes malintentionnés est quant à lui passé de 5,4 à 6,4[1]. Enfin, le nombre d'incidents dus à la négligence d'un collaborateur ou d'un sous-traitant a légèrement reculé, passant de 14,5 à 13,7.



1 Les données de 2016 concernent uniquement des entreprises basées aux États-Unis. Les données de 2022 couvrent l'Amérique du Nord, l'Europe, le Moyen-Orient et l'Afrique, et l'Asie-Pacifique. Nous pensons toutefois que les données sont comparables, car les entreprises américaines ayant participé à l'étude de 2016 étaient des multinationales.

FIGURE 7.

Fréquence des incidents d'origine interne par entreprise

La fréquence des incidents par entreprise a bondi. La figure 7 montre la fréquence consolidée moyenne par entreprise des incidents imputables à un collaborateur/sous-traitant négligent, à un utilisateur interne malintentionné ou à un voleur d'identifiants de connexion. Selon l'étude 2022, 67 % des entreprises subissent entre 21 et plus de 40 incidents par an, contre 60 % en 2020 et 53 % en 2018.

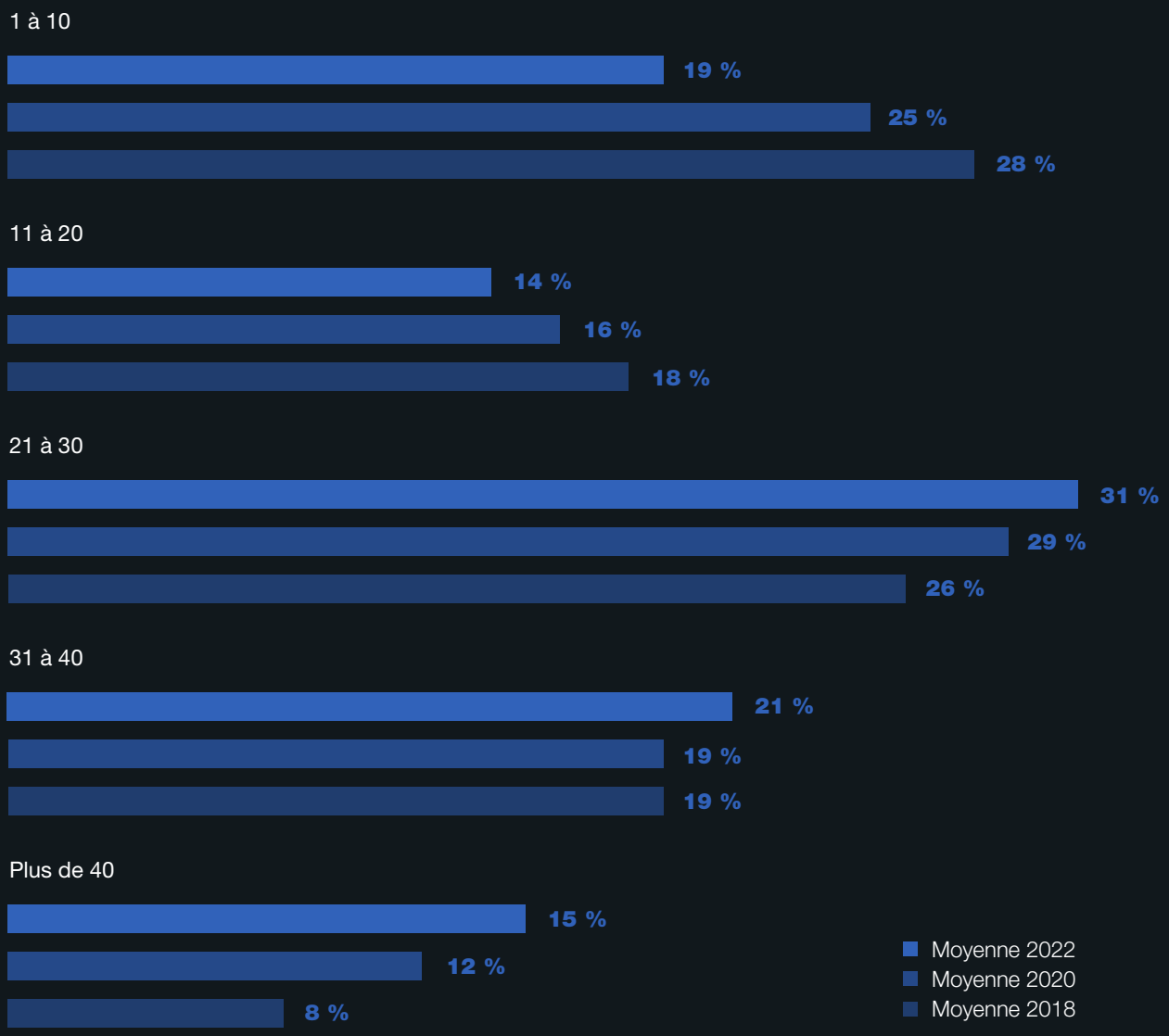


FIGURE 8.

Fréquence moyenne des incidents pour les trois profils par région

Les entreprises du Moyen-Orient et d'Afrique ont enregistré le plus d'incidents d'origine interne, tandis que les entreprises d'Asie-Pacifique sont celles qui en ont subi le moins. La figure 8 montre la fréquence des incidents d'origine interne dans les quatre régions couvertes par l'étude. Toutes régions confondues, la négligence d'un collaborateur ou d'un sous-traitant est la cause la plus fréquente des incidents d'origine interne. Les entreprises d'Amérique du Nord et du Moyen-Orient et d'Afrique sont les plus susceptibles d'être la cible d'un vol d'identifiants de connexion.

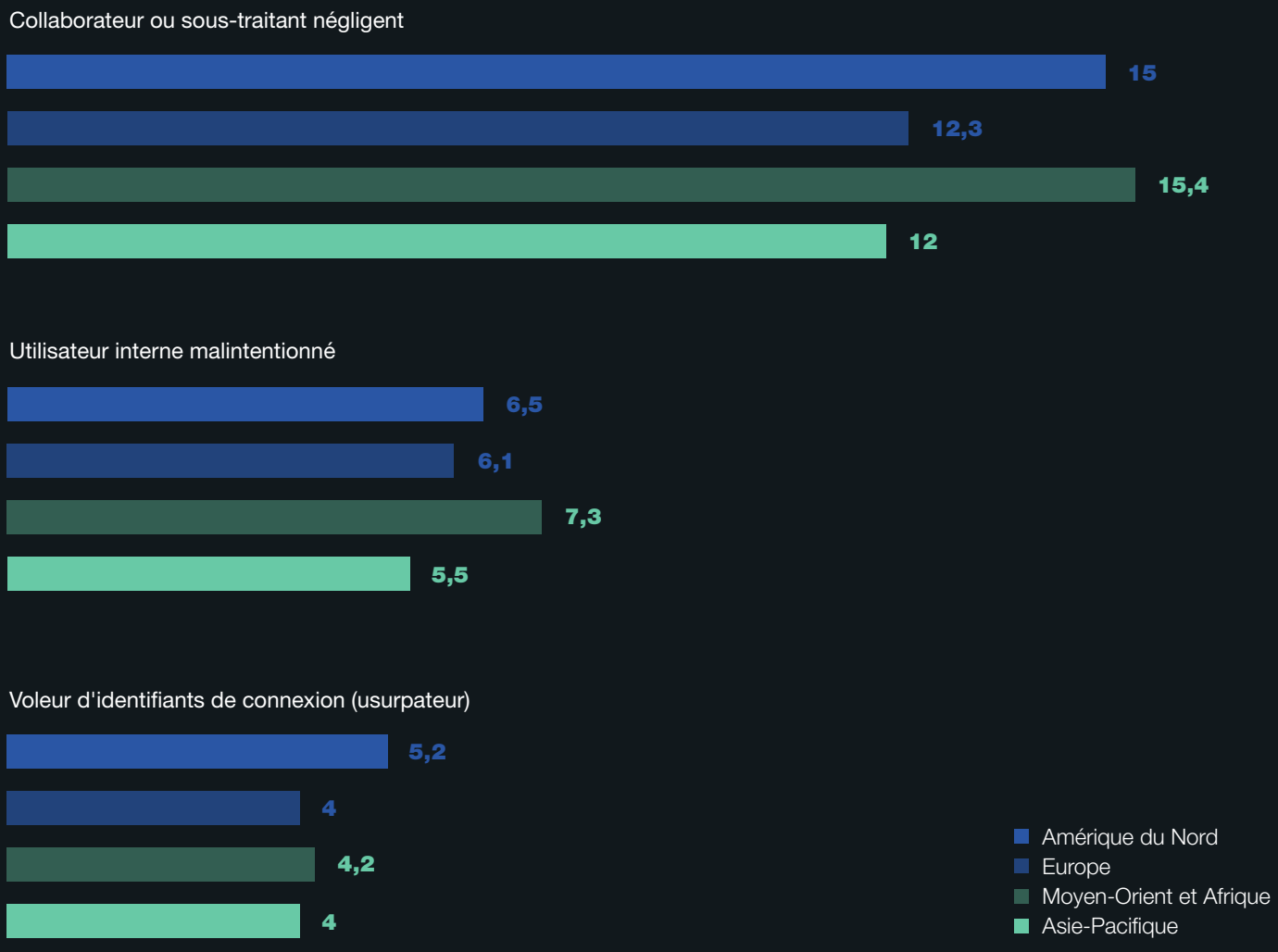


FIGURE 9.

Graphique en nuage de points des incidents d'origine interne par entreprise

La figure 9 présente un graphique en nuage de points des incidents d'origine interne par entreprise. Sur les 278 entreprises participantes, 152 (55 %) ont enregistré un coût total moyen inférieur ou égal à la moyenne de 15,4 millions de dollars au cours des 12 derniers mois. Les 125 entreprises restantes (45 %) ont dépassé cette moyenne. Ce résultat laisse entendre que la répartition est légèrement inégale.

n = 278 entreprises

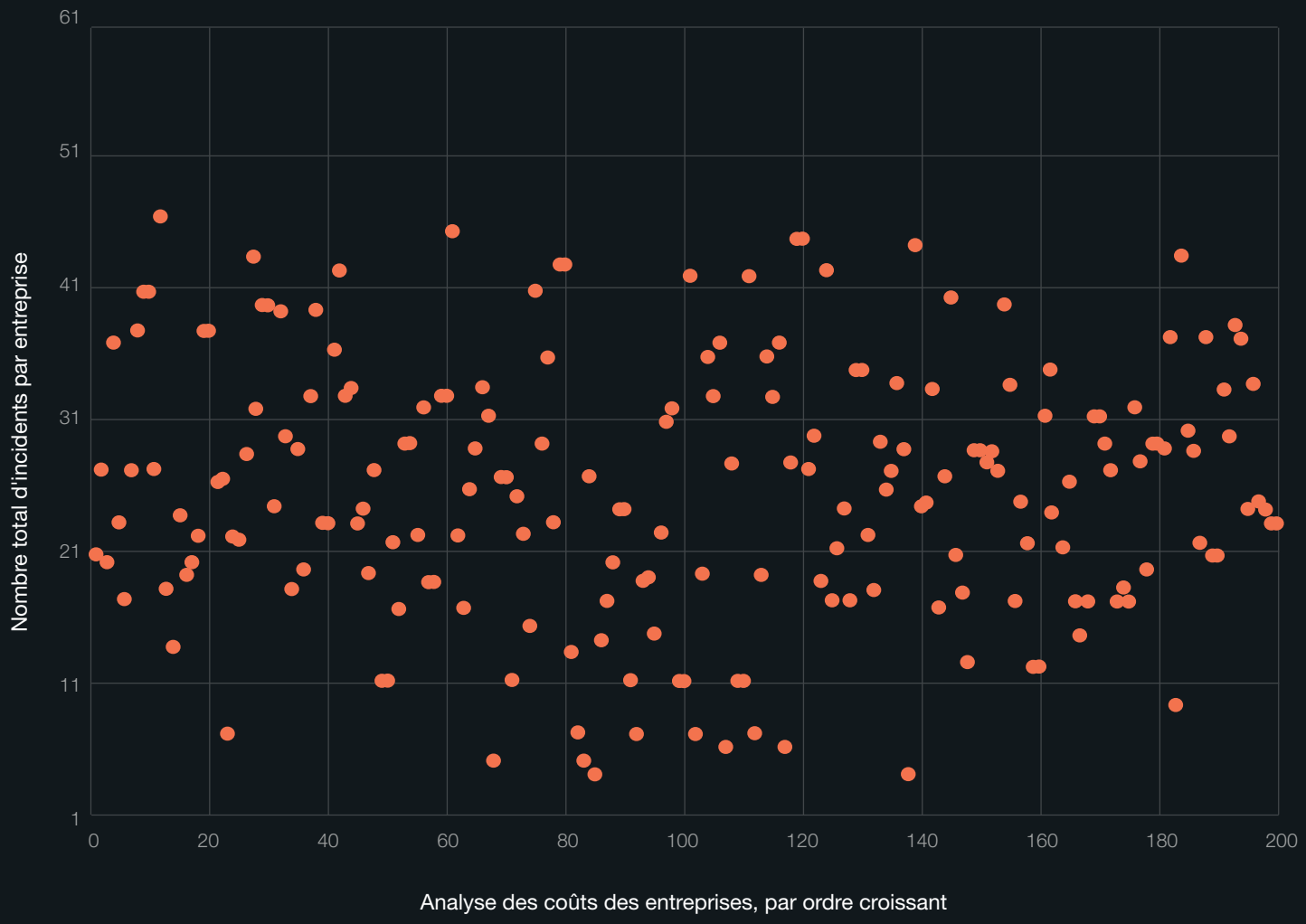


FIGURE 10.

