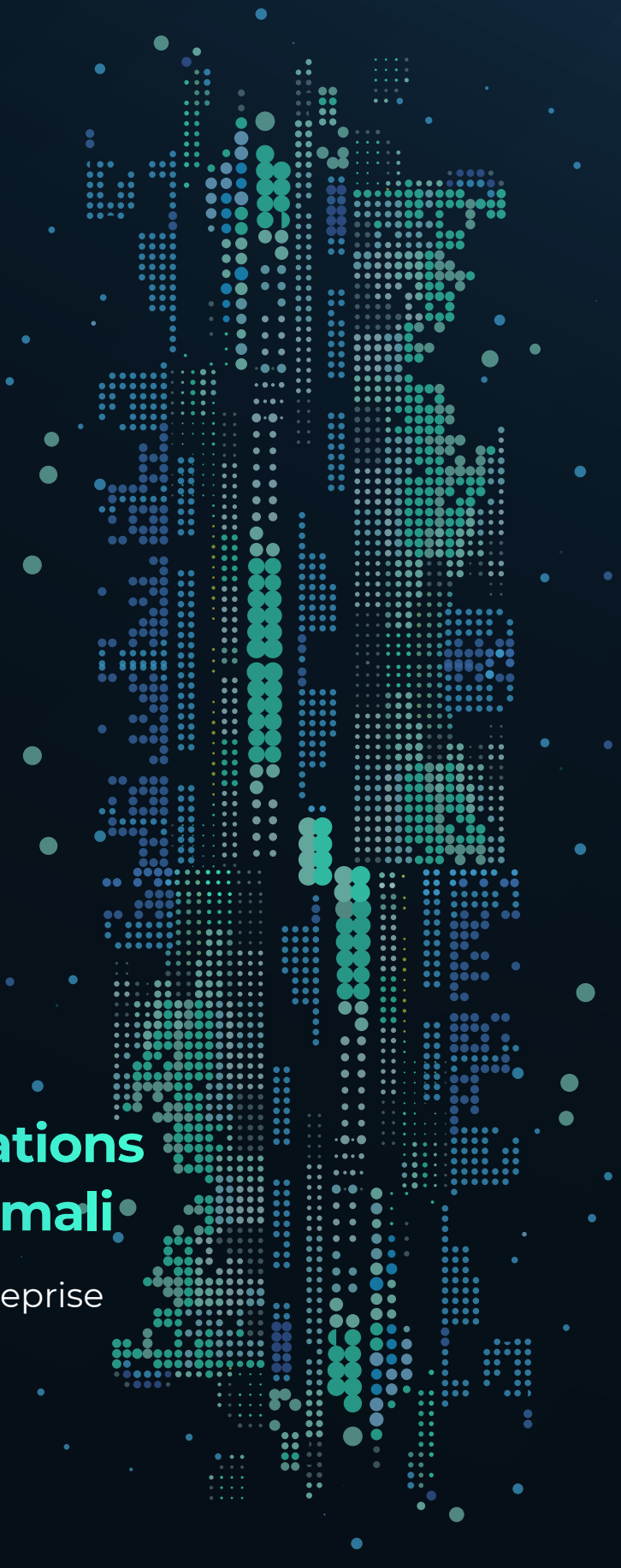
ANOMALI



2022

Rapport sur les informations de cybersécurité d'Anomali

L'état de la cyber-résilience de l'entreprise

Table des matières

Introduction

Bienvenue dans le rapport sur la cybersécurité d'Anomali 2022. Dans cette première étude, nous identifions et explorons les défis auxquels les entreprises sont confrontées pour établir et maintenir des stratégies de cybersécurité résilientes, nécessaires pour protéger et répondre aux cybermenaces avancées d'aujourd'hui et de demain.

Afin de recueillir et de développer des données fondamentales pour ce rapport, l'équipe de recherche sur les menaces d'Anomali a chargé Harris Poll d'interroger 800 décideurs en matière de sécurité dans 11 pays, issus d'entreprises comptant 5 000 collaborateurs ou plus. Étant donné que la COVID-19 a eu un impact profond sur les entreprises et la cybersécurité, nous avons demandé à ces décideurs de prendre en compte leurs positions et défis en matière de cybersécurité en 2019, afin de mieux comprendre comment la pandémie mondiale a affecté les entreprises. Les analystes de menaces de l'équipe de recherche d'Anomali ont renforcé les conclusions grâce à une analyse des tendances en matière de menaces, en fournissant aux lecteurs des informations exploitables qu'ils peuvent utiliser pour améliorer leur capacité à détecter les violations et les attaques et à y répondre.

L'un des principaux points à retenir est que même avec des investissements importants réalisés dans la cybersécurité, **de nombreuses entreprises sont confrontées à des obstacles pour atteindre le niveau de cyber-résilience nécessaire pour se protéger contre les hackers, les détecter et y répondre**. Ce constat n'est probablement pas surprenant pour la plupart des lecteurs, compte tenu de l'augmentation des violations et des cyberattaques que le monde a connue au cours des dernières années.

DÉFINITION DE LA CYBER-RÉSILIENCE

La capacité à protéger de manière proactive et réactive votre entreprise contre les menaces et les hackers, à s'adapter aux changements de situation pendant une attaque et à se rétablir après une cyberattaque.

Résumé

Notre étude a révélé de nombreuses raisons pour lesquelles il est difficile d'atteindre la cyber-résilience. En tête de liste, les entreprises doivent faire face à des lacunes en matière de performances et de capacités en matière de détection, de réponse et de restauration nécessaires pour faire face aux attaques et violations immédiates et futures.

Cette étude a révélé que les cyberattaques sont en augmentation (hausse de **15 %** par rapport aux taux de 2019 avant la pandémie). Il n'a donc pas été surprenant que trois organisations sur quatre (**74 %**) environ aient augmenté leurs budgets de cybersécurité et réévaluent leurs stratégies de cybersécurité (**78 %**).

Malgré l'augmentation des investissements, la plupart des entreprises (**87 %**) ont été victimes de cyberattaques réussies au cours des trois dernières années qui ont entraîné des dommages, des perturbations ou une violation de leurs activités. Malgré leurs efforts, environ deux tiers (**67 %**) déclarent que les cyberattaques plus réussies ont eu un impact sur leur entreprise depuis le début de la pandémie. Rien qu'en 2020, une cyberattaque sur sept (**14 %**) a réussi, entraînant une violation, des dommages ou une interruption opérationnelle. Les décideurs en matière de sécurité s'attendent à ce que ce nombre augmente, car leurs surfaces d'attaque se développent parallèlement à l'ampleur sans précédent des projets de transformation numérique. Malgré ce paysage de menaces de plus en plus dangereux, seuls 44 % ont identifié des bonnes pratiques en matière de réponse aux incidents qu'ils peuvent utiliser en cas d'attaque.

Les cyber-incidents ont un impact financier sur presque toutes les entreprises, les pertes liées aux cyberattaques ciblées, aux campagnes de logiciels malveillants, au hameçonnage, aux menaces internes et aux violations de données associées s'étant propagent à des centaines de milliers de dollars par entreprise. Près de trois entreprises sur 10 (**28 %**) ont enregistré des pertes de 500 000 $ ou plus en 2020, soit près de deux fois plus (**193 %**) qu'en 2019 et près de la moitié (**47 %**) ont enregistré des pertes de 100 000 $ ou plus. En plus des pertes importantes, les attaques elles-mêmes augmentent à un rythme incroyable.

En plus de facteurs tels que le rythme rapide de la transformation numérique et l'augmentation des attaques, de nombreux décideurs en matière de sécurité des entreprises ont cité le manque de solutions de cybersécurité intégrées comme un obstacle à la détection, à la réponse et à la récupération des cyberattaques et des violations de données.

De nombreuses personnes interrogées affirment que leur entreprise a commencé à utiliser ou prévoit d'investir dans des innovations technologiques récentes associées à la détection et à la réponse étendues (XDR) et aux renseignements avancés sur les menaces pour compenser les obstacles.

Ce qui est clair, c'est qu'il y a un réel intérêt pour des solutions de cybersécurité qui sont bien supportées (**48 %**), faciles à utiliser (**46 %**) et mieux intégrées aux infrastructures et architectures existantes (**44 %**), plus de quatre décideurs sur dix considérant ces attributs comme essentiels.

87 %

Des décideurs en matière de sécurité déclarent que leur entreprise a subi une cyberattaque réussie au cours des trois dernières années ayant entraîné des dommages, une perturbation ou une violation de leur activité.

Conclusion 1

Les entreprises ne sont que modérément efficaces pour détecter, répondre et se remettre des cybermenaces

42 % des décideurs en matière de sécurité pensent qu'ils n'ont pas atteint le niveau de résilience nécessaire pour protéger leur entreprise contre les violations et les attaques. Moins de 6 décideurs sur 10 (58 %) sont tout à fait d'accord sur la cyber-résilience de leur entreprise. Cependant, ce résultat contraste avec le fait que 87 % des entreprises ont vécu des cyberattaques au cours des trois dernières années.

