MANDIANT®

NOW PART OF Google Cloud

Threat Intelligence : les perspectives mondiales

Notre rapport « Threat Intelligence : les perspectives mondiales » révèle à quel point les équipes de sécurité s'inquiètent de l'incapacité de leurs dirigeants à réellement saisir la nature de la menace. C'est ainsi que les décisions de cybersécurité les plus critiques sont prises sans tenir compte des acteurs malveillants et de leurs modes opératoires.

Sandra Joyce
VP, Mandiant Intelligence
Google Cloud

Premier du genre, ce rapport vous invite à découvrir la manière dont les entreprises perçoivent et abordent le champ actuel des cybermenaces. Ses conclusions sont le fruit d'entretiens approfondis avec 1 350 responsables IT et métiers d'entreprises de plus de 1 000 salariés, tous dotés de pouvoirs décisionnaires sur les questions de sécurité. Ces participants travaillent pour des entreprises de 18 secteurs d'activités – dont les services financiers, la santé et les pouvoirs publics – dans 13 pays couvrant trois régions du globe.

La couverture internationale de cette étude et la qualité des réponses fournies dressent un tableau captivant de la façon dont les responsables sécurité de grandes entreprises abordent et opérationnalisent la Threat Intelligence.

Les faits marquants

Les réponses à notre étude confirment notre hypothèse de départ selon laquelle les équipes de sécurité accordent une grande importance à la Threat Intelligence qu'ils reçoivent de multiples sources, sans toutefois pouvoir l'appliquer efficacement à l'échelle de leur organisation.

Il en ressort que, dans les plus grandes entreprises de la planète, ces équipes sont confrontées non seulement à d'importantes pressions, mais aussi à des difficultés à diffuser la CTI dans toute la structure organisationnelle. Certes, elles sont clairement conscientes du besoin d'une meilleure information sur les acteurs cyber, mais n'en sont pas moins contraintes de prendre des décisions à l'aveugle, sans savoir précisément qui les attaque et pourquoi. Au final, les défenses érigées sont souvent en décalage avec les menaces en présence.

96 % des participants se disent satisfaits de la qualité de la Threat Intelligence utilisée par leur entreprise

47 % des sondés considèrent que l'une de leurs plus grandes difficultés consiste à appliquer efficacement la Threat Intelligence à tous leurs systèmes et processus de sécurité

67 % des répondants pensent que leurs dirigeants sous-estiment la cybermenace qui pèse sur leur entreprise

96 % des responsables sécurité disent qu'il est important de bien connaître le profil des acteurs cyber susceptibles de cibler leur entreprise

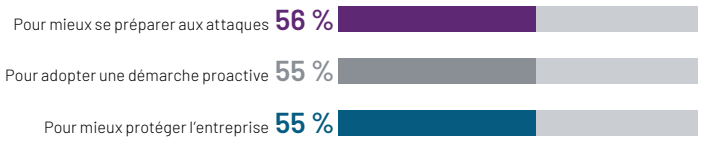
79 % des participants déclarent que, la plupart du temps, ils prennent des décisions de sécurité sans visibilité sur la nature de l'adversaire

Connaissance des menaces et confiance dans la sécurité : le grand écart

Le rapport révèle un fort décalage entre, d'une part, la grande confiance des entreprises dans leur capacité à déjouer les cyberattaques et, de l'autre, la tendance des équipes de sécurité à prendre des décisions sans disposer d'éléments complets sur les attaquants et leurs modes opératoires.

Pourtant, la quasi-totalité (96 %) des responsables sécurité pensent qu'il est important de bien cerner les attaquants qui s'en prennent à leur entreprise.

En tant que décideur sur les questions de sécurité, pourquoi pensez-vous qu'il est important de bien comprendre qui sont les acteurs cyber qui ciblent votre organisation ?

