7 VÉRITÉS QUI DÉRANGENT

SUR LA SÉCURITÉ DES SYSTÈMES

Résultats d'une enquête indépendante réalisée auprès de 3 100 responsables informatiques à la demande de Sophos

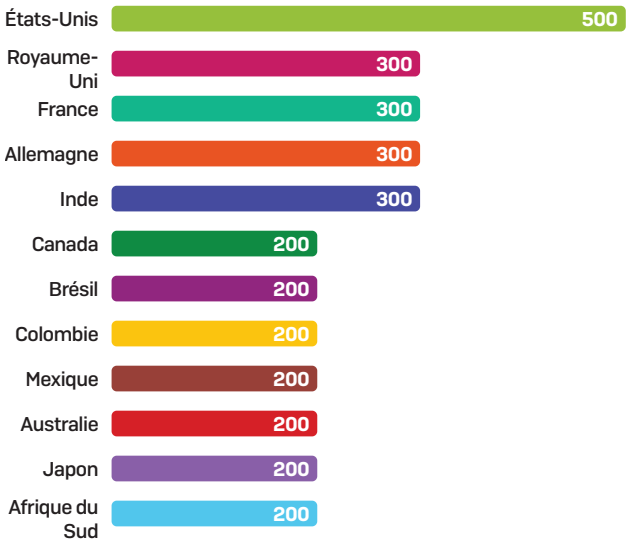
Pour comprendre les réalités de la sécurité des systèmes aujourd'hui, Sophos a demandé au cabinet d'études indépendant Vanson Bourne de mener une enquête auprès de 3 100 responsables informatiques dans le monde entier. Ce compte-rendu présente les expériences, les préoccupations et les projets futurs d'entreprises réparties dans douze pays sur six continents. Il analyse de manière approfondie les défis quotidiens auxquels les équipes informatiques sont confrontées pour protéger leur entreprise contre les cyberattaques, ainsi que leurs expériences avec les technologies EDR (Endpoint Detection and Response).

SOPHOS

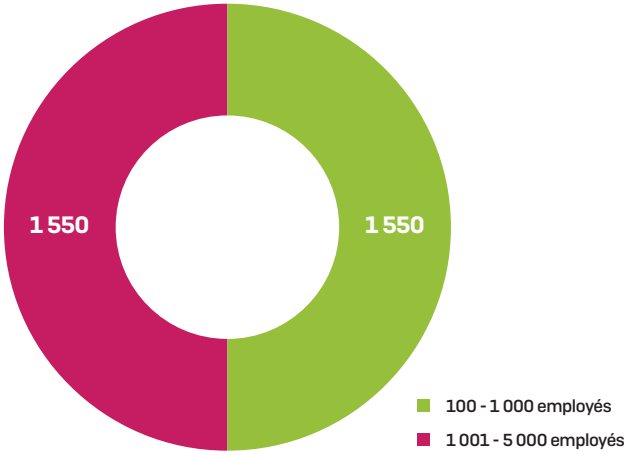
L'enquête

Le cabinet d'études britannique Vanson Bourne a interrogé 3 100 décideurs informatiques entre décembre 2018 et janvier 2019. Afin de fournir une répartition par taille représentative dans chaque pays, les participants ont été classés de manière équitable entre des entreprises allant de 100 à 1 000 utilisateurs et de 1 001 à 5 000 utilisateurs.

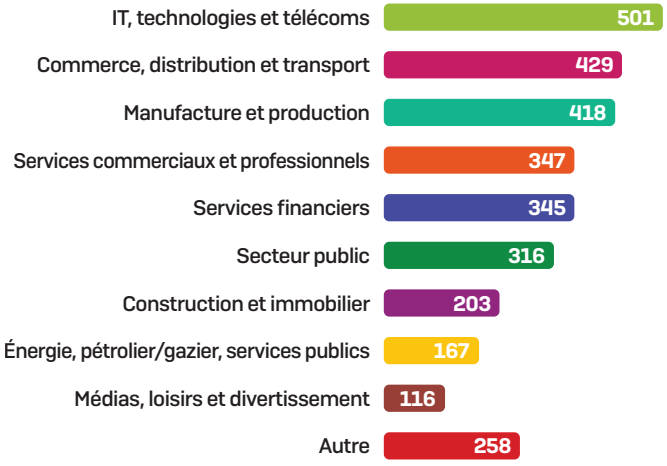
Nombre de participants par pays



Répartition des participants par taille d'entreprise



Répartition des participants par secteur



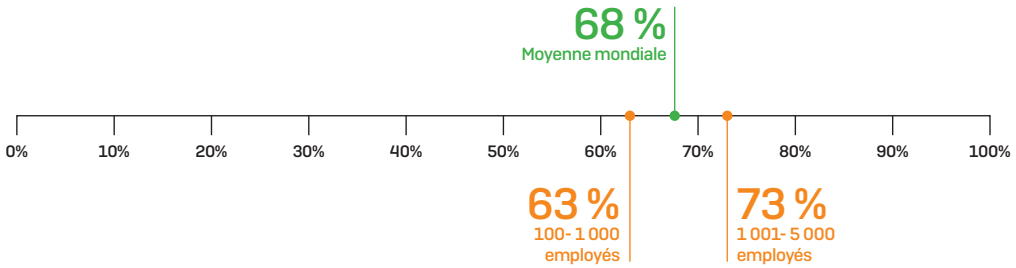
Vérité nº 1 : Être victime d'une cyberattaque est devenu monnaie courante