Conclusion 2

Un peu moins de la moitié des décideurs en matière de sécurité sont tout à fait d'accord sur le fait que leurs équipes de cybersécurité peuvent rapidement hiérarchiser les menaces en fonction des tendances, de la gravité et de l'impact potentiel

Un tiers admettent que leurs équipes peinent à mettre à jour les contrôles de sécurité pour répondre aux nouvelles attaques (31 %). Moins de la moitié (49 %) des décideurs en matière de sécurité sont tout à fait d'accord sur le fait que leurs équipes de cybersécurité peuvent rapidement hiérarchiser les menaces en fonction des tendances, de la gravité et de l'impact potentiel. Encore moins (46 %) sont convaincus que leurs technologies de cyber-protection peuvent évoluer pour détecter de nouvelles menaces identifiées à l'échelle mondiale. Un tiers (32 %) admettent que leurs équipes peinent à suivre l'évolution du paysage des menaces de cybersécurité. Les petites entreprises sont encore plus exposées aux risques. Les entreprises comptant moins de 10 000 collaborateurs sont moins susceptibles d'être armées de bonnes pratiques qui leur permettent de répondre aux cyberattaques (40 %).

Figure 1.0
CYBER-RÉSILIENCE DES ENTREPRISES (% TOUT À FAIT D'ACCORD)

49 %
TOUT À FAIT D'ACCORD

Mon équipe peut rapidement hiérarchiser les menaces en fonction des tendances, de la gravité et de l'impact potentiel sur notre entreprise

46 %
TOUT À FAIT D'ACCORD

Mes technologies de cybersécurité peuvent évoluer pour détecter de nouvelles menaces identifiées au niveau mondial

32 %
TOUT À FAIT D'ACCORD

Mon équipe a du mal à faire face à l'évolution rapide des menaces de cybersécurité

Conclusion 3

Les entreprises n'ont pas les objectifs de détection et de réponse aux cybermenaces

Le temps d'exposition (Dwell Time) est la période entre le moment où un adversaire accède à un réseau, est détecté, puis arrêté. Le temps d'exposition est directement proportionnel à la quantité de dommages qu'un attaquant peut causer. Plus ils restent longtemps à l'intérieur de votre réseau, plus ils se renseignent, plus ils volent de données et d'adresses IP, et plus ils peuvent s'introduire dans les systèmes et les infecter avec des rançongiciels et d'autres menaces. On estime que les hackers peuvent échapper à la détection pendant 140 jours en moyenne. Mais cette mesure est spécifique à la première fois qu'une menace est détectée, puis divulguée.

Un autre aspect du temps d'exposition, tout aussi précaire, est le temps nécessaire pour déterminer si une menace nouvellement divulguée est également présente dans votre environnement. Dans le cadre de cette enquête, nous avons demandé aux entreprises combien de temps il fallait pour détecter les attaques qui avaient été divulguées précédemment et y répondre. Les résultats étaient alarmants, car en moyenne, tous les décideurs en matière de sécurité ont admis qu'ils n'atteignent pas leurs objectifs globaux de détection et de réponse et sont également en retard en ce qui concerne les types de menaces spécifiques.

Figure 1.1

TEMPS MOYEN DE DÉTECTION ET DE RÉPONSE PAR RAPPORT À L'OBJECTIF

(en jours)

	Violation de données		Attaque du réseau		Cyberattaque	
	Temps moyen	Objectif moy.	Temps moyen	Objectif moy.	Temps moyen	Objectif moy.
REPÉRER	3,1	2.1	2.8	2.1	2.7	2.5
RÉPONSE	2.5	2,2	2,5	2.1	2.4	2.1

Les équipes chargées des opérations de sécurité efficaces prêteront une attention particulière à leurs indicateurs MTTR et MTTD lorsqu'il s'agit de résoudre des incidents. Il est essentiel d'être concentré pour réduire ces indicateurs au sein des entreprises, car des temps d'exposition plus courts réduisent le risque global de dommages et de perturbations. La réduction des temps d'exposition (MTTD et MTTR) commence par la compréhension des attaques et de leur impact. Les entreprises doivent également éliminer les silos et collaborer de manière transversale pour garantir des processus de détection et de réponse efficaces.

MTTD

Le temps moyen de détection, ou MTTD, reflète le temps nécessaire à votre équipe pour découvrir un potentiel

MTTR

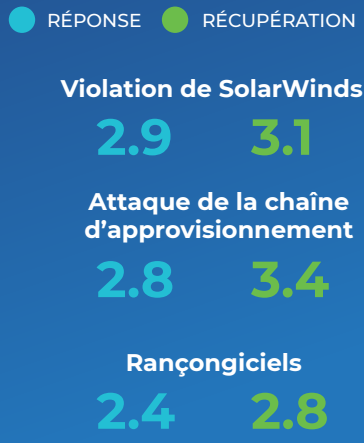
Le temps moyen de réponse, ou MTTR, est le temps nécessaire pour contrôler, corriger et/ou éliminer une menace après qu'elle a été découverte.

Figure 1.2

NOMBRE MOYEN DE JOURS POUR DÉTECTER LES CYBERATTAQUES CONNUES

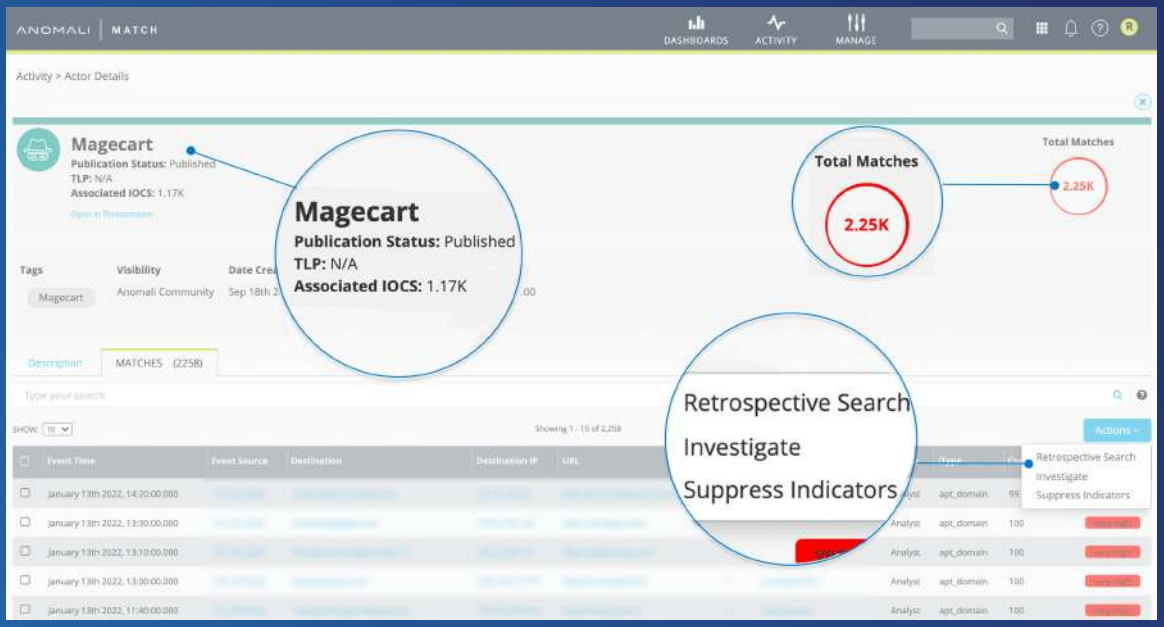
Figure 1.3

NOMBRE MOYEN DE JOURS DE RÉPONSE ET DE REPRISE APRÈS UNE CYBERATTAQUE



Anatomie de la détection des menaces

MAGECART : groupe cybercriminel malveillant ciblant des sites Web d'e-commerce pour voler des informations de carte de paiement et les vendre sur des forums criminels.



Il existe de nombreux types de menaces, et leur détection n'est généralement qu'un aspect de l'atténuation et de la réponse. La collecte d'informations supplémentaires est essentielle pour prendre des décisions basées sur les données concernant les menaces.

Les professionnels de la cybersécurité utilisent désormais les analyses de Big Data (grandes quantités d'informations recueillies à partir de plusieurs sources) pour identifier les menaces avant qu'elles ne surviennent. Avec les bonnes technologies, ces données peuvent être analysées pour obtenir des informations sur le comportement humain, prédire les tendances futures ou prévenir les failles de sécurité.

L'exemple ci-dessus montre comment les outils qui intègrent de grandes quantités de données, y compris les indicateurs de compromission (IOC), les comportements observés, les connaissances des adversaires et les modèles de menaces, peuvent être utilisés par les analystes pour savoir immédiatement si des menaces telles que Magecart sont présentes dans leur environnement et depuis combien de temps. Lorsque les entreprises ont accès à des renseignements immédiats, elles peuvent réagir rapidement et de manière décisive, ce qui est essentiel pour mettre en place une stratégie de sécurité proactive et résiliente.