Répartition en % des incidents d'origine interne en fonction du délai de confinement

Le confinement d'un incident de sécurité d'origine interne nécessite en moyenne 85 jours. D'après la figure 10, le délai de confinement moyen des incidents d'origine interne au sein de notre échantillon de référence est de 85 jours. Seuls 12 % des incidents ont été confinés en moins de 30 jours.

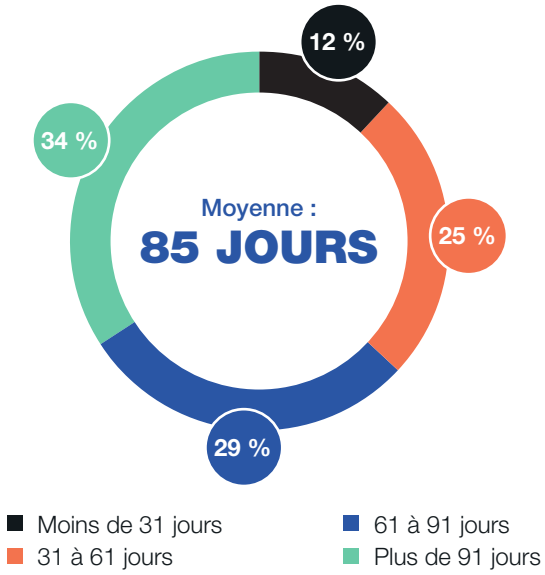


TABLEAU 1.

Activités et outils permettant de réduire les menaces internes

D'après les entretiens que nous avons réalisés, les trois technologies les plus à même de réduire les coûts sont la prévention des fuites de données, la gestion des accès avec privilèges et l'analyse du comportement des utilisateurs et des entités, comme le montre le tableau 1.

Plusieurs réponses possibles

TECHNOLOGIES UTILISÉES POUR RÉDUIRE LE COÛT DES TROIS CAUSES PREMIÈRES DE RISQUES INTERNES	%
Prévention des fuites de données (DLP)	64 %
Gestion des accès avec privilèges (PAM)	60 %
Analyse du comportement des utilisateurs et des entités (UEBA)	57 %
Gestion des événements et des informations de sécurité (SIEM)	53 %
Détection et réponse aux incidents pour endpoints (EDR)	50 %
Gestion des menaces internes (ITM)	41 %
Autre (veuillez préciser)	3 %
Total	**328 %**

LE COÛT DES INCIDENTS D'ORIGINE INTERNE

FIGURE 11.

Pourcentage des coûts liés aux incidents d'origine interne par conséquence pour l'entreprise

Les perturbations et les temps d'arrêt, ainsi que les technologies, représentent les coûts les plus élevés en matière de gestion des incidents d'origine interne. La figure 11 montre la ventilation en % des coûts liés aux incidents d'origine interne imputables aux collaborateurs négligents, aux utilisateurs internes malintentionnés et aux voleurs d'identifiants de connexion, selon sept catégories de coûts. Les deux catégories de coûts les plus importantes sont les conséquences de la perturbation des activités en raison de la baisse de productivité des collaborateurs/utilisateurs (23 % du coût total) et les technologies, qui comprennent la valeur amortie et les licences pour le matériel et les logiciels déployés en réponse à des incidents d'origine interne (21 %).

Les coûts liés aux processus incluent les activités des systèmes de gouvernance et de contrôle en réaction à des menaces ou des attaques. Les frais généraux incluent un large éventail de coûts divers encourus pour le personnel d'assistance et l'infrastructure de sécurité informatique.

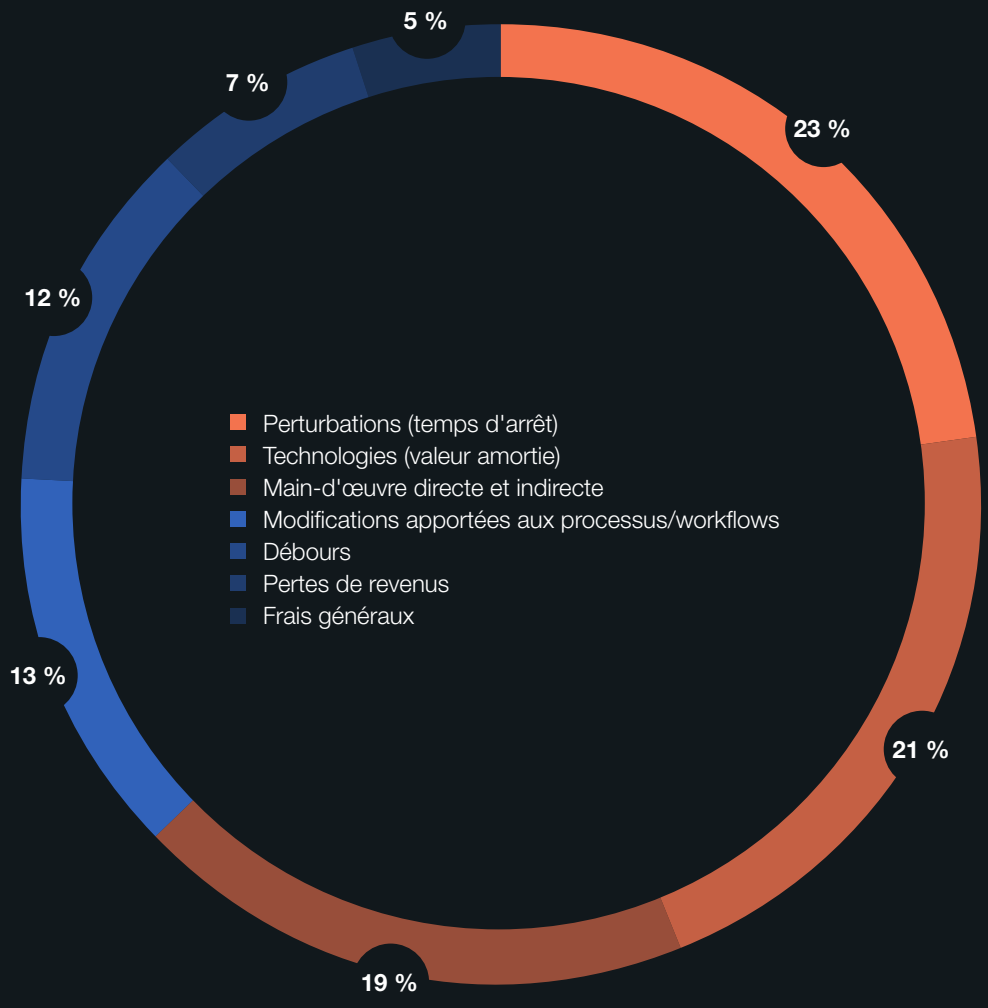


FIGURE 12.

Incidents d'origine interne selon l'effectif (taille de l'entreprise), par ordre croissant

PLUS L'ENTREPRISE EST GRANDE, PLUS ELLE EST VICTIME D'INCIDENTS D'ORIGINE INTERNE.

La figure 12 montre la répartition des incidents d'origine interne en fonction de l'effectif ou de la taille des entreprises participantes, par ordre croissant. La pente ascendante laisse entendre que la fréquence des incidents d'origine interne est positivement corrélée à la taille de l'entreprise. Cette corrélation est d'autant plus flagrante pour les entreprises de plus grande taille.

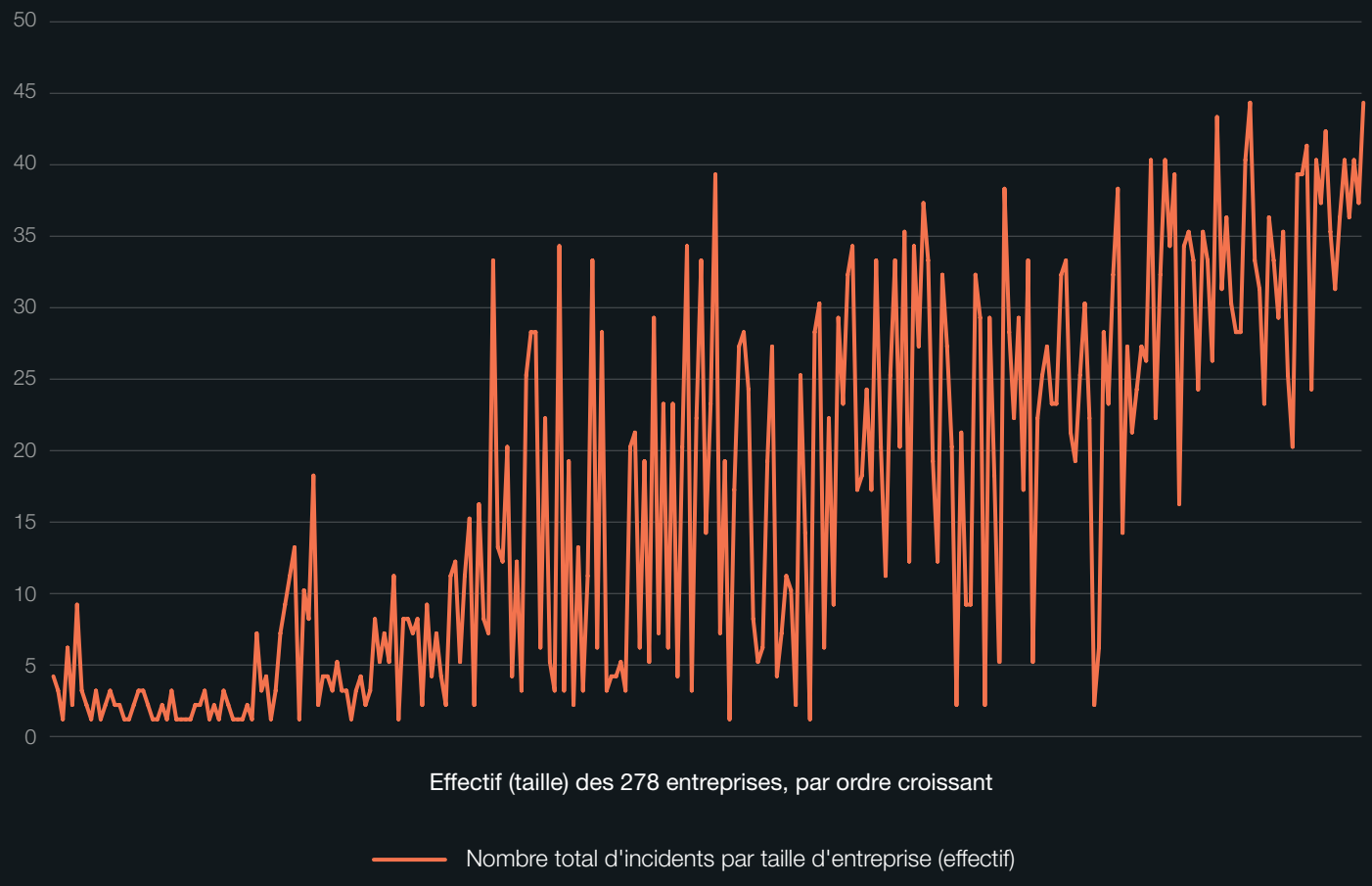


TABLEAU 2.