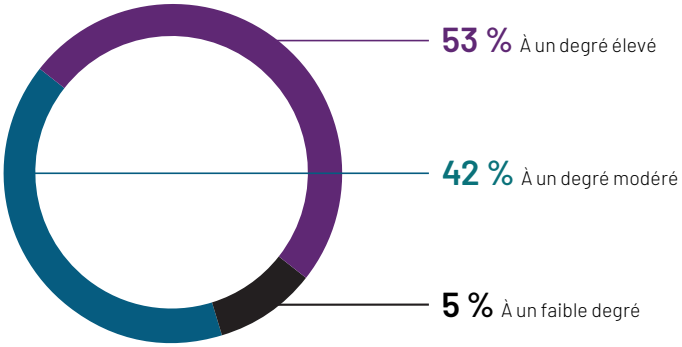


Malgré ce fort consensus sur l'importance de dresser un portrait précis des acteurs cyber en présence – et en dépit d'une satisfaction quasi totale quant à la qualité de la CTI dont ils disposent – 79 % des répondants admettent prendre leurs décisions sans réellement savoir qui sont les assaillants qui les ont dans leur viseur. Dans cette même veine, seules 35 % des entreprises interrogées ont une connaissance complète des différents groupes cyber et de leurs modes opératoires.

Autre fait marquant, 67 % des responsables cybersécurité pensent que leurs dirigeants continuent de sous-estimer la menace qui pèse sur leur organisation. Et ils sont encore plus nombreux (68 %) à penser que leur entreprise devrait avoir une meilleure compréhension du champ des menaces.

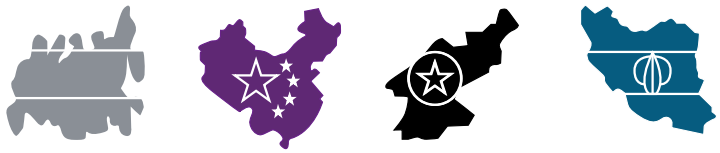
Malgré toutes ces préoccupations, les participants à notre enquête sont très majoritairement confiants dans la capacité de leur entreprise à neutraliser les menaces de sécurité. Ils sont ainsi 95 % à déclarer pouvoir prouver à leurs dirigeants, à un degré allant de modéré à élevé, que leur programme de sécurité est efficace.

À quel degré pensez-vous pouvoir prouver l'efficacité de votre programme de cybersécurité à vos dirigeants (Comex et conseil d'administration) ?

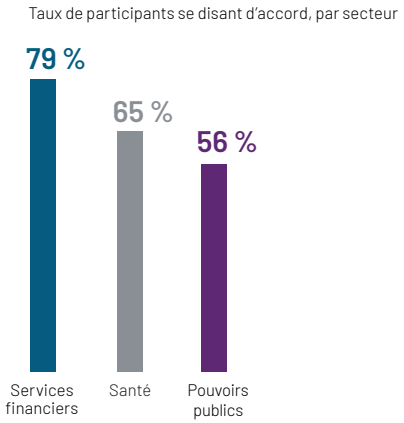


Une très grande majorité de décideurs pensent ainsi être prêts à se défendre contre une cyberattaque de grande ampleur, qu'elle soit perpétrée par des acteurs à motivations financières (91 %), des hacktivistes (89 %) ou des groupes étatiques (83 %).

En cas d'attaque perpétrée par un groupe étatique, contre quelles puissances étrangères pensez-vous ne pas pouvoir vous défendre totalement ?

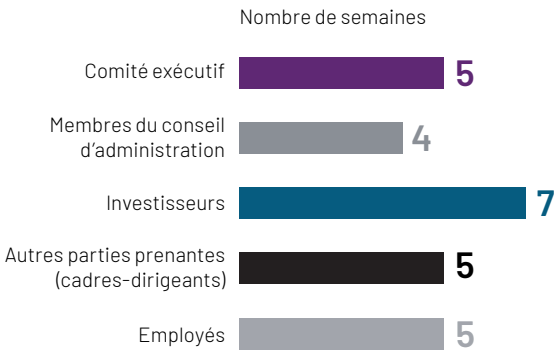


Êtes-vous d'accord avec ce qui suit ? Mon entreprise doit améliorer sa compréhension du champ des menaces.



