Les incontournables de la cybersécurité pour tout décideur d’entreprise proactif.

Janvier 2022

kaspersky BRING ON THE FUTURE

kaspersky

Sommaire

Avant-propos : Ajouter la « touche de l’expert » à la cyber-protection automatisée.

Les APT, les attaques ciblées, les attaques contre les chaînes d’approvisionnement, sans oublier la multiplication des appareils utilisés, les services dans le cloud et l’Internet des objets : le panorama des cybermenaces et leurs points d’entrée évoluent vite et ne cessent de se complexifier.

D’après certaines entreprises, le manque de ressources, de réglementation et d’expertise sont les principaux freins à la mise en œuvre d’une stratégie de cyberprotection adéquate. La protection traditionnelle des terminaux ne suffit plus à détecter rapidement les cybermenaces afin d’y réagir de manière adaptée et d’assurer la protection des ressources critiques des entreprises. Alors, quelle est la solution pour préserver les entreprises des cybermenaces ?

Les décideurs ont besoin de connaissances approfondies, exhaustives et à jour des cybermenaces mondiales, des cyberincidents qui leur sont associés et du panorama des menaces. Les entreprises performantes doivent pouvoir compter sur une threat intelligence robuste à l’échelle mondiale qui contribue à assurer leur immunité contre les cyberattaques, même inédites. Elles souhaitent une plateforme unifiée tout-en-un : outils intégrés, détection multiniveaux des menaces et protection centralisée de nombreux points d’entrée.

Quelle que soit la taille de l’entreprise, les décideurs doivent répondre tant aux problèmes de cybersécurité qu’aux besoins de leur organisation. La moindre erreur pourrait exposer à un problème susceptible d’échapper à tout contrôle.

Ce rapport a pour but d’aider les dirigeants à assurer la sécurité de toutes les ressources critiques de leur entreprise. Il présente les dernières tendances du marché, les principaux points faibles ainsi qu’une checklist pas à pas. Accessible aux néophytes, il offre aux décideurs une vision globale et des informations incontournables.

Cela étant posé, entrons dans le vif du sujet. Intéressons-nous de plus près au partenaire de cybersécurité qui bénéficie d’une visibilité complète pour vous permettre de vous concentrer sur l'innovation, sans crainte.

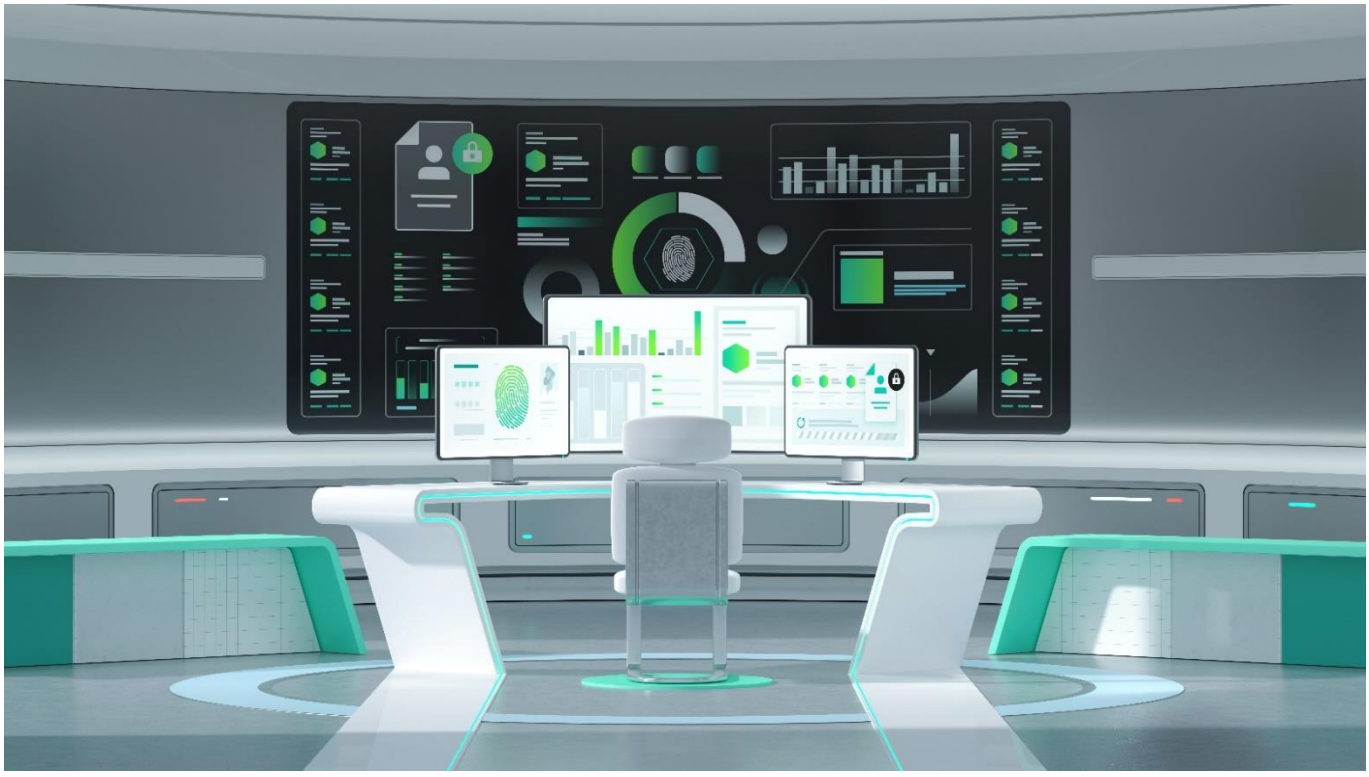
Bertrand Trastour, General Manager chez Kaspersky France et Afrique du Nord, de l’Ouest et du Centre.