Coût annuel moyen par incident pour les trois types d'incidents

Le vol d'identifiants de connexion demeure le type d'incident de sécurité d'origine interne le plus coûteux. Le tableau 2 présente le coût moyen par incident, le nombre moyen d'incidents et le coût annualisé moyen. Comme vous pouvez le voir, la négligence d'un collaborateur ou d'un sous-traitant est la cause la plus fréquente des incidents d'origine interne. Cependant, le coût moyen pour ce type d'incident est bien inférieur à celui des vols d'identifiants de connexion et des incidents causés par des utilisateurs internes malintentionnés.

Le coût des incidents imputables aux utilisateurs internes malintentionnés a enregistré une hausse continue et régulière entre 2018 et 2020, passant de 614 192 à 755 761 dollars, mais a ensuite diminué pour atteindre 648 062 dollars cette année. Le nombre moyen de vols d'identifiants de connexion a considérablement augmenté depuis 2018, tandis que le coût moyen de la correction de ces incidents s'élève à 804 997 dollars cette année.

PROFILS 2018	COÛT MOYEN PAR INCIDENT	NOMBRE MOYEN D'INCIDENTS PAR AN	COÛT ANNUALISÉ MOYEN
Collaborateur ou sous-traitant négligent	277 557 USD	13,2	3 663 752 USD
Utilisateur interne malintentionné	614 192 USD	4,6	2 825 283 USD
Voleur d'identifiants de connexion (usurpateur)	672 112 USD	2,7	1 814 702 USD
			8 303 737 USD

PROFILS 2020			
Collaborateur ou sous-traitant négligent	317 111 USD	14,9	4 724 954 USD
Utilisateur interne malintentionné	755 761 USD	5,4	4 081 109 USD
Voleur d'identifiants de connexion (usurpateur)	871 686 USD	3,2	2 789 395 USD
			11 595 458 USD

PROFILS 2022			
Collaborateur ou sous-traitant négligent	484 931 USD	13,7	6 643 555 USD
Utilisateur interne malintentionné	648 062 USD	6,4	4 147 597 USD
Voleur d'identifiants de connexion (usurpateur)	804 997 USD	5,7	4 588 483 USD
			15 378 635 USD

En millions USD

ANALYSE DES COÛTS

CETTE ÉTUDE EXAMINE LES PRINCIPALES ACTIVITÉS LIÉES AUX PROCESSUS QUI GÉNÈRENT UNE SÉRIE DE DÉPENSES ET DE COÛTS ASSOCIÉS À LA RÉPONSE DES ENTREPRISES AUX INCIDENTS D'ORIGINE INTERNE.

Les sept centres de coûts utilisés dans ce rapport sont définis comme suit[2] :

- **Surveillance :** activités permettant à une entreprise de détecter raisonnablement et d'éventuellement empêcher les incidents ou attaques d'origine interne. Cela inclut les coûts (frais généraux) associés à certaines technologies permettant d'améliorer l'atténuation des risques ou la détection précoce des menaces.
- **Investigations :** activités nécessaires à l'identification précise de la source, de la portée et de l'ampleur d'un ou de plusieurs incidents.
- **Remontée des problèmes :** activités réalisées pour sensibiliser les principales parties prenantes de l'entreprise aux incidents survenus. Cela inclut les mesures prises pour organiser une réponse initiale de la direction.
- **Réponse aux incidents :** activités liées à la formation et à l'implication de l'équipe de réponse aux incidents. Cela inclut les mesures prises pour élaborer une réponse finale de la direction.
- **Confinement :** activités visant à empêcher les incidents ou les attaques d'origine interne ou à limiter leur gravité. Cela inclut la mise hors service des applications et des endpoints vulnérables.
- **Analyse ex post :** activités permettant à l'entreprise de réduire les incidents et attaques d'origine interne à venir. Cela inclut les mesures prises pour communiquer avec les principales parties prenantes au sein et en dehors de l'entreprise, notamment l'élaboration de recommandations pour réduire les dégâts potentiels.
- **Application de mesures correctives :** activités associées à la réparation et à la correction des systèmes et des processus métier fondamentaux de l'entreprise. Cela inclut la restauration des actifs informationnels et de l'infrastructure informatique ayant subi des dommages.

2 Les coûts internes sont extrapolés en utilisant le temps de main-d'œuvre comme indicateur des coûts directs et indirects. Cette méthode permet également d'allouer une composante « frais généraux » aux coûts fixes, notamment pour les investissements pluriannuels dans les technologies.

TABLEAU 3.

Tendance moyenne des coûts par incident pour les sept centres de coûts

Le confinement des incidents de sécurité d'origine interne est un poste de dépenses conséquent pour les entreprises. Comme nous l'avons mentionné précédemment, le délai moyen de confinement d'un incident est passé de 77 à 85 jours depuis la dernière étude. Le tableau 3 présente le coût moyen pour les trois types d'incidents d'origine interne et les sept centres de coûts. Comme nous l'avons expliqué, les investigations et le confinement de l'incident constituent les centres de coûts les plus onéreux, tandis que l'analyse ex post et la remontée des problèmes sont les moins onéreux. Les coûts des activités ont bondi de 80 % depuis 2016.

CENTRES DE COÛTS	2016	2018	2020	2022
Surveillance	9 620 USD	12 634 USD	22 124 USD	35 080 USD
Investigations	41 461 USD	78 398 USD	103 798 USD	128 056 USD
Remontée des problèmes	8 919 USD	12 542 USD	21 805 USD	32 228 USD
Réponse aux incidents	66 371 USD	91 263 USD	118 317 USD	120 391 USD
Confinement	122 796 USD	173 161 USD	211 553 USD	184 548 USD
Analyse ex post	8 498 USD	11 491 USD	19 480 USD	26 563 USD
Application de mesures correctives	91 397 USD	138 532 USD	147 776 USD	119 131 USD
Total	**349 152 USD**	**517 921 USD**	**644 853 USD**	**645 997 USD**

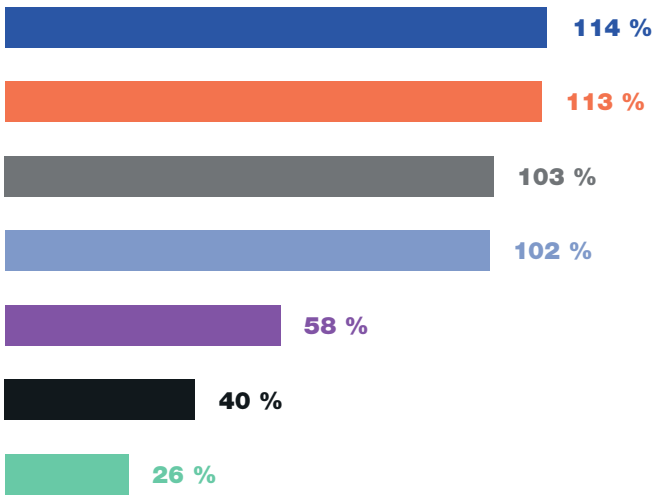


FIGURE 13.

Augmentation nette en % du coût annuel moyen entre 2016 et 2022

Depuis 2016, les coûts de réponse aux incidents d'origine interne ont grimpé en flèche. Comme le montre la figure 13, la surveillance et la remontée des problèmes sont les centres de coûts qui ont le plus augmenté depuis 2016 (114 et 113 %, respectivement). L'augmentation annuelle moyenne des coûts des activités s'élève à 80 % depuis 2016.

TABLEAU 4.

Coût de sept activités par type d'incident en 2022

Le confinement des incidents d'origine interne représente le pourcentage le plus élevé du coût total pour les incidents imputables aux voleurs d'identifiants de connexion (imposteurs) et aux utilisateurs internes négligents. Le tableau 4 présente le coût annualisé moyen des sept activités en fonction du type d'incident.

CENTRES DE COÛTS 2022	COLLABORATEUR OU SOUS-TRAITANT NÉGLIGENT	UTILISATEUR INTERNE MAL-INTENTIONNÉ	VOLEUR D'IDENTIFIANTS DE CONNEXION (USURPATEUR)	COÛT MOYEN
Surveillance	34 517 USD	34 511 USD	36 213 USD	35 080 USD
Investigations	121 511 USD	126 545 USD	136 111 USD	128 056 USD
Remontée des problèmes	29 121 USD	31 112 USD	36 451 USD	32 228 USD
Réponse aux incidents	112 345 USD	119 711 USD	129 118 USD	120 391 USD
Confinement	151 311 USD	149 814 USD	252 518 USD	184 548 USD
Analyse ex post	23 515 USD	26 733 USD	29 441 USD	26 563 USD
Application de mesures correctives	12 611 USD	159 636 USD	185 145 USD	119 131 USD
Total	**484 931 USD**	**648 062 USD**	**804 997 USD**	**645 997 USD**

FIGURE 14.

Coût moyen des activités par incident pour les trois types d'incidents en 2022

Le vol d'identifiants de connexion enregistre le coût moyen des activités le plus élevé. La figure 14 montre la différence considérable entre le coût des activités pour les incidents dus à la négligence d'un collaborateur ou d'un sous-traitant et pour les vols d'identifiants de connexion.

En USD

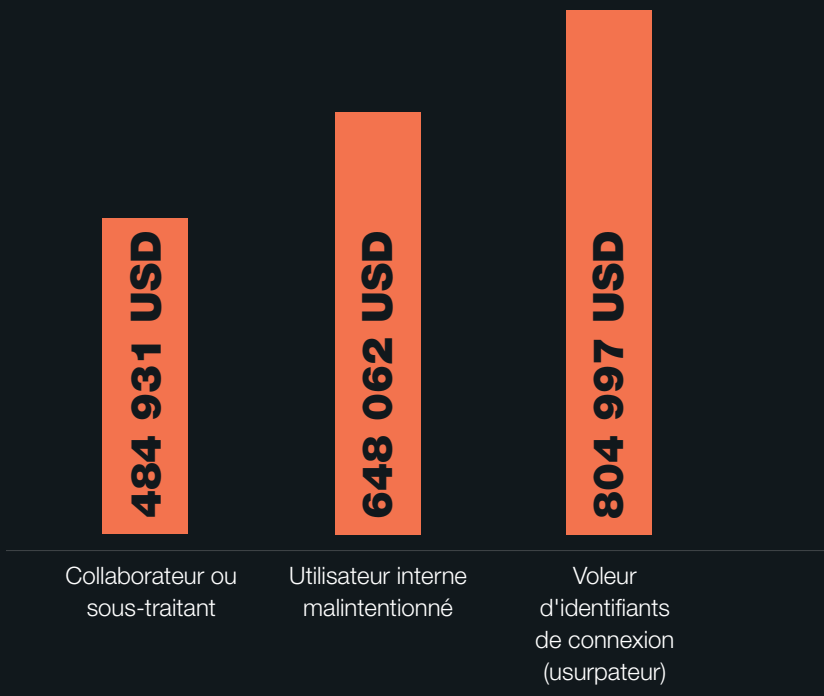


FIGURE 15.

Coût moyen des activités par région

LES ENTREPRISES NORD-AMÉRICAINES DÉPENSENT PLUS QUE LE COÛT MOYEN POUR LA GESTION DES MENACES INTERNES.

Le coût moyen total de la résolution des menaces internes sur une période de 12 mois s'élève à 15,4 millions de dollars environ. Comme le montre la figure 15, les entreprises nord-américaines ont enregistré le coût total le plus élevé, à savoir 17,53 millions de dollars. Elles sont suivies par les entreprises européennes, avec 15,44 millions de dollars. Le coût moyen pour les entreprises d'Asie-Pacifique s'est révélé très inférieur au coût total moyen pour l'ensemble des 278 entreprises, avec 11,90 millions de dollars.