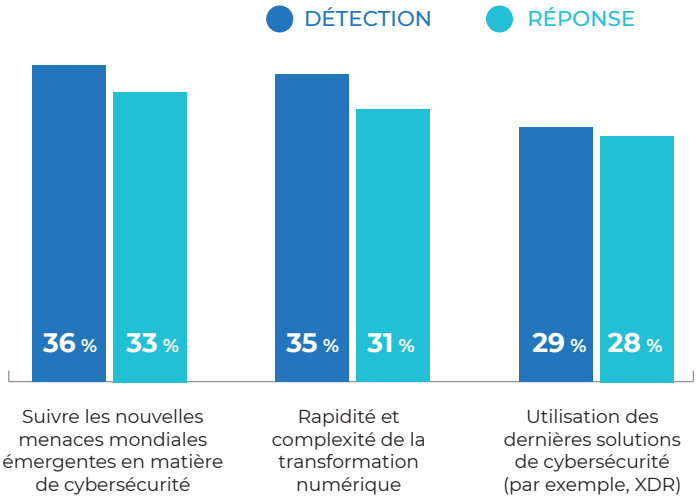
Conclusion 4

Tenir compte des nouvelles menaces mondiales émergentes en matière de cybersécurité, ainsi que de la vitesse et de la complexité de la transformation numérique sont des défis majeurs

Les entreprises sont confrontées à de nombreux défis en matière de détection. Parmi les plus importants, figure le fait de suivre les nouvelles menaces mondiales et émergentes en matière de cybersécurité (36 %), la vitesse et la complexité de la transformation numérique (35 %) et l'adoption des avancées en matière de cybersécurité telles que XDR (29 %). Des défis presque identiques ont été relevés pour répondre aux menaces et les résoudre.

Figure 1.4

DÉFIS LIÉS AUX CYBERATTAQUES, AUX ATTAQUES SUR LE RÉSEAU ET AUX VIOLATIONS DE DONNÉES



Conclusion 5

Le manque de capacité à partager les renseignements sur les menaces entre les ressources internes entrave les efforts d'atténuation

Suivre les nouvelles menaces mondiales émergentes en matière de cybersécurité, ainsi que la vitesse et de complexité de la transformation numérique figurent parmi les défis cités par décideurs en matière de sécurité d'entreprise. Mais plus que tout, il peut s'agir de l'absence de solutions intégrées et de la capacité à partager les renseignements sur les menaces de manière transversale, ce qui entrave la plupart des efforts de détection, de réponse et de reprise des cyberattaques. Un peu plus de la moitié (53 %) des décideurs estiment que leur entreprise est très efficace pour partager des informations sur les menaces entre les ressources internes.

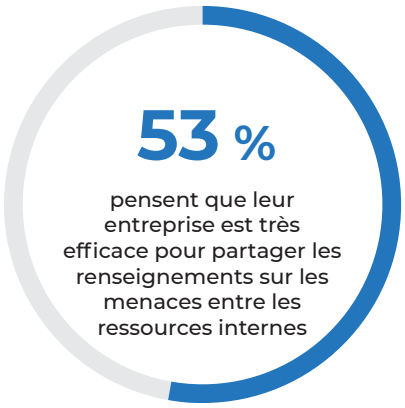
PRINCIPAUX DÉFIS POUR ATTEINDRE LA CYBER-RÉSILIENCE

Les renseignements sur les menaces sont complexes et les variables sont nombreuses et souvent décrites différemment. Pour que les efforts de partage des informations soient fructueux, des normes telles MITRE, NIST, STIXX, et d'autres ont émergé et amélioré les processus.

Pour comprendre comment partager, les entreprises doivent également savoir ce qu'elles tentent de distribuer. Pour réduire encore davantage la complexité, la veille des menaces peut être divisée en deux catégories : les IOC et les acteurs des menaces, ce qui peut aider les professionnels de la sécurité et du risque à comprendre comment utiliser ces informations.

Figure 1.5

EFFICACITÉ DU PARTAGE DES RENSEIGNEMENTS SUR LES MENACES ENTRE LES RESSOURCES INTERNES



IOC

- Les flux OSINT (veille Open Source) peuvent être faciles à obtenir si des processus sont en place pour assimiler et étiqueter les données en conséquence.
- Les plateformes de renseignements sur les menaces (TIPS) peuvent faire une grande partie de ce travail pour vous en fusionnant les flux de veille sur les menaces provenant de vos sources de veille (gratuites et commerciales).
- Les bases de données et référentiels IOC tels qu'AlienVault (OTX), Hybrid Analysis, MalwareBazaar, PolySwarm, VirusTotal, VirusBay, VirSCAN, URLhaus et URLScan, entre autres, sont d'excellents outils pour recueillir le contexte et prendre des décisions basées sur les données.
- Des sandbox comme AnyRun, Hatching, Hybrid Analysis, Inquest, Joe, Valkyrie Comodo, entre autres, sont utiles pour voir les tendances globales et les TTPS afin de créer des signatures pour les tactiques courantes de logiciels malveillants.
- Les référentiels linguistiques de détection OSINT pour Yara, SIGMA, Snort, etc., sont un excellent moyen de couvrir les comportements malveillants courants.

SOURCES DES MENACES

- Les sources OSINT telles que ThaiCERT, MITRE Groups, Malpedia et Maltego sont d'excellentes sources de données sur les menaces.
- Les TIP doivent avoir de nombreux acteurs de menace documentés et des associations IOC en temps réel pour se tenir au courant des groupes prolifiques.
- Connaître quelles familles de programmes malveillants sont exécutées par différents groupes, vendues « en tant que service », les logiciels malveillants génériques modifiés, les outils légitimes ou les programmes malveillants personnalisés, permettra une position proactive lors de la mise en place d'une stratégie d'atténuation de ces menaces.

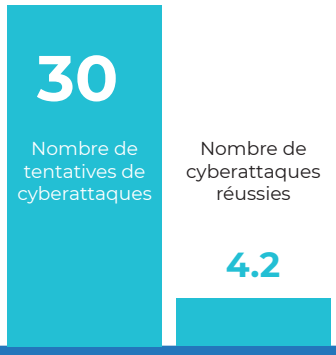
La catégorisation des types d'informations permet de mieux détecter les hackers et les violations et d'y répondre. Les entreprises se tournent vers des innovations qui permettent d'automatiser et d'exploiter les renseignements sur les menaces sur l'ensemble des infrastructures de sécurité afin d'optimiser davantage leur valeur. Des rapports récents publiés par les principaux analystes du secteur révèlent que la demande de solutions sur le marché du renseignement sur les menaces, qui comprend les plateformes de gestion des menaces, connaîtra une hausse annuelle de 16 % au cours des trois prochaines années.

Conclusion 6

Les cyberincidents sont répandus et ont augmenté depuis le début de la pandémie

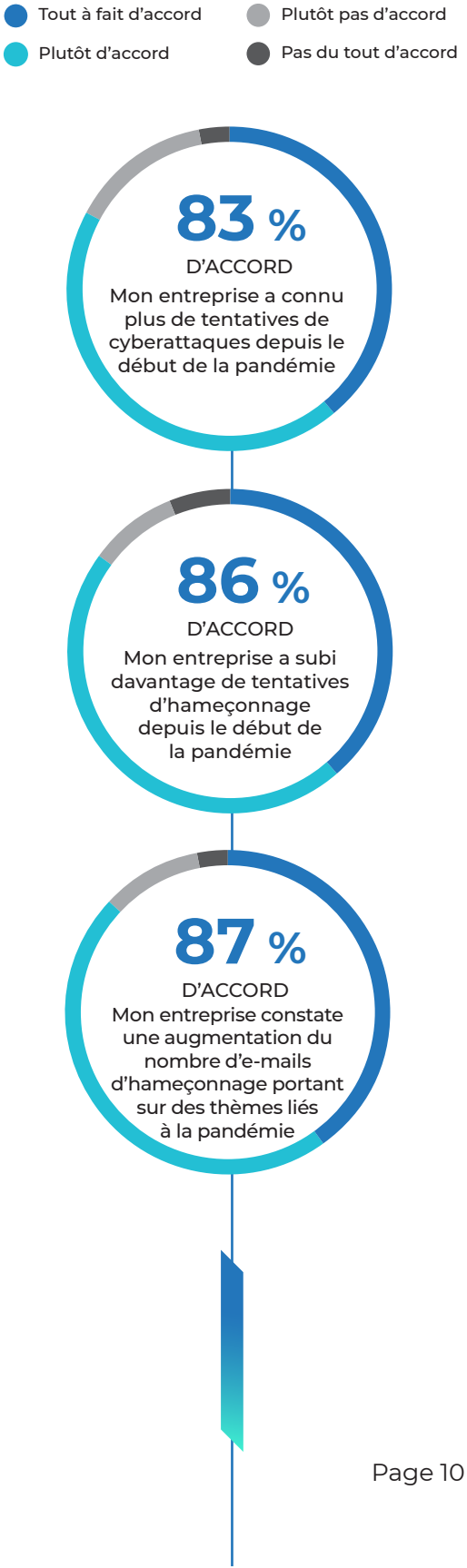
La plupart des décideurs en matière de sécurité d'entreprise s'accordent à dire que leur entreprise a connu plus de tentatives de cyberattaques (83 %) et a subi plus de tentatives d'hameçonnage (86 %) depuis le début de la pandémie. Ces entreprises sont également confrontées à une augmentation des e-mails d'hameçonnage portant sur des thèmes liés à la pandémie (87 %). En 2020, les entreprises comptant 5 000 collaborateurs ou plus ont signalé 30 cyberattaques en moyenne, contre 26 un an plus tôt. Une de ces cyberattaques sur sept (14 %) a été couronnée de succès, entraînant des dommages, des perturbations ou une violation des réseaux, de l'infrastructure et des appareils.