Enquête européenne : les décideurs des entreprises gagneraient à être davantage proactifs en matière de cybersécurité

D'après les prévisions de l'institut de recherche Gartner, la responsabilité personnelle des trois quarts des PDG aura été engagée dans des incidents de cybersécurité au sein de leur entreprise d'ici 2024. Les organisations doivent donc impérativement faire preuve de proactivité en renforçant les mesures de sécurité contre les cybermenaces.

Une récente enquête de Kaspersky révèle que les décideurs des entreprises sont prêts à renforcer les mesures de sécurité, tout en accusant encore un certain retard. Selon cette étude, 60 % des décideurs français aimeraient être davantage proactifs en matière de cybersécurité dans leur entreprise, mais ils ne disposent pas des connaissances nécessaires. En outre, les dirigeants sont souvent confrontés à un manque de ressources et d'expertise ainsi qu'à des contraintes budgétaires qui les empêchent de réaliser les investissements requis pour accroître le niveau de sécurité au sein de leur entreprise.

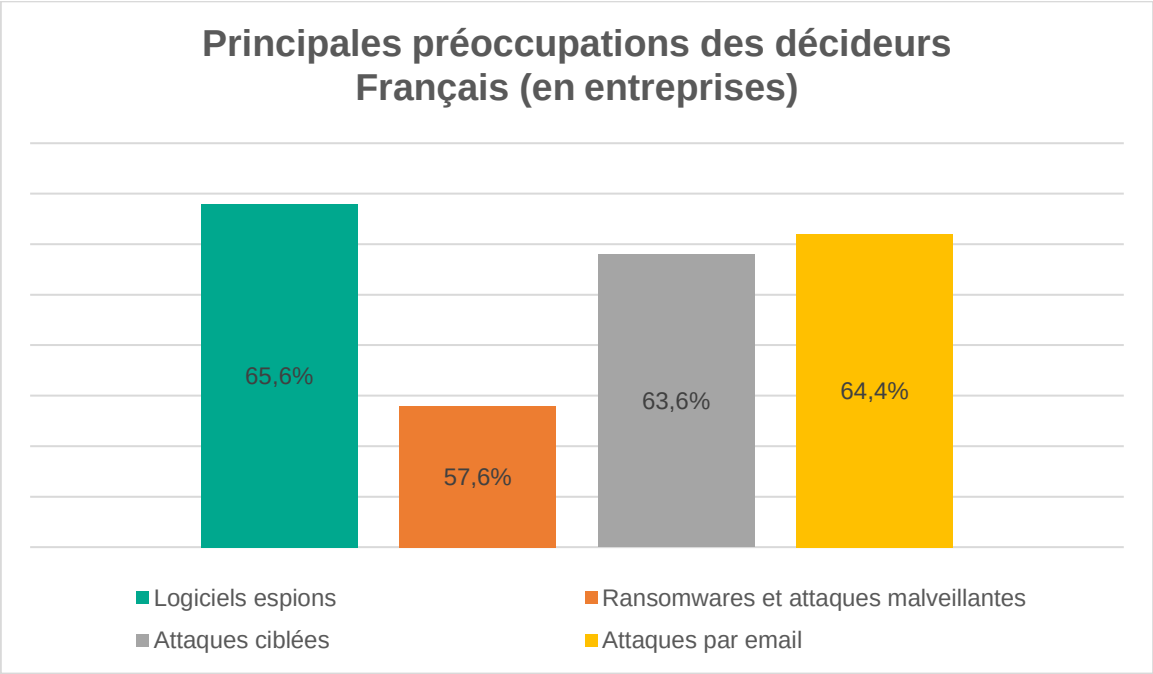
Méthodologie : cette enquête a été menée par Arlington Research pour le compte de Kaspersky en août 2021. 1 500 décideurs d'entreprise européens ont été interrogés sur Internet dans six pays (Allemagne, Royaume-Uni, France, Italie, Espagne et République tchèque), soit 250 personnes par pays. 62 % des décideurs sondés travaillent dans une PME employant entre 50 et 999 personnes. 38 % travaillent dans une grande entreprise de plus de 1 000 salariés.