Le manque d'information sur les acteurs cyber pourrait s'expliquer par un déficit de communication entre les responsables sécurité et le reste de l'entreprise. D'après nos participants, les questions de sécurité ne sont discutées en moyenne qu'une fois toutes les quatre ou cinq semaines avec le CA, le Comex et d'autres cadres-dirigeants hors SSI. Les échanges sont même encore plus rares avec les investisseurs, où la moyenne tombe à moins d'une fois toutes les sept semaines.

À quelle fréquence votre département aborde-t-il les sujets de cybersécurité avec les interlocuteurs de ces différentes catégories ? (moyenne pour l'ensemble des régions)

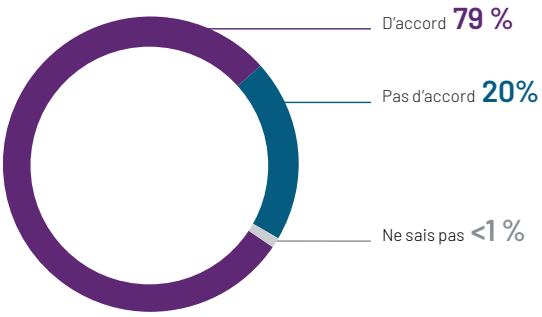


Mise en action de la CTI : difficultés et risques

Les responsables sécurité ont conscience de l'importance de la Threat Intelligence. Une très grande majorité d'entre eux estiment ainsi qu'il est important d'identifier l'auteur d'une attaque (85 %), les outils et techniques qu'il utilise (88 %) et ses motivations (87 %). On constate cependant un écart très important entre ce qu'ils disent et ce qu'ils font. Ainsi, seuls 34 % des répondants déclarent toujours prendre en compte la source d'une attaque potentielle lorsqu'ils testent la solidité de leurs défenses.

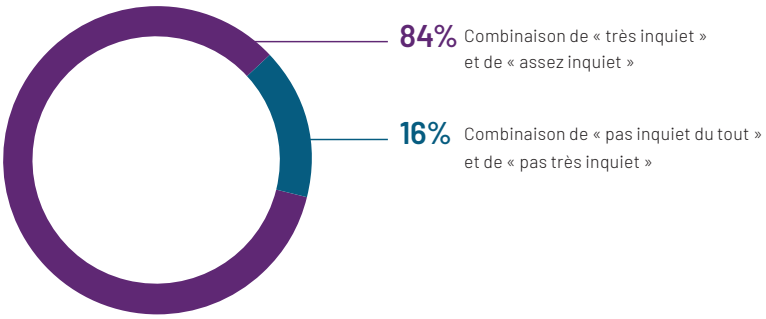
Dans un même ordre d'idée, les équipes de sécurité passent trop peu de temps à identifier et à réagir aux menaces. La plupart des répondants (79 %) pensent que leur entreprise pourrait consacrer davantage de temps et d'énergie à identifier les mouvements tectoniques sous-jacents de la cybersécurité, tandis que presque tous (98 %) s'accordent à dire qu'ils devraient réorienter plus rapidement leur stratégie de cybersécurité à la lumière des nouveaux éléments CTI en leur possession.

Êtes-vous d'accord avec ce qui suit ? Mon entreprise pourrait consacrer plus de temps et d'énergie à mieux comprendre les tendances critiques de la cybersécurité