Figure 2.2
NOMBRE MOYEN DE CYBERATTAQUES CONTRE L'ENTREPRISE



Les entreprises comptant 10 000 collaborateurs ou plus ont subi plus de tentatives de cyberattaques en 2019 et 2020 que les entreprises comptant entre 5 000 et 9 999 collaborateurs (en 2019, 29,1 contre 23,3 ; en 2020, 32,4 contre 27,8)

Figure 2.1
DIVERSIFICATION DES TYPES DE CYBERATTAQUES DEPUIS LA PANDÉMIE

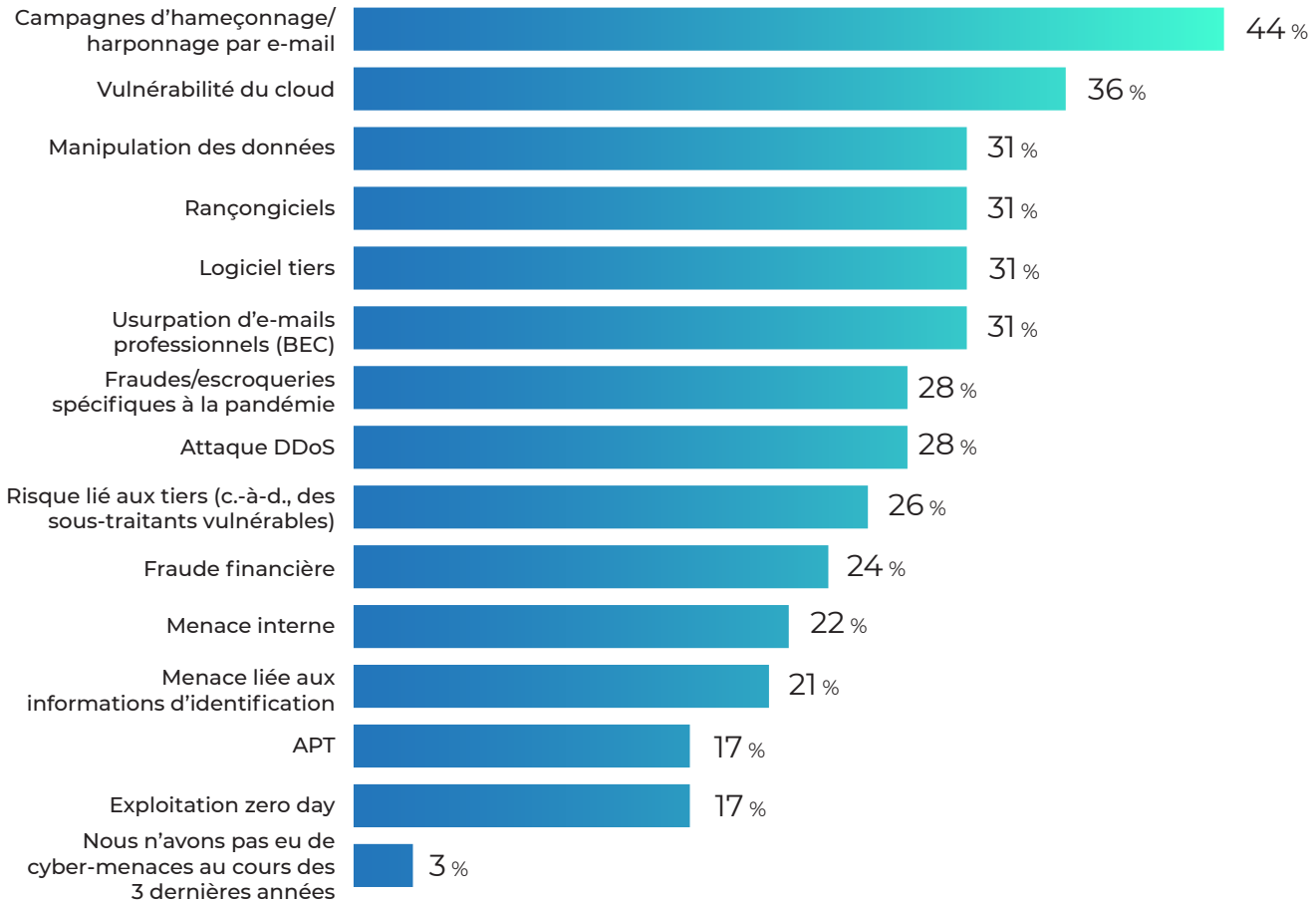


Conclusion 7

Les tentatives d'hameçonnage par e-mail constituent la menace la plus fréquente

Quarante-quatre pour cent des entreprises ont subi des attaques d'hameçonnage au cours des trois dernières années, l'attaque la plus courante. Les acteurs de toutes les menaces, quelle que soit leur complexité, utilisent l'hameçonnage en raison des outils standard disponibles et du vivier de cibles en croissance constante. Les kits d'hameçonnage générique permettent aux cybercriminels peu sophistiqués de mener des campagnes potentiellement dommageables qui fournissent des logiciels malveillants courants. Les documents malveillants (maldocs) eux-mêmes sont également banalisés grâce à des outils comme **EtterSilent**. Les acteurs et groupes de menaces compromettent également les comptes de messagerie cible pour propager davantage les activités malveillantes. Ils incluent souvent des documents légitimes pour rendre leur activité plus authentique. Notre étude a observé l'utilisation de documents légitimes dans les campagnes de **Gamadon** (Primitive Bear) et **Mustang Panda**, avec la première utilisation probable de documents privés avant leur publication.

Figure 2.3
LES CYBERMENACES OBSERVÉES AU COURS DES 3 DERNIÈRES ANNÉES



Conclusion 8

Les organisations cybercriminelles sont perçues comme étant la plus grande menace pour la cybersécurité (44 %), suivies par les hackers individuels (21 %)

Il faut en moyenne 3 à 4 jours pour que les entreprises détectent les attaques de ces entités suite à la divulgation

44 % des décideurs en matière de sécurité d'entreprise déclarent que les groupes cybercriminels représentent la plus grande menace pour leur entreprise. Nous n'avons pas perçu cela comme une surprise, car les attaques et les violations les plus préjudiciables qui se produisent aujourd'hui résultent de ce type d'acteur de menace. 15 % des décideurs en matière de sécurité d'entreprise pensent que les acteurs soutenus par les États-nations représentent la menace la plus importante en matière de cybersécurité pour leurs organisations, la Russie (39 %) et la Chine (33 %) figurant en tête de la liste. Moins d'entre eux sont préoccupés par les menaces émanant de l'Iran (10 %) ou de la Corée du Nord (8 %). Les décideurs en matière de sécurité des entreprises comptant moins de 10 000 collaborateurs sont moins enclins à comprendre pleinement les motivations de ces acteurs que les grandes entreprises comptant au moins 10 000 collaborateurs.