kaspersky

Deux décideurs européens sur trois sont préoccupés par les cybermenaces

Près des deux tiers des décideurs d'entreprise français (62,4 %) craignent d'être victimes d'une cyberattaque, qu'ils travaillent pour une grande entreprise (66,7 %) ou pour une PME (60 %).



En moyenne, les dirigeants dont l'entreprise a déjà été victime d'une cyberattaque sont plus susceptibles de s'en inquiéter ; en effet, près des trois quarts (74,8 %) des sondés français ayant déjà subi une ou plusieurs attaques sont préoccupés à ce sujet. Un peu moins d'un sondé sur cinq (19,6 %) indique que son entreprise a été jusqu'à présent épargnée par les cyberattaques.

Décideurs d'entreprise : la protection de l'État n'est pas adaptée aux cybermenaces

Lorsque nous sommes victimes de vol dans la vie réelle, en général, la police nous porte secours. Des lois et des réglementations existent depuis de nombreuses années en Europe pour protéger les particuliers et les entreprises dans tous les domaines de la vie quotidienne.

Malheureusement, la cybercriminalité fait exception. D'après la dernière étude en date, près de deux tiers (63 %) des décideurs d'entreprise européens et 66,4 % des décideurs d'entreprise français pensent que les organisations faisant l'objet d'une cyberattaque ne reçoivent pas la même protection ni le même soutien que les victimes dans le monde réel.

Le Règlement général européen sur la protection des données (RGPD) protège les données personnelles des clients, mais il laisse peser la responsabilité de cette protection sur l'entreprise. Les organisations de toutes tailles sont confrontées à un double défi : d'une part, les cyberattaques menacent les données de l'entreprise elle-même et de ses clients, d'autre part, le cadre européen de protection des données les rend responsables des éventuels incidents de sécurité. Lorsque cette question a été posée aux décideurs français…

- Il n'est pas surprenant que 54,4 % des décideurs d'entreprise interrogés critiquent le soutien apporté par l'État aux entreprises dans leur pays.
- Près de sept sondés sur dix (66,8 %) pensent que la cybercriminalité devrait être punie aussi sévèrement que les crimes commis dans la vie réelle.
- 63 % des personnes interrogées s'inquiètent du risque de poursuites pénales à leur encontre pour des incidents de sécurité dont leur propre entreprise serait victime (cf. enquête de Gartner).

Les dirigeants évoquent également un manque de soutien en interne, la moitié (50 %) des sondés s'inquiétant de la prévention des incidents de sécurité au sein de leur propre entreprise.