Moyenne = 15,38 millions USD

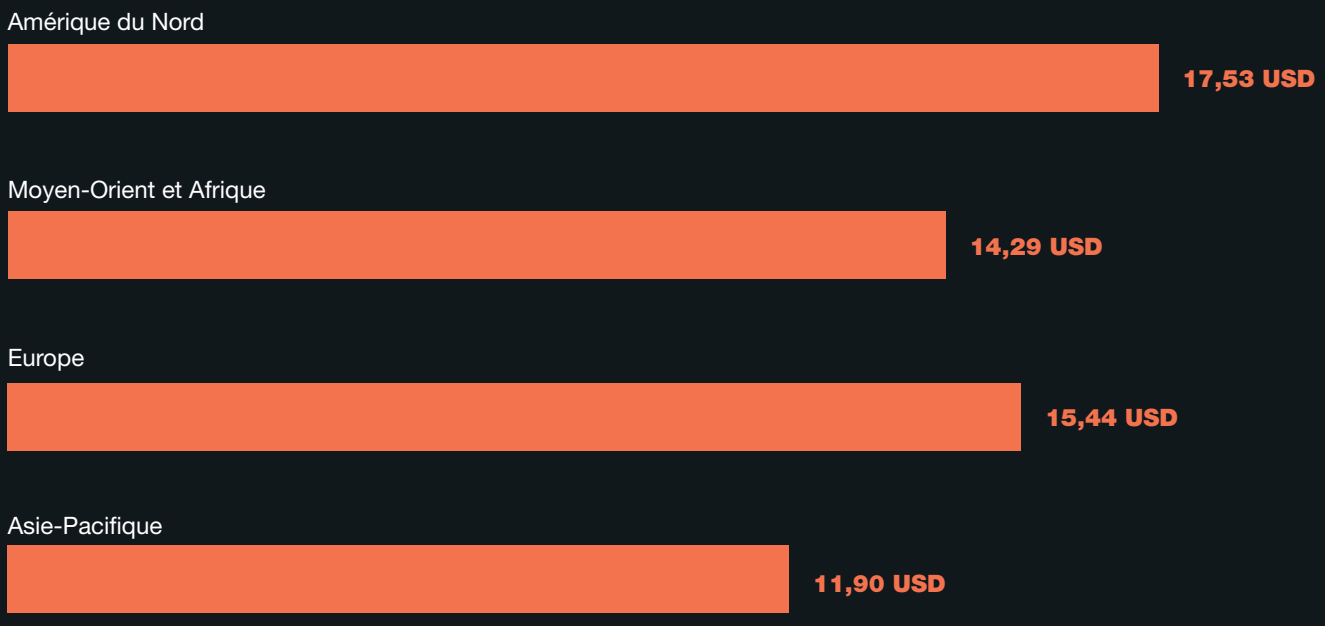


FIGURE 16.

Coût moyen des activités selon l'effectif

La résolution des incidents d'origine interne est un poste de dépenses conséquent pour les grandes entreprises. Comme le montre la figure 16, les entreprises comptant entre 25 000 et 75 000 collaborateurs dépensent beaucoup plus (23 millions de dollars en moyenne) pour résoudre un incident.

Moyenne = 15,38 millions USD

Vue consolidée pour les trois profils

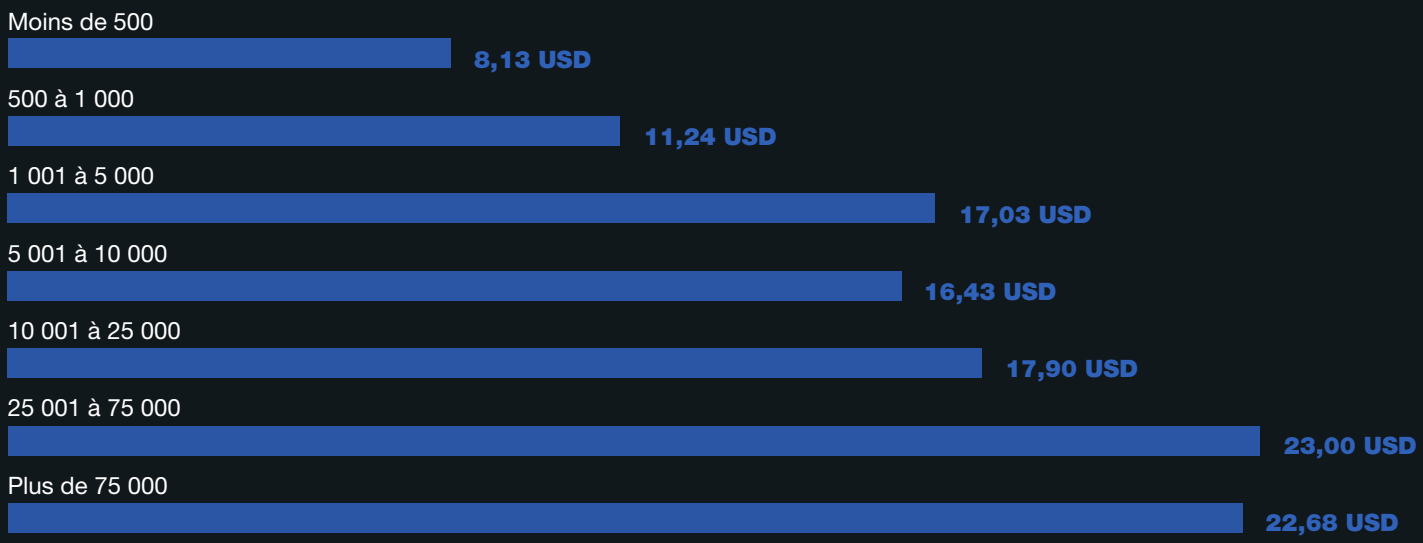


FIGURE 17.

Coût moyen des activités en fonction du délai de confinement des incidents

Plus le délai de confinement est court, moins le coût des activités est élevé. Le coût annualisé total des incidents d'origine interne semble être positivement corrélé à leur délai de confinement. Comme le montre la figure 17, les incidents dont le confinement a pris plus de 90 jours ont enregistré le coût total moyen le plus élevé par an (17,19 millions de dollars). À l'inverse, les incidents dont le confinement a pris moins de 30 jours ont affiché le coût total le plus faible (11,23 millions de dollars). Le coût annuel moyen s'élève à 15,38 millions de dollars.

Moyenne = 15,38 millions USD

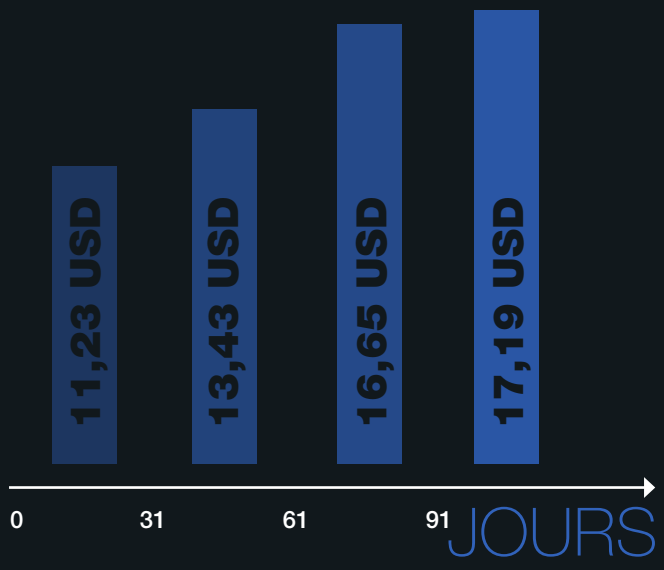


FIGURE 18.

Coût en % des incidents d'origine interne par activité

Le confinement représente un tiers de tous les coûts. Le graphique circulaire ci-dessous montre le coût en % des sept activités. D'après la figure 18, le confinement représente 29 % du coût annualisé total des incidents d'origine interne. Les activités liées aux investigations et à la réponse aux incidents représentent respectivement 20 et 19 % du coût total.

n = 278 entreprises

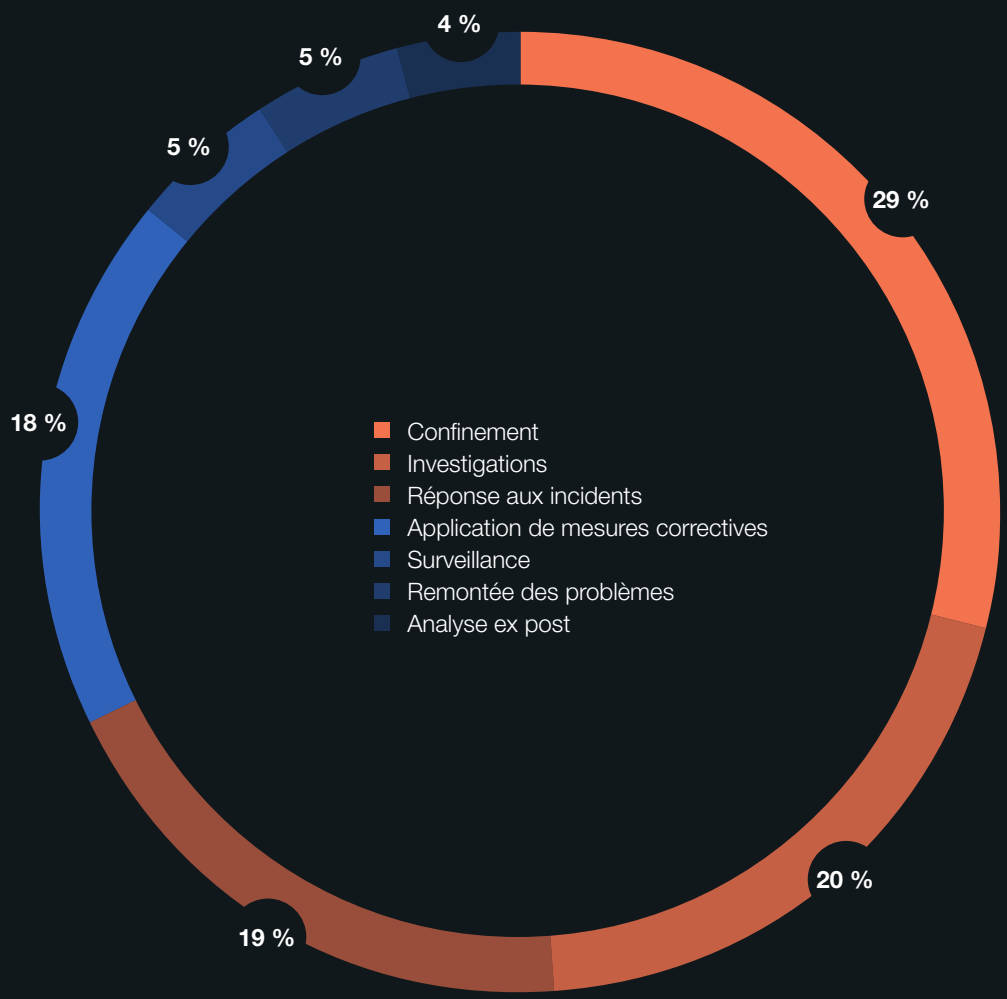


FIGURE 19.

Coût annualisé des activités par secteur

LES COÛTS DES ACTIVITÉS SONT PLUS ÉLEVÉS POUR LES SERVICES FINANCIERS ET LES SERVICES.

D'après la figure 19, le coût moyen des activités s'élève à 21,25 millions de dollars pour les services financiers et à 18,65 millions de dollars pour les services, des chiffres bien supérieurs à la moyenne de 15,4 millions de dollars. Les services incluent les cabinets comptables, d'avocats et de conseil.