Figure 2.4

LA PLUS GRANDE MENACE POUR UNE ENTREPRISE

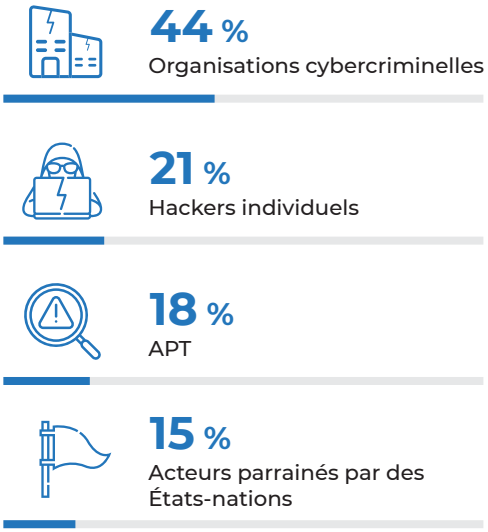


Figure 2.5

PAYS QUI REPRÉSENTE LA PLUS GRANDE MENACE EN MATIÈRE DE CYBERSÉCURITÉ

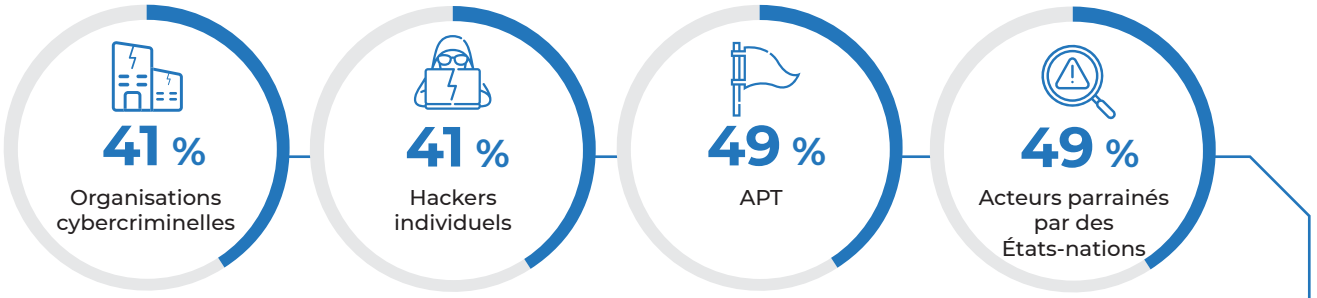
Conclusion 9

Près de la moitié des décideurs en matière de sécurité d'entreprise admettent qu'ils ne comprennent pas très bien les motivations de leurs adversaires

Le tumulte persistant des menaces moins sophistiquées peut faire passer les indicateurs de compromission (IOC) pour une goutte d'eau dans l'océan. Malgré tout cela, des groupes plus sophistiqués peuvent profiter de ce tumulte pour créer des outils personnalisés et des programmes malveillants, ou abusent de logiciels légitimes, pour mener des attaques ciblées. Par conséquent, il est essentiel de comprendre les motivations des personnes à l'origine des menaces pour savoir comment elles fonctionnent et lesquelles peuvent cibler votre entreprise.

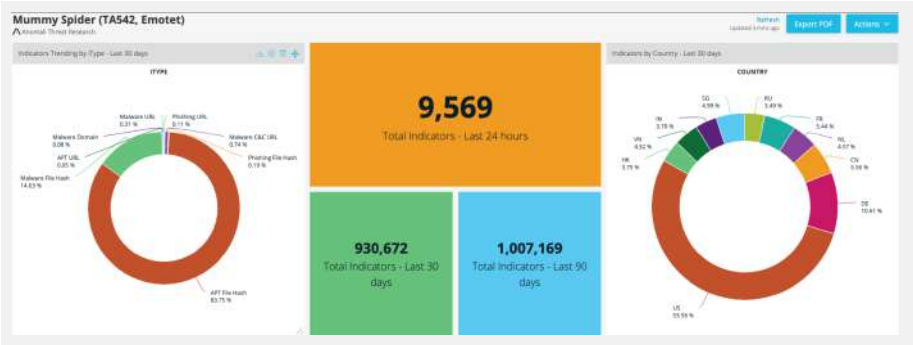
Figure 2.6

POURCENTAGE DE DÉCIDEURS EN MATIÈRE DE SÉCURITÉ QUI NE COMPRENNENT PAS TRÈS BIEN LES MOTIVATIONS, TACTIQUES, TECHNIQUES ET PROCÉDURES DES ADVERSAIRES



Les entreprises de services financiers et professionnels sont les plus susceptibles de croire qu'elles comprennent très bien les motivations des cybercriminels (64 % et 65 %, respectivement), tandis que celles des organismes de santé sont les moins susceptibles d'avoir cette compréhension (45 %).

SOURCES DES MENACES : PLUS DE PRÉCISION



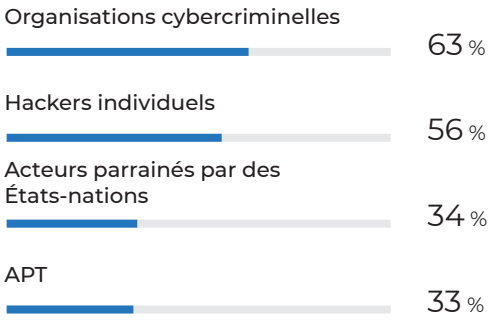
L'équipe de recherche sur les menaces d'Anomali a développé ce tableau de bord pour montrer comment gérer les renseignements sur les menaces afin d'avoir un champ de recherche large et de résumer les données. Avec ce niveau de précision, il est plus facile de comprendre les motivations et les objectifs des acteurs de la menace. Dans ce cas, nous avons appliqué le tableau de bord à **Mummy Spider**, un groupe cybercriminel lié au développement du programme malveillant communément appelé Emotet ou Geodo.

Conclusion 10

Près de 9 entreprises sur 10 (87 %) ont été victimes d'un certain type de cyberattaque au cours des trois dernières années

Au sein de ce groupe, plus de la moitié a été la cible d'attaques par des organisations cybercriminelles et des hackers individuels. Un tiers a été la cible d'acteurs soutenus par les États-nations et d'attaques de menaces persistantes avancées (APT).

Figure 2.7
LANCEMENT RÉUSSI D'UNE CYBERATTAQUE CONTRE L'ENTREPRISE



Conclusion 11

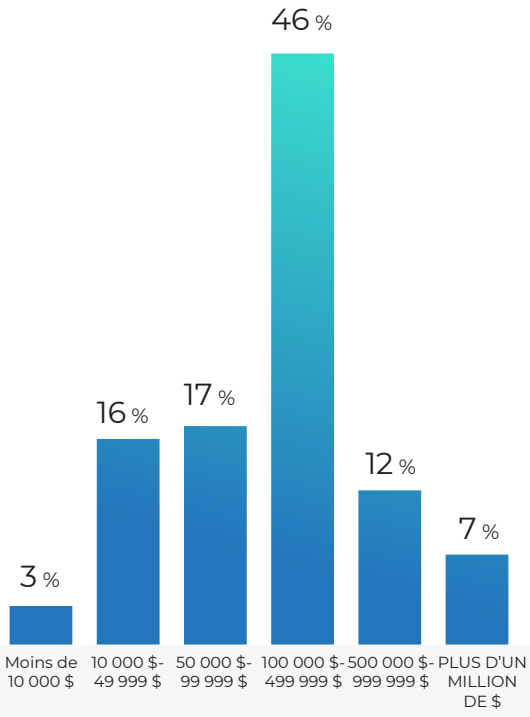
Environ la moitié des entreprises (52 %) ont été touchées par des rançongiciels au cours des trois dernières années

Environ 40 % des personnes touchées ont payé une rançon (39 %), une entreprise sur cinq (19 %) dépensant 500 000 $ ou plus. Bien qu'il s'agisse de l'une des menaces les plus répandues et les plus connues, les rançongiciels continuent de semer le chaos parmi toutes les entreprises. Pour se protéger contre cette situation, les entreprises doivent savoir où se trouvent leurs vulnérabilités, segmenter correctement les réseaux, restreindre et surveiller les autorisations des utilisateurs, conserver des sauvegardes et être en mesure de détecter et de répondre aux rançongiciels avant qu'ils ne pénètrent dans les réseaux.

39 %

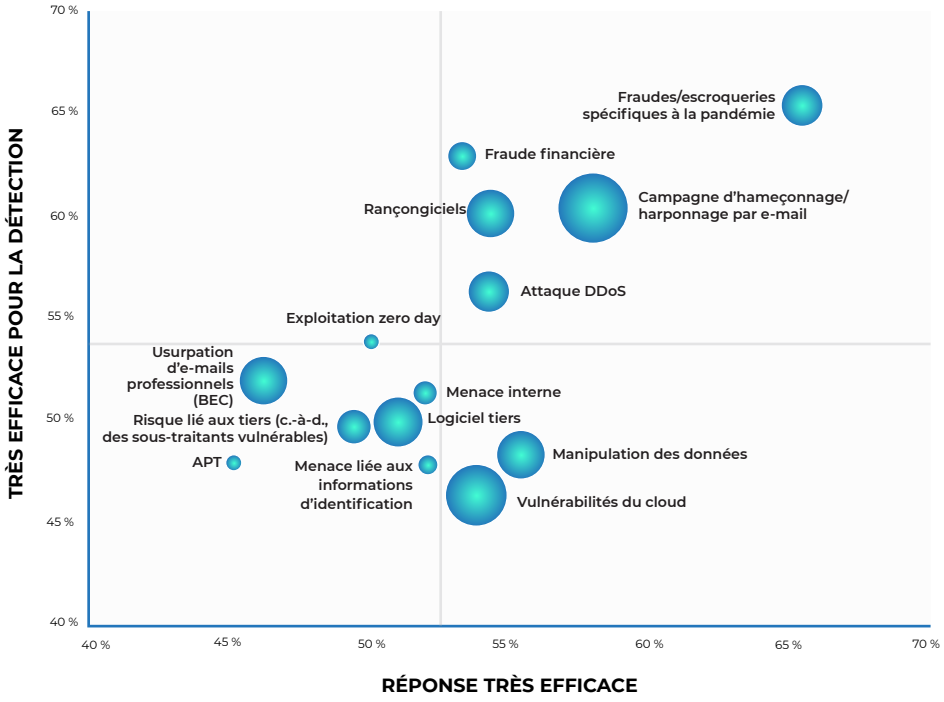
Rançon payée pour une attaque de rançongiciel au cours des 3 dernières années