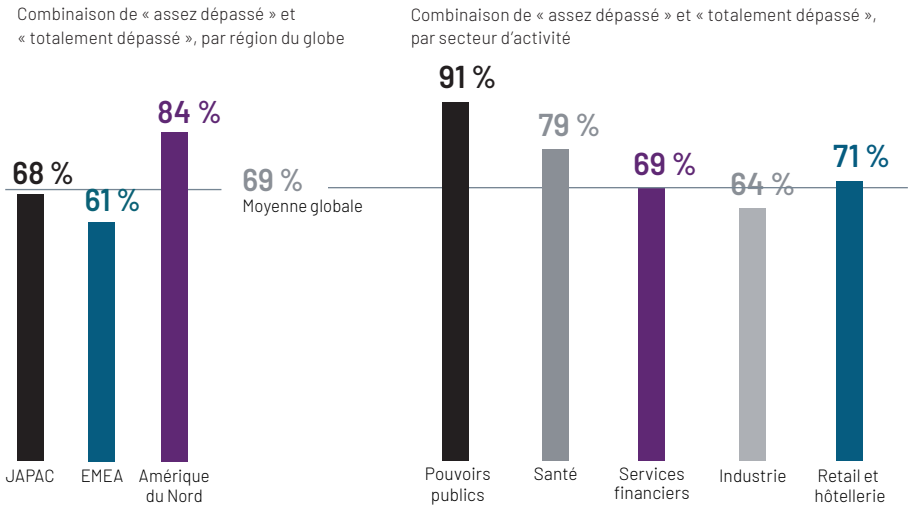
Pour obtenir une Threat Intelligence actionnable, les équipes de sécurité doivent chaque jour passer au crible des quantités phénoménales de données. Une très grande partie des répondants (84 %) se disent ainsi inquiets de laisser certaines menaces ou incidents leur échapper, faute de pouvoir traiter un tel déluge d'alertes et d'incidents. Ce trop-plein d'information va même jusqu'à impacter le bien-être des professionnels de sécurité, puisque plus de deux tiers d'entre eux (69 %) confient se sentir dépassés.

Êtes-vous inquiet de ne pas pouvoir bloquer certaines menaces ou incidents en raison de la surabondance d'alertes et d'incidents que vous devez traiter ?



C'est en Amérique du Nord que l'avalanche de données et d'alertes cause le plus de risques de burnout. De tous les secteurs d'activité interrogés, c'est dans les pouvoirs publics que les répondants sont les plus nombreux à se sentir dépassés.

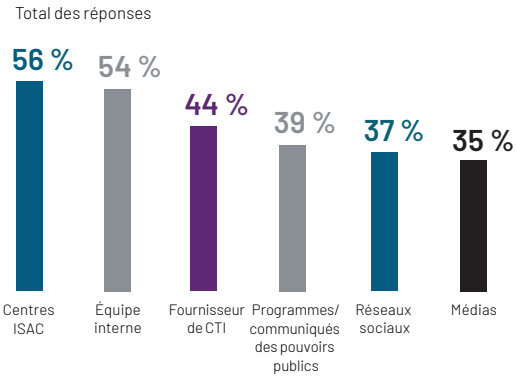
À quel degré vos équipes de sécurité se sentent-elles dépassées par la quantité de données et/ou d'alertes qu'elles doivent traiter ?



Alors que le surplus d'information apparaît clairement comme un problème pour quasiment toutes les entreprises interrogées, près de la moitié des répondants (47 %) considèrent l'application transverse de la Threat Intelligence comme l'un de leurs plus grands défis, tandis que 38 % évoquent des difficultés à savoir que faire de cette information. Plus de la moitié (53 %) des personnes interrogées voient dans la pénurie de talents en cybersécurité un obstacle à leur capacité à anticiper les dernières menaces. Pour 42 % de participants, le caractère mouvant des menaces représente également un problème.

Malgré certaines difficultés à mettre leur CTI en pratique, les équipes continuent de récolter l'information à partir d'un large éventail de sources.

Auprès de quelles sources votre entreprise puise-t-elle ses informations sur l'état de la menace ?



Les équipes de sécurité gardent souvent pour elles les informations récoltées, ou ne les communiquent qu'avec parcimonie. Elles sont ainsi 61 % à déclarer partager leur Threat Intelligence soit avec les équipes IT pour corriger les vulnérabilités de leur applications ou éléments d'infrastructure, soit avec leur hiérarchie directe pour définir les priorités. Par contraste, seuls 38 % disent diffuser la Threat Intelligence à d'autres collaborateurs pour les sensibiliser aux risques.