« Les décideurs d'entreprise doivent renforcer de manière proactive les mesures de sécurité contre les cyberattaques afin d'offrir à leur entreprise un avenir sûr. Pour s'acquitter efficacement de cette mission, ils peuvent combiner une technologie qui détecte et neutralise automatiquement les cybermenaces avec le soutien extérieur de spécialistes de la cybersécurité expérimentés, pour que l'équipe informatique interne soit libre de se concentrer sur les tâches essentielles » Bertrand Trastour, General Manager chez Kaspersky France et Afrique du Nord, de l'Ouest et du Centre

kaspersky

La pression sur les coûts et le manque de ressources empêchent d'investir dans la cybersécurité

La question demeure : compte tenu de la complexité du panorama des menaces, pourquoi tant d'entreprises restent passives au lieu de prendre des mesures de cybersécurité proactives ?

La réponse est indéniablement liée à la pression omniprésente sur les coûts, qui se retrouve chez tous les sondés indépendamment de la taille de leur entreprise.

Dans le cadre de l'enquête, plus de la moitié (57,2 %) des décideurs d'entreprise français ont déclaré qu'ils aimeraient faire appel à des experts en cybersécurité externes. Malheureusement, ils ne disposent pas des ressources nécessaires pour trouver un partenaire de confiance. Pour 52,4 % des personnes interrogées (et 54,3 % dans toute l'Europe), il est très difficile d'obtenir un budget dédié à l'amélioration de la cybersécurité au sein de leur entreprise.

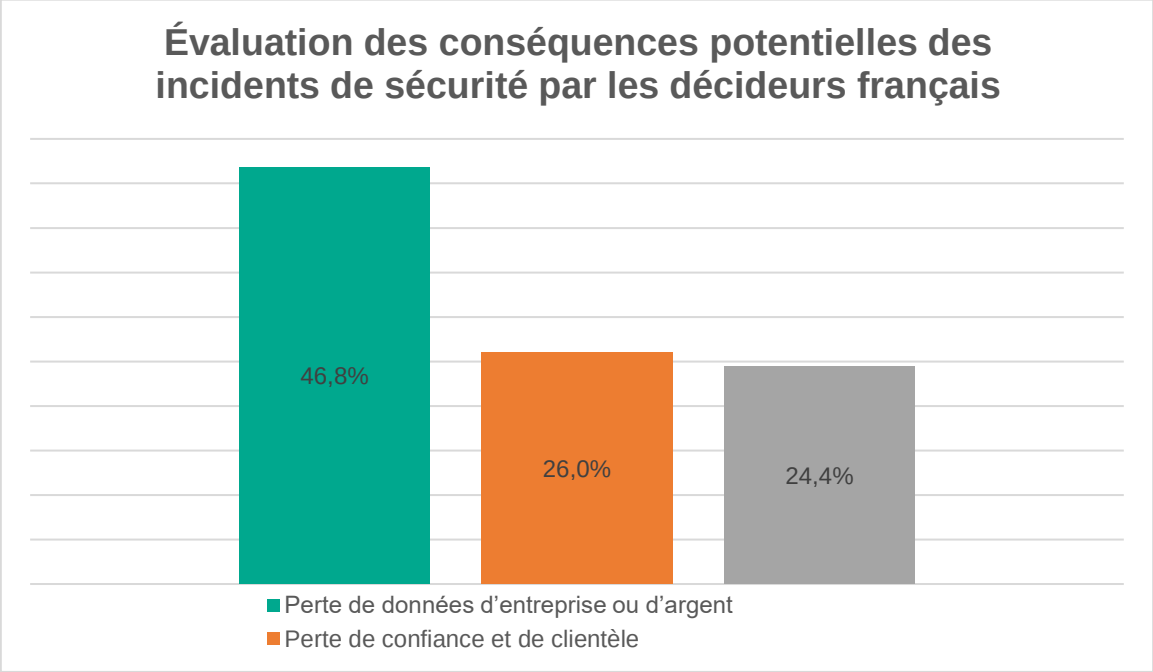
« En fait, il y a souvent un décalage entre les besoins (perçus) des décideurs d'entreprise et ce dont les équipes informatiques et de sécurité ont réellement besoin. C'est la conséquence d'un manque de connaissances approfondies sur la prise de décision. La solution est évidente : plus les décideurs investiront dans la lutte contre les cybermenaces de manière proactive, plus les retombées seront bénéfiques pour la sécurité de l'entreprise. »
Bertrand Trastour

Les cyberattaques ont souvent de graves conséquences

Les cybermenaces se complexifient de plus en plus, elles évoluent en permanence et menacent les performances des entreprises. Dans les entreprises, un incident de sécurité sur dix (qu'il s'agisse de programmes malveillants, d'attaques ciblées ou d'attaques contre les chaînes d'approvisionnement) est qualifié de grave.