Figure 2.8
MONTANT PAYÉ EN RANÇON
(ÉQUIVALENT EN DEVISE AMÉRICAINE)



PAYSAGE ACTUEL DES MENACES

Figure 2.9
DOMAINES DE VULNÉRABILITÉ POTENTIELS



REMARQUE : La taille de la bulle représente la fréquence de la menace survenue au cours des 3 dernières années

17 % des entreprises ont subi une attaque APT au cours des trois dernières années, et environ la même proportion (18 %) considère les APT comme la plus grande menace pour la cybersécurité de leur entreprise. Les décideurs en matière de sécurité d'entreprise estiment qu'ils sont moins équipés pour faire face à ces menaces que les autres types de cyberattaques, et peu d'entre eux affirment que leur entreprise est très efficace pour détecter (45 %) et répondre (48 %) aux menaces APT.

Lorsque la pandémie a commencé, les analystes en veille sur les menaces d'Anomali ont détecté **6 200 indicateurs de compromission (IOC) et au moins 15 campagnes distinctes**. Ils étaient associés à 11 acteurs ou groupes de menaces qui distribuaient 39 familles de programmes malveillants différentes à l'aide de 80 techniques MITRE ATT&CK. Anomali a évalué tôt que la menace présentée par les campagnes d'hameçonnage liées à la COVID-19 contre les entreprises publiques et privées continuerait à augmenter, les Conclusions 6 et 7 montrant que ces attaques s'intensifient.

Conclusion 12

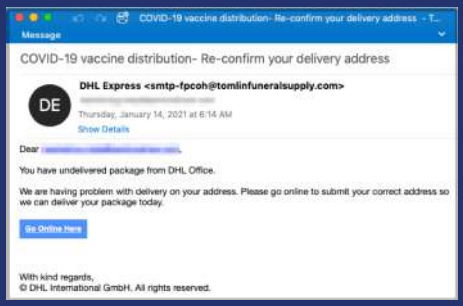
La pandémie a contraint les entreprises à réévaluer leurs stratégies de cybersécurité

Plus de 3 décideurs en matière de sécurité d'entreprise sur 4 (78 %) affirment que la pandémie les a conduits à repenser leurs stratégies de cybersécurité. Selon nous, cela s'est produit pour plusieurs raisons. Les projets de transformation numérique, la croissance du personnel à distance et l'expansion de l'infrastructure cloud correspondante ont augmenté la surface d'attaque plus rapidement qu'elle ne l'était avant la pandémie. Ces facteurs ont contraint les entreprises à augmenter la visibilité de leurs systèmes, ce qui permet d'expliquer les investissements planifiés et l'utilisation existante dans des éléments tels que XDR, MITRE ATT&CK et Threat Intelligence (Conclusion 13). En outre, la COVID-19 a donné aux acteurs des menaces un sujet reconnaissable pour mener des campagnes d'hameçonnage et d'autres activités malveillantes, car la pandémie s'est avérée être une bonne arme pour susciter la confusion, la peur, la curiosité et d'autres émotions qui incitent les gens à cliquer sur des liens malveillants. Avec l'apparition constante de nouveaux variants liés à la COVID, les entreprises doivent accroître leur capacité à s'adapter, en particulier lorsqu'il s'agit d'attaques courantes telles que les campagnes d'hameçonnage par e-mail.

Figure 3.1
IMPACT DE LA PANDÉMIE SUR LA STRATÉGIE DE CYBERSÉCURITÉ

LA PANDÉMIE MONDIALE DONNE UN AVANTAGE AUX HACKERS

Depuis le début de la pandémie de COVID-19, l'équipe de recherche sur les menaces d'Anomali a observé et détecté de nombreuses campagnes malveillantes exploitant la pandémie mondiale comme un leurre. L'image de droite montre un exemple de fausse application pour appareil mobile COVID-19 diffusée publiquement dès juin 2020. Pour aider la communauté de la sécurité et les consommateurs à rester protégés contre ces types de tentatives frauduleuses de propagation de programmes malveillants, les analystes de veille sur les menaces d'Anomali ont publié un article détaillé sur le sujet : **L'équipe de recherche sur les menaces d'Anomali identifie les fausses applications de suivi des contacts COVID-19 utilisées pour télécharger des programmes malveillants qui surveillent les terminaux et vole les données personnelles**



Outre les fausses applications de suivi des contacts liées à la COVID-19, les analystes de veille sur les menaces d'Anomali ont également détecté des campagnes d'hameçonnage par e-mail exploitant le thème de la pandémie. L'e-mail ci-dessous a été détecté en février 2021.

Crédit : Les acteurs des menaces profitent de l'actualité du vaccin COVID-19 pour lancer des campagnes, AWS est utilisé pour héberger des PDF malveillants, via l'équipe de recherche sur les menaces d'Anomali

Conclusion 13

L'impact financier des cybermenaces peut être mesuré à la fois en termes de hausse des budgets de cybersécurité et de pertes directes dues aux cyber-incidents et aux attaques par rançongiciel

Les entreprises doivent maintenir une posture défensive solide pour se protéger contre un large éventail de cybermenaces, allant des campagnes d'hameçonnage par e-mail aux vulnérabilités du cloud, en passant par les rançongiciels et les APT. Les entreprises consacrent désormais près de 40 % de leur budget informatique à la cybersécurité (38 %), et trois décideurs sur quatre (74 %) en matière de sécurité d'entreprise affirment que les budgets ont augmenté au cours de l'année passée.

Pourtant, malgré ce niveau de dépenses, les pertes directes dues aux cyber-incidents continuent d'augmenter. En 2019, seulement environ un tiers des entreprises dans le monde (36 %) ont enregistré des pertes d'au moins 100 000 $ (équivalent en devise américaine). En 2020, ce niveau a atteint près de la moitié (47 %). Les pertes déclarées de 500 000 $ ou plus et de 1 million de dollars ou plus ont doublé sur cette même période d'un an (pertes de 500 000 $ ou plus : 15 % en 2019 contre 28 % en 2020 ; pertes de 1 million de dollars ou plus : 5 % en 2019 contre 11 % en 2020). Les chiffres de 2021 n'étaient pas disponibles au moment de l'enquête.

Figure 3.2

BUDGET DE CYBERSÉCURITÉ

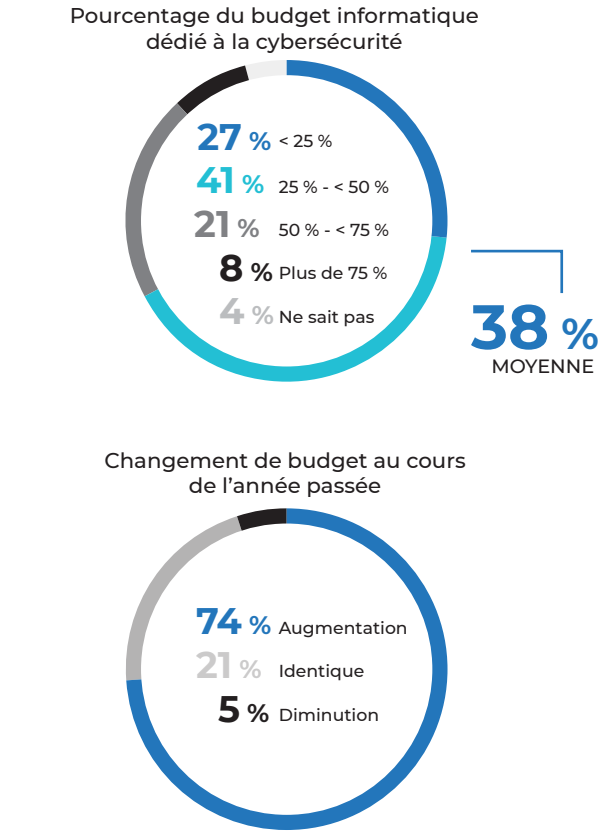
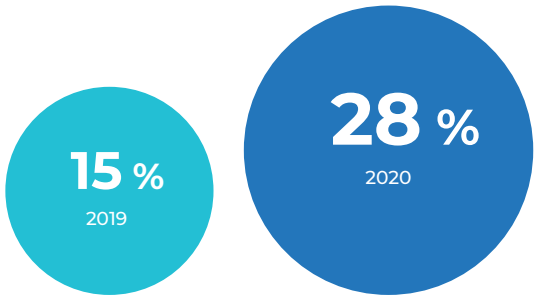