Pour mettre la CTI en action et maximiser la valeur de vos investissements :

Assurez-vous que les données dont vous dépendez sont fiables, récentes et actionnables

Un bon programme de Threat Intelligence doit reposer sur des fondations solides. C'est là un point de départ essentiel.

Dressez un état des lieux des menaces actives qui ciblent directement votre secteur et votre entreprise

Établissez un tableau précis des adversaires, de leurs motivations et de leurs modes opératoires pour adapter vos défenses en conséquence.

Communiquez avec vos parties prenantes

Communiquez régulièrement les bonnes informations (tactiques, opérationnelles ou stratégiques) aux bonnes personnes, jusqu'au sommet de la hiérarchie, pour fiabiliser les décisions métiers et de sécurité.

Concentrez vos ressources sur les priorités

Passez votre CTI à la loupe pour dresser la liste des menaces les plus urgentes à traiter. Attribuez des scores de risques aux vulnérabilités et expositions recensées, puis traitez-les par ordre de priorité.

Mettez votre sécurité à l'épreuve

Prenez les devants en testant régulièrement vos capacités de réponse aux offensives des adversaires identifiés. Validez vos protections face à leurs tactiques de prédilection et mesurez les progrès accomplis au fil du temps.

Agissez

Opérationnalisez votre Threat Intelligence sur tous vos systèmes et processus de sécurité pour mettre en place une défense proactive face aux menaces potentielles.

Conclusion

Dans un paysage cyber particulièrement mouvant, les entreprises et administrations sont confrontées à deux grands types d'adversaires. D'une part, des cybermafias obnubilées par l'appât du gain ; de l'autre, des groupes étatiques ou paraétatiques qui cherchent à espionner, perturber l'activité économique ou paralyser les infrastructures d'importance vitale de puissances étrangères.

Comme dans tout conflit, l'information est le nerf de la guerre. C'est pourquoi les dirigeants doivent se doter d'une Threat Intelligence qui leur permet de combattre les menaces à la racine, avant qu'elles ne deviennent un vrai problème. La plupart des décideurs sont d'ailleurs conscients de cet enjeu et savent qu'une bonne information leur permet de prendre de bonnes décisions.

Pourtant, malgré ce consensus quasi unanime, les équipes de sécurité peinent encore à faire de la CTI l'arme qu'elle devrait être face aux menaces. C'est dans ce contexte qu'au moins la moitié des décisions sont prises en l'absence de toute connaissance des attaquants potentiels.

Les équipes de sécurité en sont convaincues : elles laissent certaines menaces réelles leur échapper par manque de temps, de moyens et parfois de compétences pour traiter cette masse d'informations à leur disposition. Tant qu'elles ne parviendront pas à mieux assimiler et interpréter leur CTI, elles s'exposeront à des cyberattaques toujours plus nombreuses, perturbatrices et destructrices.

Méthodologie de l'enquête – Réalisée pour Mandiant, l'enquête « Threat Intelligence : les perspectives mondiales » a été menée entre août et septembre 2022 par Vanson Bourne, un cabinet d'études de marché internationales. L'étude porte sur un échantillon de 1 350 responsables IT et sécurité d'entreprises de plus de 1 000 salariés, dans les régions EMEA, Amérique du Nord et JAPAC.

Pour en savoir plus, rendez-vous sur www.mandiant.fr

Mandiant

11951 Freedom Dr, 6th Fl, Reston,
VA 20190, USA
00 1 703 935 1700
info@mandiant.com

À propos de Mandiant

Mandiant est un leader reconnu dans les services de cyberdéfense, Threat Intelligence et réponse aux incidents. Fort de plusieurs décennies d'expérience sur la ligne de front de la cybersécurité, Mandiant aide les entreprises à mieux se préparer et répondre aux cybermenaces. Mandiant fait désormais partie de Google Cloud.

MANDIANT
NOW PART OF Google Cloud

EXT-RT-FR-FR-000482-01