En millions USD

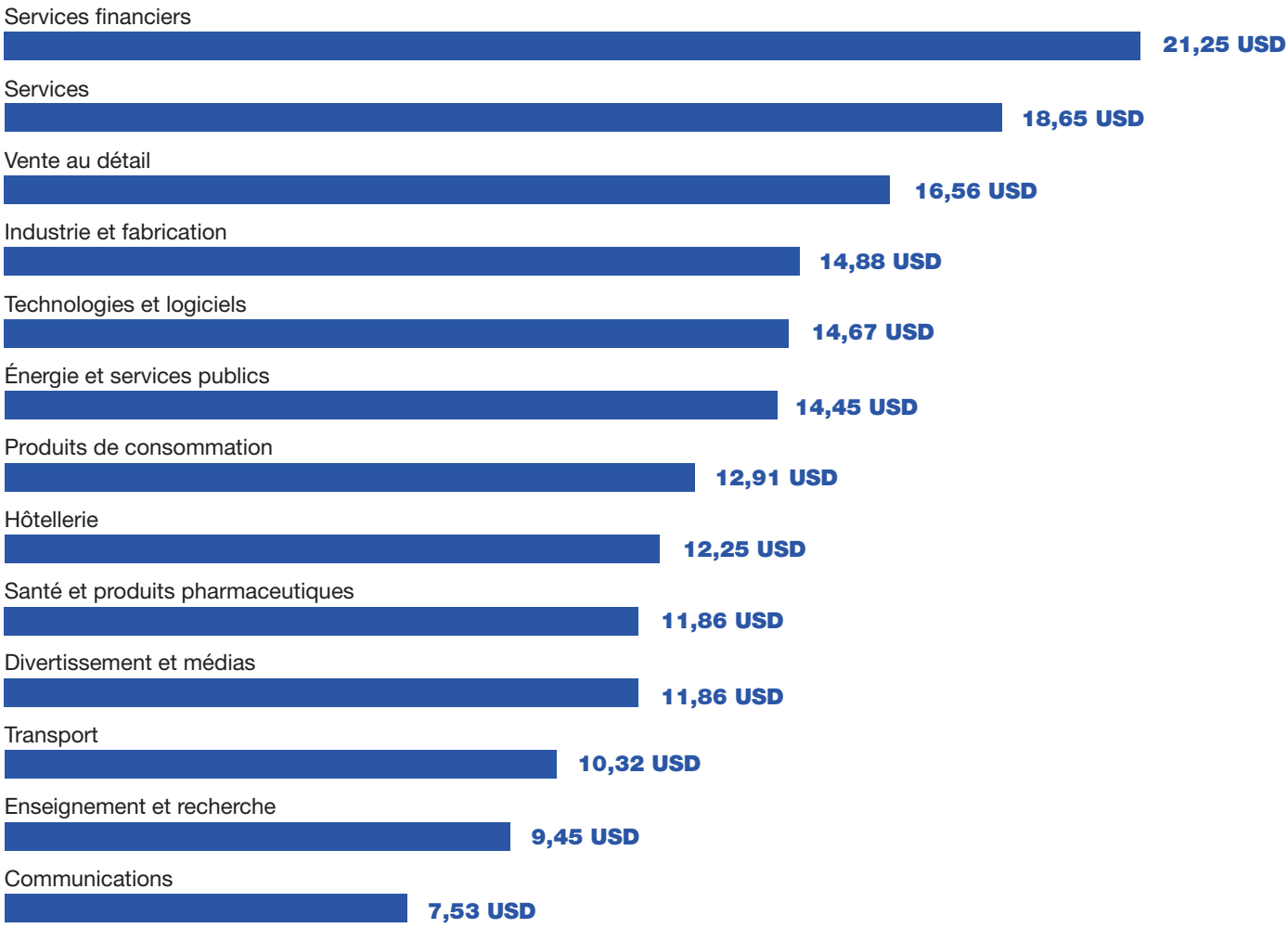
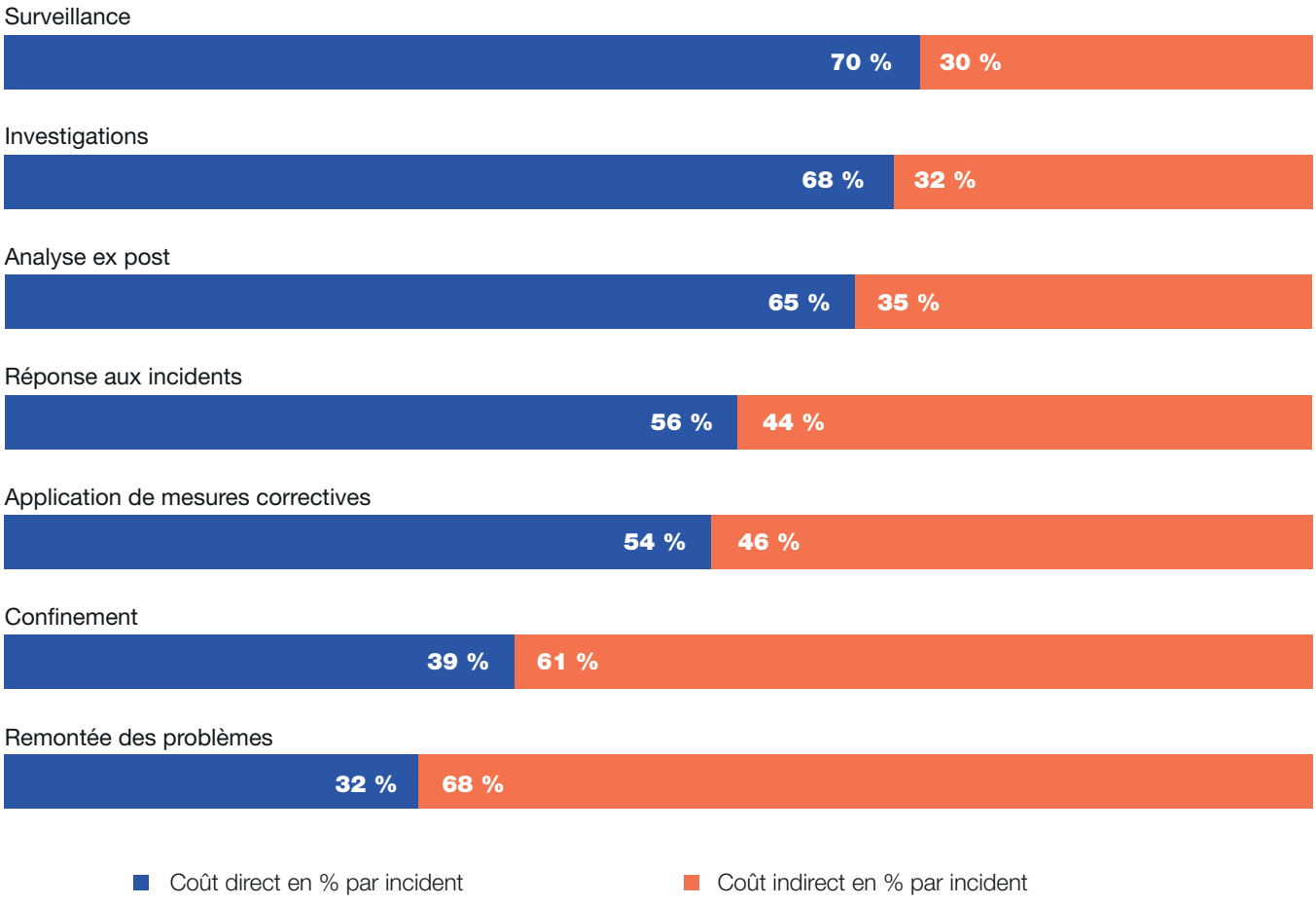


FIGURE 20.

Pourcentage de coûts directs et indirects par activité

Les entreprises ont été invitées à estimer les coûts directs et indirects d'une activité donnée. La figure 20 montre le pourcentage de coûts directs et indirects[3] pour les sept centres de coûts liés aux activités internes. Comme vous pouvez le voir, les coûts liés à la surveillance et aux investigations représentent le pourcentage de coûts directs le plus élevé (70 et 68 %, respectivement). Le confinement et la remontée des problèmes enregistrent quant à eux le pourcentage de coûts indirects le plus élevé (61 et 68 %, respectivement).

Vue consolidée pour les trois profils



3 Les coûts directs correspondent aux dépenses consenties pour réaliser une activité donnée, tandis que les coûts indirects désignent le temps, les efforts et autres ressources engagés pour résoudre un incident.

EN PLUS DE DÉTERMINER LE COÛT DES MENACES INTERNES POUR LES ENTREPRISES DANS LE CADRE DE L'ÉTUDE, NOUS AVONS INTERROGÉ LES PARTICIPANTS AU SUJET DE LEURS EXPÉRIENCES DE CE TYPE DE MENACES ET DES MESURES QU'ILS PRENNENT POUR RÉDUIRE LES RISQUES.

FIGURE 21.

Quelles sont les menaces internes qui vous préoccupent le plus ?

Parmi tous les types de menaces internes couverts dans cette étude, c'est le vol d'identifiants de connexion qui préoccupe le plus les entreprises. Comme nous l'avons mentionné précédemment, le nombre de vols d'identifiants de connexion a presque doublé depuis la dernière étude. Il s'agit en outre du type d'incident d'origine interne dont la correction coûte le plus cher. 55 % des sondés craignent avant tout qu'un cyberpirate vole les identifiants de connexion d'un collaborateur. Ils sont bien moins nombreux (21 %) à être préoccupés par la négligence des utilisateurs internes.

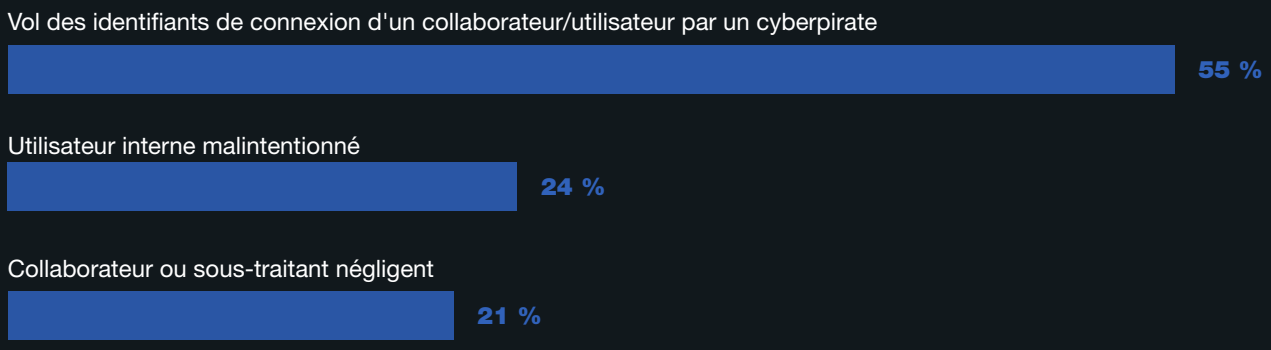


FIGURE 22.

Certains des incidents impliquaient-ils les comportements suivants ?

La plupart des incidents d'origine interne sont causés par des collaborateurs négligents et des voleurs d'identifiants de connexion. Comme le montre la figure 22, 57 % des sondés indiquent que les incidents d'origine interne qu'ils ont subis étaient dus à la négligence d'un collaborateur, tandis que 51 % affirment qu'un cybercriminel externe a volé des données en compromettant les identifiants ou les comptes d'utilisateurs internes.

Plusieurs réponses possibles

FIGURE 23.

Quels vecteurs de fuite de données d'origine interne vous préoccupent le plus ?

Les terminaux IoT vulnérables présentent le risque le plus élevé de fuite de données. La multitude de terminaux IoT utilisés dans les entreprises accroît les risques internes. 63 % des sondés admettent craindre la fuite de données sensibles via des terminaux IoT non gérés. D'autres redoutent que la même chose se produise via le cloud (52 %) et le réseau (51 %), comme le montre la figure 23.