Les décideurs interrogés dans le cadre de l'enquête évaluent différemment les conséquences potentielles des incidents de sécurité :

- Une personne sur deux (46,8 %) voit la perte de données de l'entreprise ou d'argent comme la pire conséquence d'une potentielle cyberattaque. Plus d'un quart des sondés (26 %) juge que la perte de confiance et de clientèle est la conséquence la plus grave. Ils sont presque aussi nombreux (24,4 %) à estimer que les mesures et enquêtes internes, les litiges ou les amendes constituent les plus graves répercussions d'un incident de sécurité.
- Au niveau européen, seul un tiers (36,7 %) des décideurs d'entreprise est convaincu que les ressources dédiées à la sécurité interne de l'entreprise sont suffisantes pour contrer efficacement les cybermenaces. 61,8 % des participants de l'étude pensent que leur organisation devrait compter au moins en partie sur l'aide d'experts externes en cas d'incident de sécurité.



Comment les décideurs d'entreprise sont-ils proactifs face aux cybermenaces actuelles

Voilà une autre raison pour laquelle les décideurs devraient se demander si leur investissement dans la prévention des cyberattaques est suffisant pour contrer toutes les menaces. Et s'ils ne regrettent pas d'accuser un certain retard en matière de technologies de pointe.

Dans l'enquête, près d'un tiers (30 %) des décideurs français admettent que leur entreprise n'investit pas assez dans les mesures préventives de cybersécurité. Plus de la moitié (51 %) des sondés sont satisfaits des investissements actuels et moins d'un sur cinq (18,9 %) les jugent trop élevés. En bref, les entreprises doivent réévaluer leur point de vue sur les investissements en matière de cybersécurité. Il ne s'agit pas de faire des économies sur l'utilisation d'une solution, mais de garantir la sécurité de toutes les ressources d'une organisation.

Cela vaut la peine d'investir dans des solutions de sécurité informatique externes : d'après l'étude, le pourcentage d'organisations victimes d'attaques alors qu'elles ont recours aux services de professionnels de la cybersécurité est inférieur de presque dix points à celui des entreprises qui travaillent avec des solutions de cybersécurité internes.

Par conséquent, les décideurs des entreprises de toutes tailles qui souhaitent protéger leur organisation de manière proactive et exhaustive contre les cybermenaces devraient songer à faire appel à un prestataire de services externe dont l'expérience en matière de cybersécurité est sans égal. Ils doivent anticiper la question de la cybersécurité et investir dans des solutions et des ressources adaptées. À défaut, ils risqueraient de se retrouver distancés par leurs concurrents.

À cet égard, Kaspersky est le partenaire idéal. Cette entreprise offre une combinaison de solutions de sécurité automatisées (Endpoint Detection and Response) et de systèmes MDR (Managed Detection and Response) grâce auxquels des experts en sécurité aident les professionnels à identifier et à neutraliser les cyberattaques dans les plus brefs délais. En ce qui concerne les grandes entreprises, le centre opérationnel de sécurité (SOC) et l'arrivée de systèmes de gestion des événements et des informations de sécurité (SIEM) augmentent également le niveau de sécurité. Fort d'une expertise qui n'est plus à démontrer en matière de solutions de détection au niveau des terminaux ainsi que de ses capacités de threat intelligence qu'il met au service de la recherche et de la détection de cybermenaces de tous types, qui reposent sur plus de 20 ans d'expérience de l'équipe d'experts GReAT (Global Research and Analysis Team), Kaspersky est le partenaire parfait pour aider les entreprises à mettre en œuvre une protection complète à l'épreuve du temps.

Kaspersky Endpoint Detection and Response

- Élimination des failles de sécurité et réduction des temps d'arrêt dus aux attaques
- Automatisation des tâches manuelles pendant la détection des menaces et l'intervention
- Allègement de la charge de travail du personnel des services informatiques, lui permettant de se consacrer à d'autres tâches essentielles
- Simplification de l'analyse des menaces et de la réponse aux incidents
- Réduction du temps nécessaire à la détection et au blocage des menaces
- Établissement de processus unifiés et efficaces de recherche des menaces, de gestion et de réponse aux incidents
- Augmentation de l'efficacité de votre centre d'opérations de sécurité interne : plus de perte de temps dans l'analyse des carnets de bords des terminaux.