Figure 3.3

LES ENTREPRISES ONT PERDU PLUS DE 500 000 $ EN RAISON DE CYBERATTAQUES (ÉQUIVALENT EN DEVISE AMÉRICAINE)



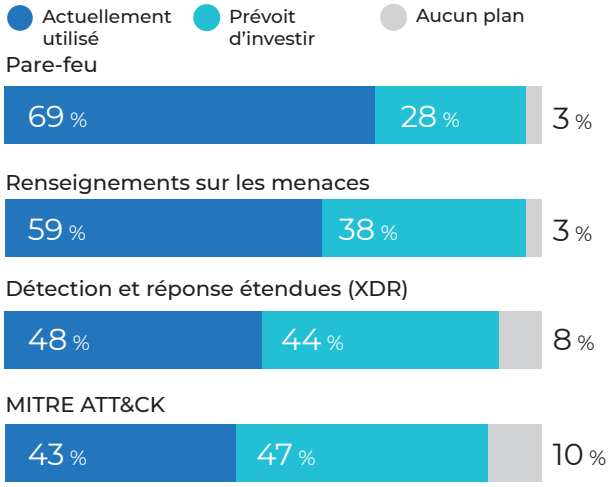
Les attaques par rançongiciel sont également devenues très coûteuses. Deux organisations sur cinq (39 %) sont touchées par des attaques de rançongiciel et ont choisi de payer une rançon. Parmi celles-ci, près des deux tiers (65 %) ont versé 100 000 $ ou plus en dollars américains ou équivalents.

Conclusion 14

Les entreprises continuent d'utiliser les technologies existantes, mais envisagent de nouvelles innovations

7 entreprises sur 10 (69 %) utilisent encore des pare-feu pour détecter les menaces sur le réseau. Cependant, 59 % utilisent de la Threat Intelligence (38 % prévoient d'investir), 48 % utilisent XDR (44 % prévoient d'investir) et 43 % utilisent le Framework TMIT ATT&CK (47 % prévoient d'investir). Nous pensons que cette transition vers l'utilisation et l'investissement dans de nouveaux outils est fondée sur le fait que, bien que les solutions existantes continuent de jouer un rôle dans les stratégies défensives, elles ne peuvent plus être utilisées uniquement pour détecter et répondre aux menaces en constante évolution.

Figure 4.1
INNOVATIONS ACTUELLES UTILISÉES



Conclusion 15

Les nouvelles solutions de cybersécurité doivent être intégrées aux infrastructures et architectures existantes

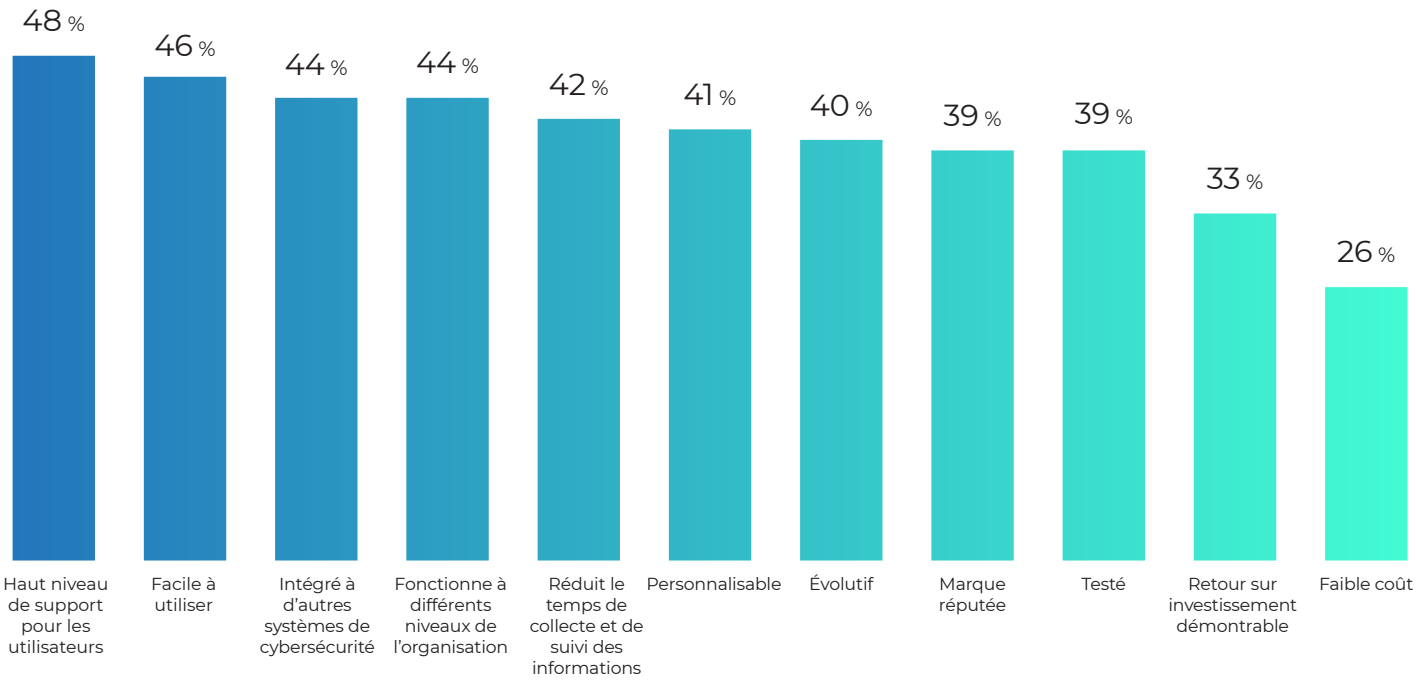
Pour faire face aux cybermenaces auxquelles ils sont confrontés chaque jour, les décideurs en matière de sécurité d'entreprise recherchent de nouvelles solutions qui sont bien prises en charge, faciles à utiliser et intégrées à d'autres systèmes de cybersécurité et à différentes parties de leur entreprise.

La personnalisation et l'évolutivité sont également considérées comme des attributs essentiels lors de l'évaluation des nouveaux outils de cybersécurité par au moins 4 décideurs sur 10 (41 %). Presque autant (39 %) recherchent des solutions réputées qui ont été testées avec succès.

Il est intéressant de noter que seul un tiers des entreprises estiment qu'il est essentiel qu'une nouvelle solution de cybersécurité démontre un retour sur investissement (33 %). Le faible coût est la moindre de leurs préoccupations, avec seulement un quart des décideurs (26 %) citant cela comme une exigence essentielle.

RÉPONSE AUX CYBERATTAQUES

Figure 4.2
ATTRIBUTS ESSENTIELS DE L'ÉVALUATION DES SOLUTIONS DE CYBERSÉCURITÉ



Malgré des résultats qui montrent une dépendance continue envers les technologies existantes, il était encourageant de découvrir que les entreprises utilisent actuellement ou prévoient d'investir dans des innovations capables de résoudre ce problème, telles que le framework TMIT ATT&CK, XDR et Threat Intelligence.

Conclusion 16

Pour suivre le rythme des menaces, la plupart des entreprises utilisent des outils et des technologies conçus pour surveiller les menaces mondiales

La mise en œuvre des renseignements sur les menaces est de plus en plus essentielle à la capacité d'une entreprise à gérer les cyber-risques et à développer la cyber-résilience. Les équipes de sécurité peuvent souvent se retrouver submergées par la quantité de données qu'elles ont collectées ainsi que par les alertes qu'elles reçoivent. Grâce à leur capacité à répondre aux menaces liées à leur empreinte numérique spécifique, elles deviennent plus efficaces.

Selon cette étude, 62 % des entreprises utilisent des outils et des technologies pour surveiller les menaces mondiales et accélérer leurs performances en matière de renseignements sur les menaces. Cette observation s'aligne sur les indicateurs du secteur qui montrent que la demande en plateformes de gestion des menaces qui utilisent l'intelligence globale pour détecter les menaces, ainsi que d'autres technologies qui permettent d'automatiser la collecte et la corrélation des données pour les rendre opérationnelles pour les équipes de sécurité, augmente.

Ces outils fournissent également des processus permettant aux professionnels des renseignements de gérer les exigences des parties prenantes, d'optimiser l'analyse des données en comprenant les intentions et les objectifs des adversaires, ainsi que de prévoir et d'améliorer la prise de décision.

La cybersécurité est désormais une stratégie commerciale essentielle. Pour comprendre les menaces de cybersécurité et les atténuer, il est nécessaire de disposer des outils, des connaissances et de l'expertise adéquats. Un programme efficace de renseignements sur les menaces aide les entreprises à détecter les menaces tôt et leur permet d'agir rapidement contre ces menaces.