Plusieurs réponses possibles

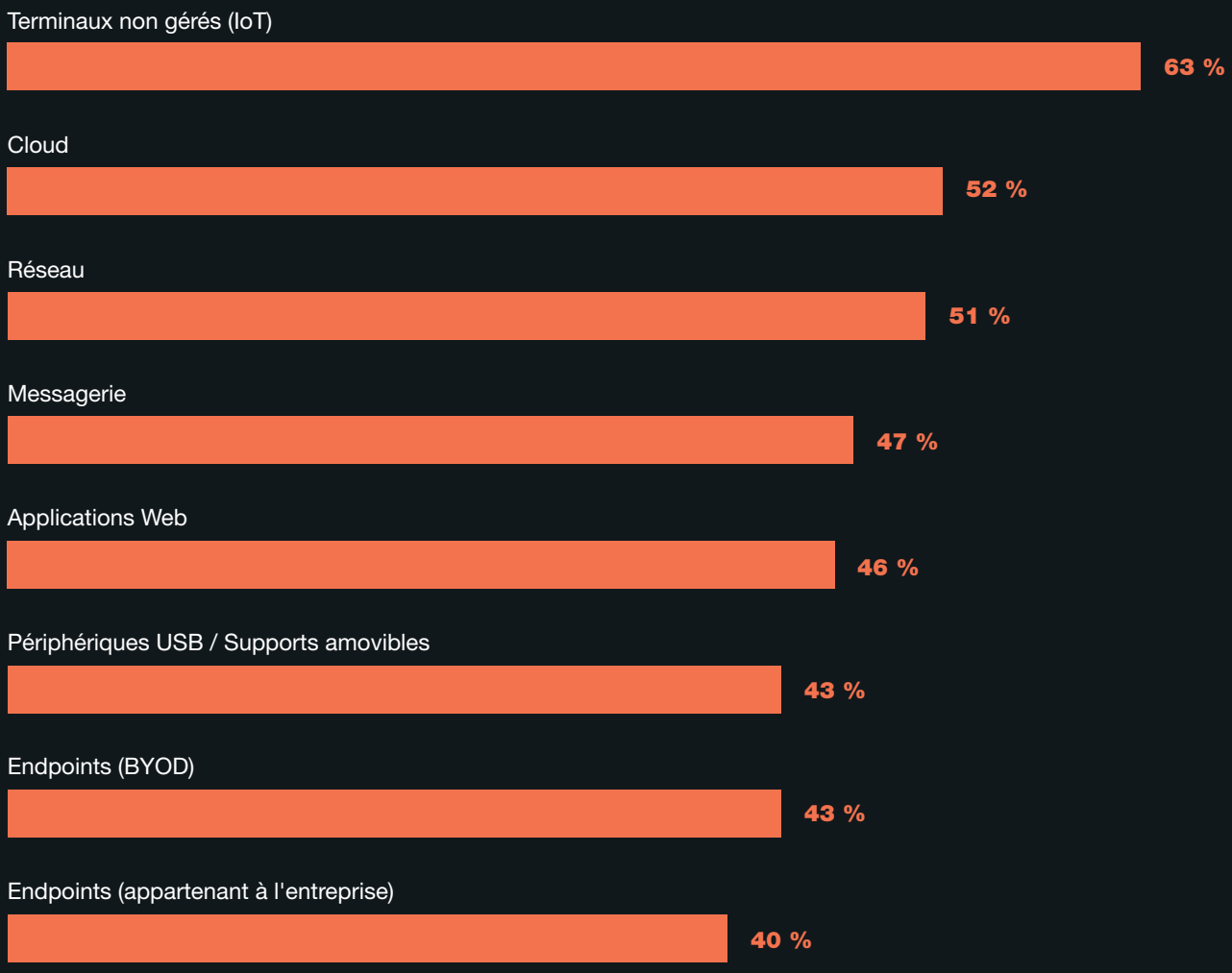


FIGURE 24.

Où vos utilisateurs stockent-ils les données sensibles de votre entreprise, comme les données personnelles, la propriété intellectuelle et autres informations métier stratégiques ?

La plupart des données sensibles se trouvent dans les emails des collaborateurs. D'après la figure 24, 65 % des sondés affirment que les collaborateurs stockent les données les plus sensibles de leur entreprise, comme les données personnelles, la propriété intellectuelle et autres informations métier stratégiques, dans leurs emails. Les programmes de formation et de sensibilisation sont indispensables pour combattre la négligence des collaborateurs lorsqu'ils envoient et reçoivent des informations sensibles.

Trois réponses possibles

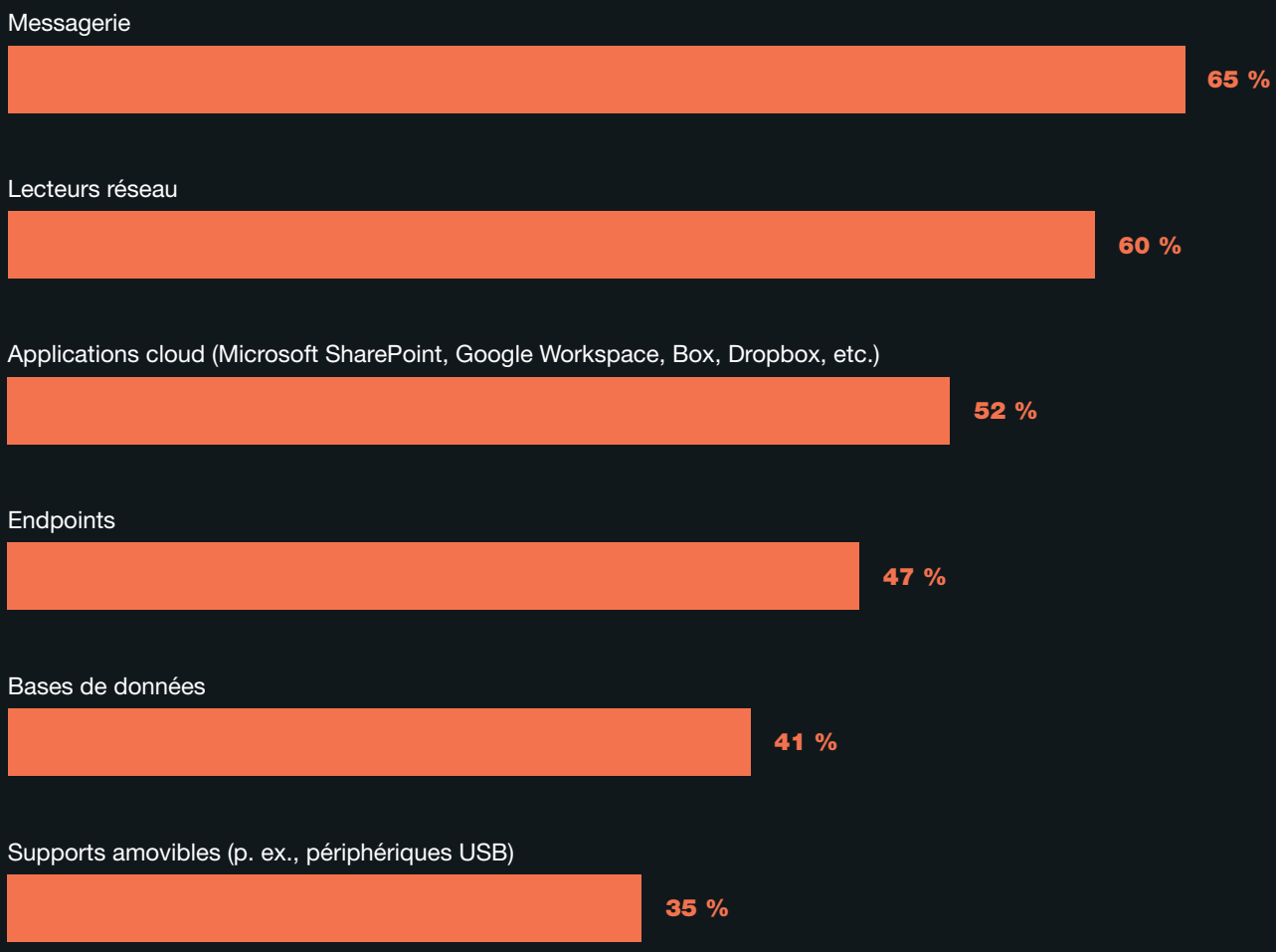


FIGURE 25.

Comment vos utilisateurs communiquent-ils et collaborent-ils avec des collègues et des tiers ?

Comme le montre la figure 25, les outils de chat professionnels et la messagerie sont les principales méthodes employées pour communiquer et collaborer en interne et avec des tiers, selon 61 et 52 % des sondés.

Trois réponses possibles

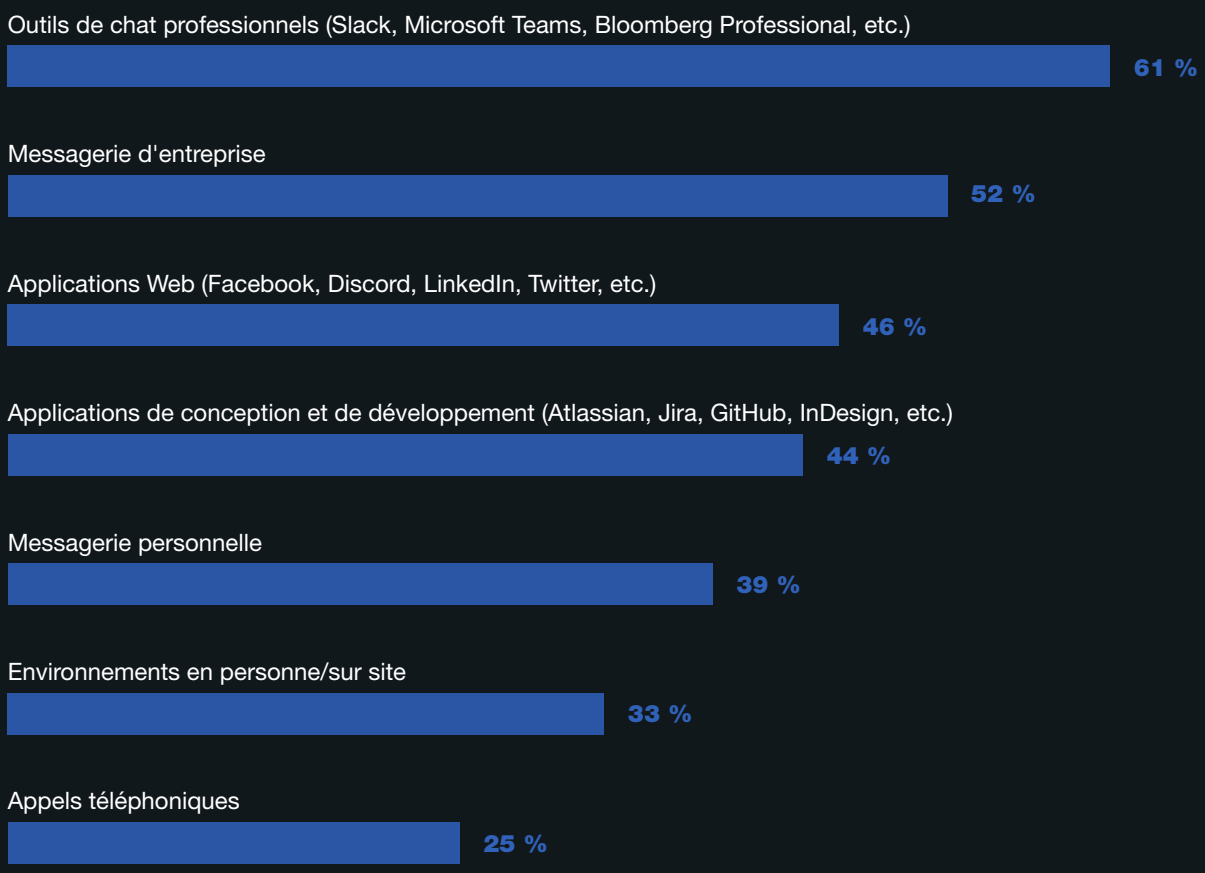


FIGURE 26.

Des utilisateurs internes malintentionnés ont-ils réalisé les activités suivantes dans votre entreprise ?

Les utilisateurs internes malintentionnés se servent de la messagerie d'entreprise pour voler des données sensibles. La figure 26 présente une liste d'activités réalisées par des utilisateurs internes malintentionnés dans les entreprises ayant participé à l'étude. 74 % des sondés déclarent que des utilisateurs internes malintentionnés ont envoyé des données sensibles à des tiers par email, 62 % qu'ils ont recherché des ports ouverts et des vulnérabilités, et 60 % qu'ils ont accédé à des données sensibles sans lien avec leur rôle ou fonction.