Kaspersky Managed Detection and Response

- Un déploiement clé en main, rapide et évolutif, permettant d'obtenir une sécurité informatique mature instantanément sans qu'il soit nécessaire d'investir dans du personnel ou des compétences supplémentaires
- Une protection supérieure, même contre les menaces d'origine non malveillante les plus complexes et les plus innovantes, afin d'empêcher les interruptions d'activité et de réduire l'impact général des incidents
- Une réponse entièrement gérée ou guidée aux incidents, permettant une réaction rapide tout en gardant le contrôle total de toutes les actions
- Une visibilité en temps réel sur toutes vos ressources et leur statut de protection, assurant une connaissance situationnelle permanente à travers divers canaux de communication

kaspersky

Checklist : les étapes clés pour protéger les actifs de votre entreprise

Adopter la bonne approche au bon moment s'avère crucial pour protéger les actifs de l'entreprise et améliorer sa cybersécurité de manière proactive. Pour permettre aux décideurs de s'y retrouver dans le panorama des cybermenaces et de mettre en place des garde-fous et des processus adaptés en faisant appel à un partenaire de cybersécurité, Kaspersky vous suggère de suivre les six étapes clés ci-dessous.

Évaluez et comprenez les risques

Pour protéger votre entreprise, vous devez connaître tous les risques susceptibles de la menacer. Afin de mieux comprendre les cybermenaces qui pèsent sur votre entreprise, vous avez besoin d'une visibilité à 360 degrés sur l'intégralité du réseau de votre organisation. Cela requiert une approche combinant technologie et avis d'expert.

Les cybermenaces d'aujourd'hui sont multiples et sophistiquées. Elles vont des ransomwares aux APT, en passant par les attaques contre les chaînes d'approvisionnement et les violations de données. Mais en ce qui concerne la protection de l'intégrité des données et des actifs des entreprises, les cybermenaces ne sont pas les seuls risques susceptibles d'avoir des conséquences financières colossales et de porter atteinte à la réputation d'une entreprise. Les employés mécontents, les anciens salariés et même les clients peuvent présenter un risque si l'entreprise n'a pas mis en place des mesures adaptées pour protéger ses données et ses actifs.

Preuve que le problème peut atteindre des proportions considérables lorsqu'il n'est pas pris au sérieux : d'après une étude récente de Kaspersky, une violation de données découverte plus d'une semaine après une cyberattaque coûte un demi-million de dollars aux entreprises européennes (ce montant est inférieur pour les PME, il s'élève à 122 963 $). Les entreprises qui détectent instantanément une attaque, elles, en seraient quittes pour payer 213 737 $ (97 817 $ dans le cas d'une PME).

kaspersky

Posez les bonnes questions

En gardant cela à l'esprit, la prochaine étape cruciale en matière de cybersécurité consiste à poser les bonnes questions afin de s'assurer que tout a été examiné à la loupe pour créer un plan idoine. Cela commence par comprendre les processus métier les plus importants et les technologies clés dont ils dépendent, avant même d'évoquer les budgets et les solutions.

Comment l'infrastructure réseau est-elle actuellement gérée et sécurisée ? Quels sont les processus métier critiques et dans quels domaines un temps d'arrêt entraînerait-il une perte de chiffre d'affaire et une détérioration des relations ? Quel est le niveau de connaissance actuel des employés en matière de sécurité ? Comment les incidents de sécurité ont-ils été gérés et résolus par le passé ? Quelles sont les lacunes en termes de savoir et de compétences ?

Une approche orientée résultat aidera à déterminer les véritables priorités et à définir les investissements à réaliser en fonction des niveaux de protection nécessaires aux différents domaines d'activité.

Sensibilisez et responsabilisez les parties prenantes

La culture d'entreprise doit impérativement mettre l'accent sur la sécurité pour améliorer le niveau de cybersécurité dans toute l'entreprise. Dans ce but, chaque collaborateur au sein de l'organisation doit comprendre son rôle et ses responsabilités. Plus de la moitié des violations de sécurité étant dues à des menaces internes, l'absence de sensibilisation ou l'erreur humaine sont souvent à blâmer.