Figure 4.3

COMMENT LES ENTREPRISES S'ADAPTENT À L'ÉVOLUTION RAPIDE DES MENACES

Le niveau de cyber-résilience atteint par les organisations

Pour cette enquête, nous avons défini la cyber-résilience comme la capacité à protéger de manière proactive et réactive votre entreprise contre les menaces et les hackers, à s'adapter aux changements de situation pendant une attaque et à se rétablir après une cyberattaque. Nous avons constaté que même si les entreprises augmentent leurs budgets en matière de cybersécurité, ajoutent des couches de sécurité innovantes et se concentrent sur l'efficacité plutôt que sur les coûts, elles ont encore beaucoup de travail à faire si elles espèrent réussir à trouver une véritable issue à l'avenir.

Après près de deux ans de défis et de perturbations sans précédent dans notre travail et notre vie personnelle, certains décideurs en matière de sécurité d'entreprise pensent qu'ils progressent, mais nous ne pouvons pas en conclure que c'est le cas. Bien que 6 décideurs sur 10 (58 %) soient tout à fait d'accord sur la cyber-résilience de leur entreprise, 87 % ont été victimes d'une cyberattaque réussie au cours des trois dernières années qui a entraîné des dommages, des perturbations ou une violation de leur activité. 42 % estiment qu'ils n'ont pas atteint le niveau de résilience nécessaire peuvent évaluer plus précisément leurs postures de sécurité. Près de la moitié des décideurs en matière de sécurité, même ceux qui prétendent avoir atteint la résilience, ont déclaré que l'expansion des projets de transformation numérique et le travail à distance en cours augmenteraient leur probabilité d'être victimes d'une attaque.

Figure 5.1.
CYBER-RÉSILIENCE DE L'ENTREPRISE
(TOUT À FAIT D'ACCORD)

À PROPOS D'ANOMALI

Anomali est le leader des solutions de cybersécurité de détection et de réponse étendues (XDR) basées sur l'intelligence. Soutenue par la gestion des Big Data et affinée par l'intelligence artificielle et l'apprentissage automatique, la plate-forme Anomali offre des fonctionnalités propriétaires qui mettent en corrélation un volume extraordinaire de télémétrie des solutions de sécurité déployées par les clients avec les plus grands référentiels de renseignements globaux, permettant aux équipes chargées des opérations de sécurité de détecter les menaces avec précision, d'optimiser la réponse, d'atteindre la résilience, et d'arrêter les hackers et les violations. Nos solutions SaaS orientées Cloud s'intègrent facilement aux piles technologiques de sécurité existantes et permettent un déploiement hybride. Fondée en 2013, la société Anomali est au service des entreprises du secteur public et privé, des ISAC, des MSSP et des organisations du classement Global 1000 dans tous les secteurs majeurs du monde. Les plus grandes sociétés de capital-risque, notamment Google Ventures, General Catalyst et IVP, soutiennent Anomali. Pour en savoir plus, rendez-vous sur www.anomali.com.

COMMENT ANOMALI PEUT VOUS AIDER

Les cybercriminels, les acteurs soutenus par les États-nations et les hacktivistes s'efforcent de cibler les organisations à des fins d'exploitation. Les entreprises ont besoin de données et d'informations sur les menaces pour comprendre pleinement leurs vulnérabilités afin de garder une longueur d'avance sur les menaces et de réagir rapidement aux événements.

La détection et la réponse étendues (XDR) d'Anomali, basées sur l'intelligence, fournissent aux équipes de sécurité le contexte nécessaire pour prévenir et traiter les menaces plus rapidement et plus efficacement. En automatisant le processus de collecte et d'analyse des données, des informations et des renseignements sur les menaces internes et externes, les équipes de sécurité peuvent rapidement comprendre les menaces, déterminer leur impact et apporter une réponse optimisée.

PRODUITS ANOMALI

Anomali ThreatStream

Gestion des renseignements sur les menaces qui automatise la collecte et le traitement des données brutes et les transforme en renseignements exploitables sur les menaces pour accélérer la détection, rationaliser les enquêtes et augmenter la productivité des analystes.

Anomali Match

Détection et réponse étendues (XDR) basées sur l'intelligence qui aident les organisations à détecter et à répondre rapidement aux menaces en temps réel. Match met automatiquement en corrélation TOUTES les données de télémétrie de sécurité avec les renseignements sur les menaces actives afin de fournir plus de 190 billions d'événements de menace par seconde, afin d'exposer les menaces connues et inconnues et d'arrêter les violations et les hackers.

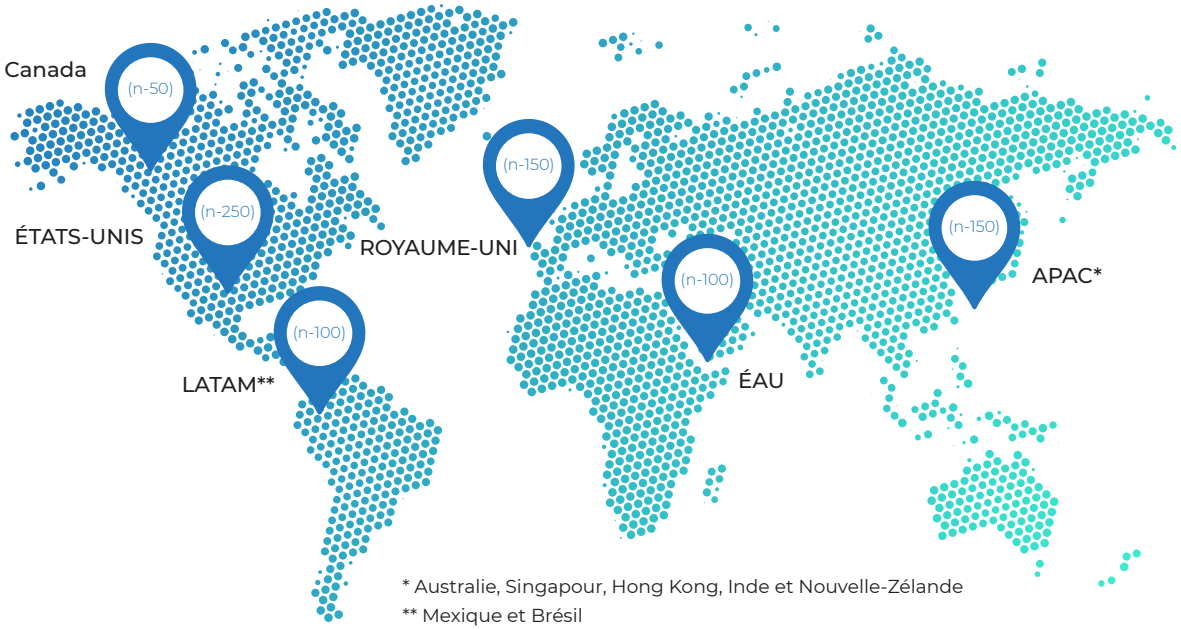
Anomali Lens

Extension pour le traitement du langage naturel (NLP) qui permet d'exploiter les renseignements sur les menaces en analysant automatiquement le contenu Web pour identifier les menaces pertinentes et rationaliser le cycle de vie des recherches et des rapports sur ces menaces.

Pour découvrir comment Anomali peut aider votre entreprise à devenir cyber-résiliente, rendez-vous sur **anomali.com.**

Méthodologie

Anomali a chargé Harris Poll de mener des enquêtes en ligne auprès des décideurs en matière de sécurité d'entreprise dans des entreprises comptant plus de 5 000 collaborateurs. L'enquête a été menée entre le 9 septembre et le 13 octobre 2021 dans les pays suivants :



* Australie, Singapour, Hong Kong, Inde et Nouvelle-Zélande
** Mexique et Brésil

CRITÈRES DE QUALIFICATION

- Âgé(e) de plus de **18 ans**
- **Employé(e) à temps plein**
- Dans **les secteurs des services financiers, de la pharmacie, de la santé, des télécommunications, de la fabrication, service professionnel**
- Occupe un **poste informatique**
- **Perspective technologique :** Niveau Manager ou supérieur et avec une influence sur les solutions de sécurité des données
- **Perspective commerciale :** Niveau Directeur ou supérieur et avec une influence sur la stratégie de sécurité des données

Les données brutes ont été pondérées, si nécessaire, par le nombre d'entreprises dans la classe de taille des collaborateurs afin de les faire correspondre à leurs proportions réelles dans la population des entreprises de plus de 5 000 collaborateurs dans les secteurs sélectionnés de la fabrication, des télécommunications, des services financiers, de la santé, des produits pharmaceutiques et des services professionnels, scientifiques et techniques, pour chaque pays séparément. Les résultats des pays ont ensuite été combinés afin de les proportionner de manière égale dans le nombre total.