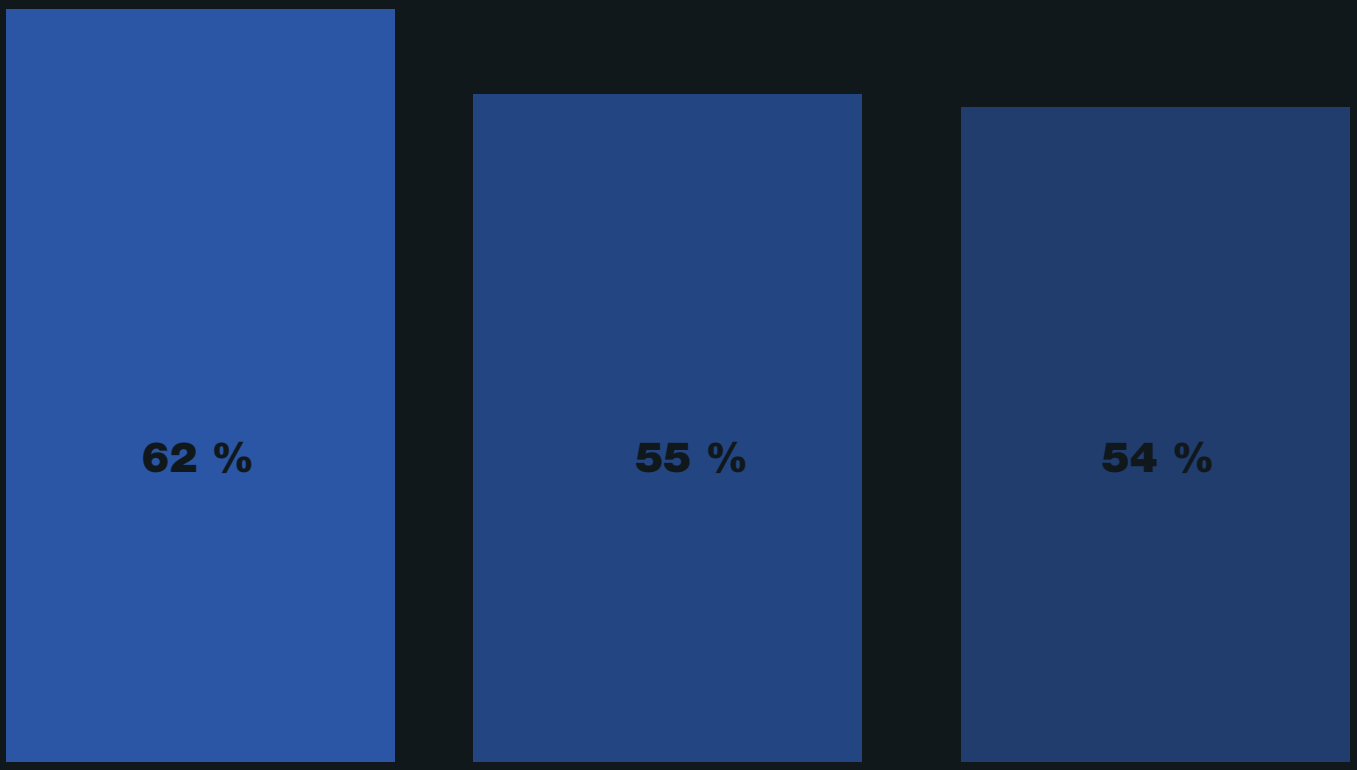
Plusieurs réponses possibles

FIGURE 27.

Quelle est l'importance des technologies avancées pour réduire les menaces internes ?

Face à la multiplication des menaces internes et à l'allongement du délai de confinement, des technologies avancées sont essentielles pour s'en prémunir. D'après la figure 27, les outils de détection des menaces internes grâce à l'analyse du comportement des utilisateurs sont considérés comme indispensables ou très importants pour réduire les menaces internes (62 % des sondés). Ils sont suivis par l'automatisation (55 % des sondés) et par l'intelligence artificielle et l'apprentissage automatique (54 %) pour la prévention, les investigations, la remontée des problèmes, le confinement et la correction des incidents d'origine interne.

Réponses « Indispensables » et « Très importants » combinées



Outils de détection des menaces internes grâce à l'analyse du comportement des utilisateurs

Automatisation pour la prévention, les investigations, la remontée des problèmes, le confinement et la correction des incidents d'origine interne

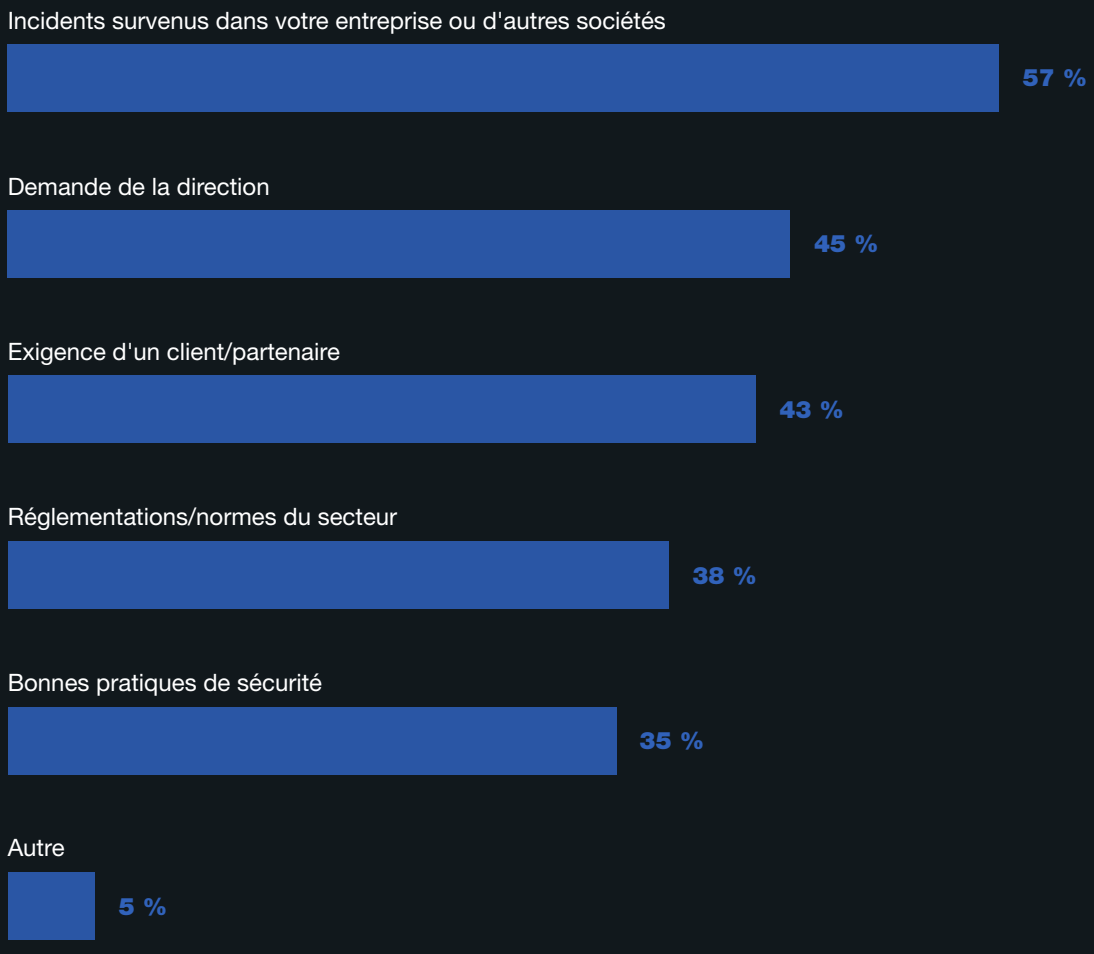
Intelligence artificielle et apprentissage automatique pour la prévention, les investigations, la remontée des problèmes, le confinement et la correction des incidents d'origine interne

FIGURE 28.

Quelle est la principale raison pour laquelle vous avez adopté un programme de gestion des menaces internes ?

Les incidents survenus poussent les entreprises à adopter un programme de gestion des menaces internes. La figure 28 présente les raisons pour lesquelles les entreprises ayant participé à l'étude prennent des mesures pour réduire les menaces internes. Les incidents survenus dont ont été victimes l'entreprise ou d'autres sociétés constituent la principale raison (57 %). Seuls 38 % des sondés indiquent que les réglementations et les normes du secteur sont des raisons d'adopter un programme de gestion des menaces internes.

Plusieurs réponses possibles



CONCLUSIONS

Ces deux dernières années, l'accélération de la transformation numérique a entraîné la prolifération des menaces internes.

De l'utilisation des terminaux personnels à des fins professionnelles à l'adoption généralisée du cloud, les entreprises ont pris conscience que l'approche traditionnelle de la protection des données n'était plus efficace.

Cela souligne l'importance pour les entreprises de mettre en œuvre un programme de gestion des menaces internes (ITM) centré sur les personnes et adapté à l'environnement de télétravail actuel. Un programme ITM efficace favorise la collaboration transversale, notamment entre les équipes informatique, juridique, de RH et de conformité. Il est important de constituer une équipe formée à la fois de représentants techniques et non techniques pour permettre à l'entreprise de bénéficier des trois éléments essentiels d'un programme ITM :

Visibilité

Mettez en œuvre une plate-forme ITM offrant à votre entreprise visibilité et contexte sur les mouvements de données. Vous pourrez ainsi raccourcir vos délais moyens de détection et de réponse. Grâce à une meilleure compréhension des mouvements de données, vous pourrez réduire efficacement le nombre moyen de jours nécessaires au confinement d'un incident d'origine interne.

Cohérence

Évaluez les risques auxquels l'entreprise est exposée, y compris les utilisateurs internes à haut risque, et développez une fonction dédiée aux menaces internes. Cela doit également inclure l'instauration d'un processus cohérent et reproductible permettant de détecter les menaces internes pertinentes en fonction du contexte et de les neutraliser. L'utilisation d'une solution spécialisée dans la gestion des risques internes garantit la mise en place d'un processus cohérent visant à réduire les délais moyens de détection et de réponse.

Transparence

Un processus d'amélioration continue doit être mis en place afin de déterminer les mesures à prendre pour mieux se prémunir des menaces internes. Tirez des enseignements des incidents survenus pour optimiser vos efforts afin de vous adapter plus efficacement aux risques en constante évolution.

Face à la multiplication des menaces internes et à l'allongement du délai de confinement, des technologies avancées sont essentielles pour s'en prémunir. La mise en œuvre d'un programme ITM permettant à votre entreprise d'identifier et de détecter de manière fiable les comportements des utilisateurs et les mouvements de données à risque, ainsi que de répondre aux incidents, est indispensable pour prévenir les fuites de données et réduire les risques internes.

CADRE

L'OBJET DE CETTE ÉTUDE EST DE DONNER UN APERÇU DU COÛT QUE PEUT REPRÉSENTER UNE MENACE INTERNE POUR UNE ENTREPRISE.

Cette étude des coûts est la seule à s'intéresser aux activités liées aux systèmes et aux processus métier fondamentaux qui engendrent une série de dépenses associées à la réponse des entreprises aux incidents dus à la négligence ou à la malveillance d'utilisateurs internes. Dans le cadre de cette étude, un incident d'origine interne est défini comme un événement affectant les données, les réseaux ou les systèmes fondamentaux d'une entreprise. Cette définition englobe également les attaques perpétrées par des acteurs externes (également appelés « usurpateurs ») en vue de dérober les identifiants de connexion de collaborateurs ou d'utilisateurs légitimes.