Il convient donc d'organiser des formations de sensibilisation et des exercices de rappel réguliers à tous les niveaux hiérarchiques, des apprentis aux cadres supérieurs, afin de vérifier qu'ils appliquent les conseils dispensés. Cela peut se faire en ligne et doit aborder les bonnes pratiques en matière de gestion des mots de passe, de sécurité de la messagerie électronique et de navigation Web sécurisée. Comprendre les risques ne suffit pas, encore faut-il savoir vers qui se tourner en cas de problème et disposer de directives et de recommandations claires afin que chacun prenne ses responsabilités.

Investissez dans la veille

S'il est important de veiller à ce que ses collaborateurs aient les compétences nécessaires pour repérer et empêcher une attaque, il est également essentiel de trouver une solution de cybersécurité performante et robuste afin d'assurer à son entreprise un avenir radieux. Cette approche holistique nécessite de disposer d'un certain niveau de Threat intelligence et d'être en mesure d'appliquer ses capacités d'analyse du big data au domaine de la sécurité. Sur la base d'informations exploitables concernant les menaces planant sur l'entreprise, il sera possible de faire évoluer les protocoles et processus en fonction de données utiles de manière à éviter aux entreprises d'être victimes de menaces ou d'incidents de sécurité à l'avenir. Pour disposer de cette veille automatisée cruciale, les décideurs doivent trouver le bon partenaire à l'expérience éprouvée qui saura automatiser la Threat intelligence afin de leur offrir une réactivité encore plus rapide.

Kaspersky soutient les entreprises en les informant des dernières menaces via notre Threat Intelligence Portal. On y trouve des données complètes sur les cyberattaques et les informations rassemblées par nos experts depuis plus de 20 ans.

kaspersky

Préparez-vous à réagir promptement

De nos jours, les cybercriminels sont doués, perfectionnés et perfides. Ils sont capables d'employer tous les moyens à leur disposition pour venir à bout des défenses de leurs victimes. La prévention seule ne suffit pas. Les organisations doivent être capables de réagir rapidement et fermement. Planifier, s'entraîner et s'assurer de la pertinence des outils de sécurité mis en place est vital.

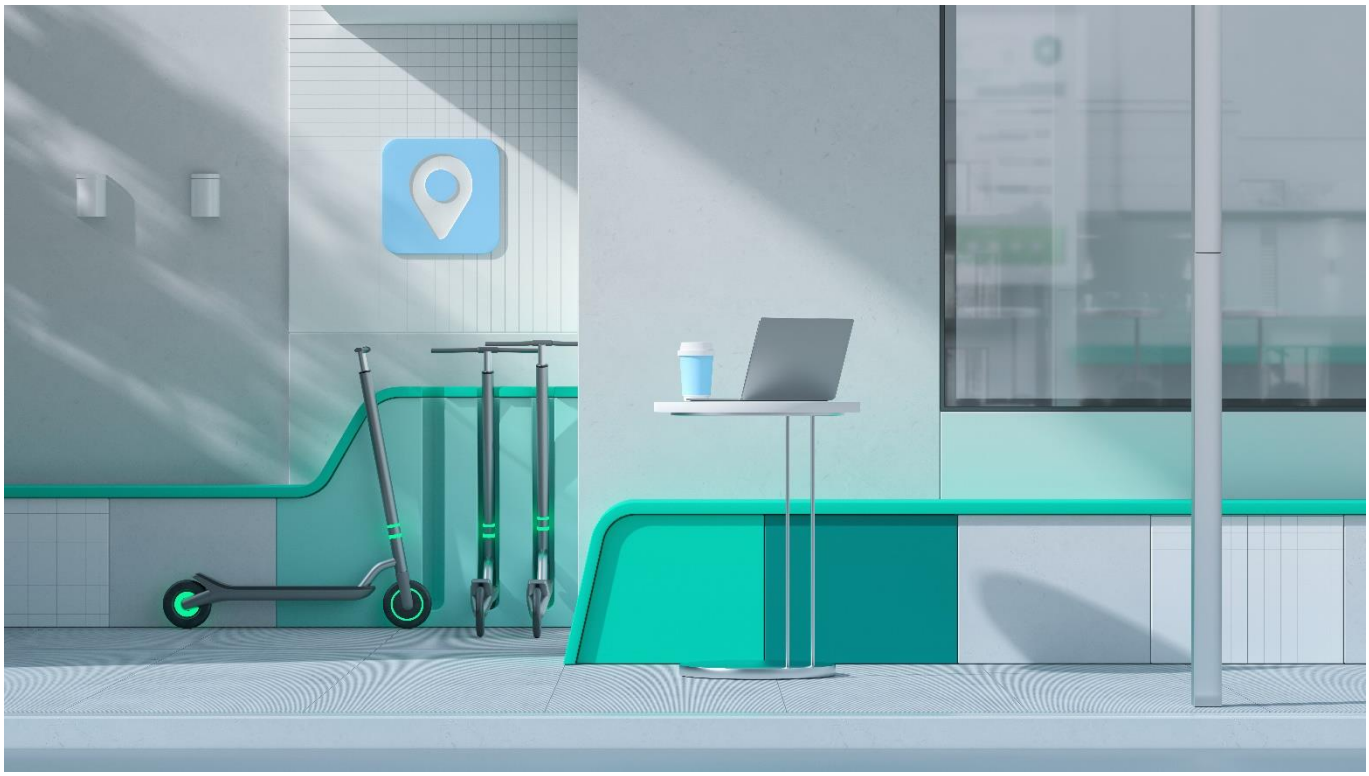
Des solutions telles que Kaspersky Endpoint Detection and Response et Kaspersky Managed Detection and Response peuvent contribuer à identifier, investiguer et résoudre promptement les incidents sur tous les terminaux des employés. Cela est d'autant plus important que l'utilisation d'appareils personnels se démocratise, surtout avec la pandémie et le recours prolongé au télétravail.

Examinez et actualisez les protocoles

Les menaces pour la sécurité, tant externes qu'internes, sont en constante évolution. Par conséquent, vos protocoles et vos processus doivent suivre le même rythme pour ne pas se laisser distancer. Les protocoles de sécurité doivent être examinés et actualisés régulièrement pour aider à déjouer les menaces informatiques et à s'en remettre.

La collaboration avec des experts tiers extérieurs à l'entreprise peut aider à maintenir à jour les protocoles et à assurer leur pérennité malgré l'évolution de l'activité et du panorama des cybermenaces.

Avec un partenaire de cybersécurité qui bénéficie d'une visibilité complète basée sur son expertise, qui vous tient au courant des menaces actuelles et qui vous fournit une plateforme unifiée tout-en-un, vous pouvez vous concentrer sur l'innovation, sans crainte.



kaspersky

Quelle est la protection la plus adaptée à votre entreprise ?

	EDR automatisé	EDR Optimum	Portail Web	Expert XDR/EDR
Ressources informatiques dont vous disposez	Vos ressources informatiques sont limitées.	En plus de l'administration de l'infrastructure, certains salariés de votre service informatique sont chargés de la gestion de la sécurité et de l'analyse lorsque cela s'avère nécessaire.	Vos ressources informatiques sont limitées.	En plus du service informatique classique, vous disposez d'une équipe dédiée à la sécurité informatique.
Expertise en matière de sécurité dont vous disposez	Vous n'avez pas de collaborateur dédié à la sécurité informatique et vous ne prévoyez pas d'approfondir vos connaissances en matière de sécurité.	Vous avez déjà une petite expérience de l'analyse d'incident ou êtes en train de vous forger votre propre expertise en matière de sécurité au sein de votre entreprise.	Vous ne souhaitez pas acquérir votre propre expertise en matière de sécurité informatique, que ce soit maintenant ou à long terme. Néanmoins, afin de bénéficier du meilleur niveau de protection possible, vous seriez prêt à externaliser cette tâche à un prestataire de services 24 h/24.	Vos collaborateurs disposent d'une bonne, voire très bonne expertise en matière de sécurité. Vous êtes en train de mettre en place une équipe d'experts dédiée ou avez déjà organisé la question de la détection et de la défense au sein d'un centre opérationnel de sécurité (SOC).

kaspersky

www.kaspersky.fr/
www.securelist.com