Nos méthodes de référence visent à faire la lumière sur les expériences réelles et les conséquences des incidents d'origine interne. Les entretiens que nous avons réalisés avec divers collaborateurs d'échelon supérieur de chaque entreprise nous ont permis de répartir les coûts en deux flux de dépenses :

- Les coûts associés à la lutte contre les menaces internes, que nous qualifions de centres de coûts internes
- Les coûts liés aux conséquences des incidents, que nous qualifions d'effets externes de l'événement ou de l'attaque

Nous analysons les centres de coûts internes de manière séquentielle, en commençant par la surveillance du paysage des menaces internes et en terminant par les activités de correction. Sont également inclus les coûts liés aux pertes d'opportunités commerciales et aux perturbations des activités. Pour chaque centre de coûts, nous avons demandé aux personnes interrogées d'estimer les coûts directs, les coûts indirects et le manque à gagner (le cas échéant), définis comme suit :

- **Coûts directs** : débours direct pour entreprendre une activité donnée
- **Coûts indirects** : temps, efforts et autres ressources engagés, autrement que sous la forme d'un débours direct
- **Manque à gagner** : coût résultant de la perte d'opportunités commerciales en raison du préjudice porté à la réputation de l'entreprise suite à l'incident

Les coûts externes tels que la perte d'actifs informationnels, la perturbation des activités, les dommages causés aux équipements et les pertes de revenus ont été calculés à l'aide de méthodes d'estimation des coûts. Les coûts totaux ont été attribués à sept vecteurs de coûts distincts[4].

4 Nous reconnaissons que ces sept catégories de coûts ne sont pas mutuellement indépendantes et qu'elles ne constituent pas une liste exhaustive des centres de coûts des entreprises.

Cette étude examine les principales activités liées aux processus qui génèrent une série de dépenses associées à la réponse des entreprises aux incidents d'origine interne. Les sept centres de coûts internes inclus dans notre cadre sont les suivants[5] :

07

centres de coûts internes

01 **Surveillance :** activités permettant à une entreprise de détecter raisonnablement et d'empêcher éventuellement les incidents ou attaques d'origine interne. Cela inclut les coûts (frais généraux) associés à certaines technologies permettant d'améliorer l'atténuation des risques ou la détection précoce des menaces.

02 **Investigations :** activités nécessaires à l'identification précise de la source, de la portée et de l'ampleur d'un ou de plusieurs incidents.

03 **Remontée des problèmes :** activités réalisées pour sensibiliser les principales parties prenantes de l'entreprise aux incidents survenus. Cela inclut les mesures prises pour organiser une réponse initiale de la direction.

04 **Réponse aux incidents :** activités liées à la formation et à l'implication de l'équipe de réponse aux incidents. Cela inclut les mesures prises pour élaborer une réponse finale de la direction.

05 **Confinement :** activités visant à empêcher les incidents ou les attaques d'origine interne ou à limiter leur gravité. Cela inclut la mise hors service des applications et des endpoints vulnérables.

06 **Analyse ex post :** activités permettant à l'entreprise de réduire les incidents et attaques d'origine interne à venir. Cela inclut les mesures prises pour communiquer avec les principales parties prenantes au sein et en dehors de l'entreprise, notamment l'élaboration de recommandations pour réduire les dégâts potentiels.

07 **Application de mesures correctives :** activités associées à la réparation et à la correction des systèmes et des processus métier fondamentaux de l'entreprise. Cela inclut la restauration des actifs informationnels et de l'infrastructure informatique ayant subi des dommages.

En plus des activités liées aux processus mentionnées ci-dessus, les entreprises font souvent face à des coûts ou conséquences externes à la suite d'un incident. L'étude révèle que les quatre centres de coûts généraux associés à ces conséquences externes sont les suivants :

04

centres de coûts généraux

01 **Coût de la fuite ou du vol d'informations :** fuite ou vol d'informations sensibles et confidentielles à la suite d'un incident d'origine interne. Ces informations incluent les secrets commerciaux, les éléments de propriété intellectuelle (notamment le code source), les informations clients et les dossiers des collaborateurs. Cette catégorie de coûts comprend également le coût de la notification de la compromission de données dans le cas où des informations personnelles sont collectées de façon injustifiée.

02 **Coût de la perturbation des activités :** impact financier des perturbations ou des arrêts non planifiés qui empêchent l'entreprise de respecter ses obligations en matière de traitement des données.

03 **Coût des dommages causés aux équipements :** coût de la correction des équipements et autres ressources informatiques à la suite d'un incident d'origine interne ciblant les ressources informationnelles et l'infrastructure critique.

04 **Perte de revenus :** perte de clients (attrition) et d'autres parties prenantes en raison de perturbations ou d'arrêts des systèmes découlant d'un incident d'origine interne. Pour extrapoler ce coût, nous employons une méthode d'estimation des coûts qui repose sur « l'indice de valeur économique » d'un client moyen défini pour chaque entreprise participante.

5 Les coûts internes sont extrapolés en utilisant le temps de main-d'œuvre comme indicateur des coûts directs et indirects. Cette méthode permet également d'allouer une composante « frais généraux » aux coûts fixes, notamment pour les investissements pluriannuels dans les technologies.

RÉFÉRENCIATION

Notre instrument de référence est conçu pour collecter des informations descriptives auprès des professionnels de l'informatique et de la sécurité des informations, ainsi que d'autres collaborateurs clés, concernant les coûts réels encourus directement ou indirectement à la suite de la détection d'une attaque ou d'un incident d'origine interne. Notre méthode de calcul des coûts ne requiert pas la collecte de résultats comptables à proprement parler auprès des participants à l'étude, mais repose sur l'estimation et l'extrapolation des données recueillies lors des entretiens sur une période de quatre semaines.

L'estimation des coûts se fonde sur les entretiens de diagnostic confidentiels réalisés avec des collaborateurs clés de chaque entreprise référencée. Les méthodes de collecte de données n'incluaient pas d'informations comptables, mais reposaient sur des estimations numériques basées sur les connaissances et l'expérience de chaque participant. Au sein de chaque catégorie, l'estimation des coûts a été réalisée en deux étapes. Premièrement, l'instrument de référence demandait aux participants de fournir une estimation des coûts directs pour chaque catégorie de coûts, au moyen d'une plage variable définie selon le format d'axe gradué ci-dessous.

Utilisation de l'axe gradué : l'axe gradué fourni sous chaque catégorie de coûts associés aux compromissions de données permet d'obtenir la meilleure estimation possible de la somme des débours, des frais de main-d'œuvre et des frais généraux encourus. Sélectionnez un point unique entre les limites inférieure et supérieure définies ci-dessus. Vous pouvez redéfinir ces limites à tout moment pendant l'entretien.

Indiquez ici votre estimation des coûts directs pour [catégorie de coûts concernée]

Limite inférieure _____|_____ **Limite supérieure**

La valeur numérique obtenue avec cet axe gradué (plutôt qu'une estimation précise de chaque catégorie de coûts présentée) a permis de préserver la confidentialité des participants et d'obtenir un taux de réponse plus important. L'instrument de référence demandait également aux participants de fournir une deuxième estimation, pour les coûts indirects et le manque à gagner, pris séparément.

Les estimations des coûts ont ensuite été regroupées pour chaque entreprise, en fonction de l'importance relative de ces coûts par rapport aux coûts directs au sein d'une catégorie donnée. Pour terminer, nous avons posé aux participants des questions générales afin d'obtenir des informations supplémentaires, notamment sur les pertes de revenus estimées à la suite d'un incident ou d'une attaque d'origine interne.

Les questions de l'enquête ont été limitées aux catégories de coûts communes à plusieurs secteurs d'activité. D'après notre expérience, une enquête qui se concentre sur les processus génère un taux de réponse plus élevé et des résultats de meilleure qualité. Nous avons par ailleurs utilisé un instrument papier plutôt qu'une enquête électronique afin d'assurer une plus grande confidentialité.

Pour maintenir une confidentialité totale, l'instrument utilisé pour l'enquête ne collectait aucune information spécifique aux entreprises. Les documents de l'enquête ne contenaient aucun code de suivi ou autre élément permettant de relier les réponses aux entreprises participantes.

Pour permettre à l'instrument de référence de rester gérable en termes de taille, nous nous en sommes tenus aux centres de coûts jugés essentiels pour mesurer les coûts. Sur la base de discussions que nous avons eues avec des spécialistes, nous avons décidé de nous concentrer sur un ensemble limité d'activités générant des coûts directs et indirects. Après avoir collecté les informations de référence, nous avons soumis tous les instruments à un examen minutieux afin de confirmer leur cohérence et leur exhaustivité. Lors de cet examen, certaines entreprises ont été écartées en raison de réponses incomplètes ou incohérentes, ou de l'absence de réponse.

Notre enquête sur le terrain a débuté en septembre 2021. Pour garantir une certaine cohérence entre toutes les entreprises de référence, la collecte d'informations concernant leur expérience a été limitée à une période de quatre semaines consécutives. Cette période n'était pas nécessairement la même pour toutes les entreprises participant à l'étude. Les coûts directs et indirects extrapolés ont été annualisés en divisant le coût total calculé sur quatre semaines (rapport = 4/52 semaines).

LIMITES DE L'ÉTUDE

CETTE ÉTUDE UTILISE UNE MÉTHODE DE RÉFÉRENCE CONFIDENTIELLE ET PROPRIÉTAIRE QUI S'EST RÉVÉLÉE CONCLUANTE LORS D'ÉTUDES ANTÉRIEURES.

Certaines limites inhérentes doivent toutefois être dûment prises en compte avant de tirer des conclusions sur la base des observations.

- **Résultats non statistiques :** cette étude s'appuie sur un échantillon représentatif et non statistique d'entreprises ayant subi un ou plusieurs incidents d'origine interne au cours des 12 derniers mois. Nos méthodes d'échantillonnage n'étant pas scientifiques, il est impossible d'appliquer des inférences statistiques, des marges d'erreur et des intervalles de confiance aux données collectées.
- **Absence de réponse :** les observations actuelles reposent sur un petit échantillon représentatif de références. Dans cette étude, 159 entreprises sont allées au bout du processus de référence. Nous n'avons pas testé le biais de non-réponse, de sorte qu'il est possible que le coût sous-jacent d'une compromission de données dans les entreprises qui n'ont pas participé soit très différent.
- **Biais du cadre d'échantillonnage :** notre cadre d'échantillonnage étant subjectif, la qualité des résultats est fonction de son degré de représentativité des entreprises étudiées. Selon nous, le cadre d'échantillonnage actuel est davantage axé sur les entreprises disposant de programmes plus matures de confidentialité ou de sécurité des informations.
- **Informations spécifiques aux entreprises :** les informations de cette étude de référence sont sensibles et confidentielles. Dès lors, l'instrument utilisé ne collecte aucune information permettant d'identifier l'entreprise interrogée. Cet instrument permet en outre aux participants d'utiliser des variables de réponse catégoriques pour communiquer des informations démographiques sur l'entreprise et son secteur d'activité.
- **Facteurs non mesurés :** pour garantir un script d'entretien concis et ciblé, nous avons décidé d'omettre d'autres variables importantes de nos analyses, telles que les principales tendances et les caractéristiques organisationnelles. Il est impossible de déterminer dans quelle mesure les variables omises pourraient expliquer les résultats de l'étude de référence.
- **Résultats des coûts extrapolés :** la qualité de l'étude de référence est fonction de l'intégrité des réponses confidentielles données par les personnes interrogées au sein des entreprises participantes. Même si certains contrôles peuvent être intégrés dans le processus, il est toujours possible que certaines réponses fournies ne soient pas honnêtes ou exactes. En outre, l'utilisation de méthodes d'extrapolation des coûts plutôt que de données de coût réelles peut introduire accidentellement un biais et des inexactitudes.

Promotion de pratiques responsables de gestion des informations

Le Ponemon Institute est un institut indépendant spécialisé dans la recherche et la formation, dont le but est de promouvoir des pratiques responsables de gestion des informations et de la confidentialité au sein des secteurs public et privé. Sa mission consiste à réaliser des études empiriques de haute qualité sur des questions critiques qui impactent la gestion et la sécurité des informations sensibles des particuliers et des entreprises.

À cette fin, le Ponemon Institute applique des normes strictes de protection des données, de confidentialité et de recherche éthique. Il ne collecte aucune donnée personnelle auprès des particuliers (ni d'information permettant d'identifier les entreprises interrogées dans le cadre de ses études destinées aux entreprises). Il applique en outre des normes de qualité strictes afin d'éviter que des questions superflues, hors sujet ou inappropriées soient posées aux participants.

À propos de Proofpoint

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.