Plus des deux tiers (68 %) des entreprises affirment avoir été victimes d'une cyberattaque au cours des douze derniers mois. Les grandes entreprises ont subi plus d'attaques (73 %) que les petites (63 %). Cette différence peut s'expliquer par deux facteurs :

- Les cybercriminels ciblent davantage les grandes organisations, qui sont considérées comme des victimes plus lucratives.
- Les grandes entreprises sont plus conscientes qu'elles ont été affectées, car elles disposent de plus de ressources informatiques pour détecter et analyser les problèmes.

Définition : Être victime d'une cyberattaque

Subir une cyberattaque que l'organisation est incapable de maîtriser et qui pénètre sur son réseau et/ou ses systèmes d'extrémité

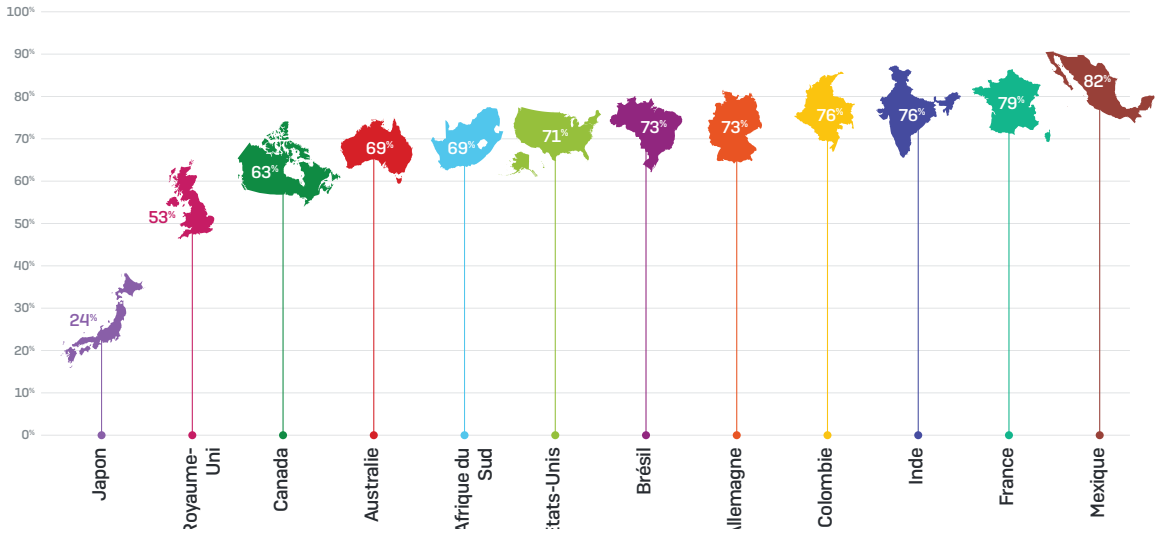


Pourcentage des entreprises ayant été victimes d'une cyberattaque au cours des douze derniers mois. Question posée à tous les participants (3 100)

Naturellement, il ne s'agit là que des attaques découvertes par les entreprises. Le nombre réel pourrait être bien plus élevé.

L'élément-clé à retenir ici est que **chaque entreprise devrait partir du principe qu'elle sera victime d'une cyberattaque**. Commencez donc de ce point de vue au moment de planifier et d'évaluer votre stratégie de sécurité, plutôt que de supposer que les menaces ne vous atteindront pas ou que vous éviterez l'attention des pirates.

Le niveau des cyberattaques varie considérablement d'un pays à l'autre. Le Japon a rapporté le moins d'attaques avec seulement 24 % des entreprises victimes d'une cyberattaque l'an dernier, tandis que le Mexique en a signalé le plus avec 82 % des interrogés ayant déclaré avoir été touchés.



Pourcentage des entreprises victimes d'une cyberattaque au cours des douze derniers mois, réparties par pays. Question posée à tous les participants (3 100)

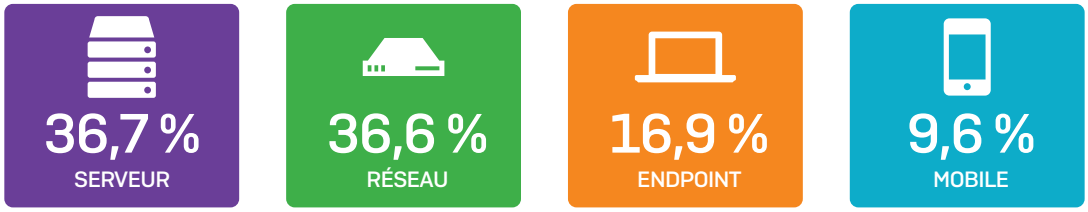
Cette différence s'explique entre autres par le fait que les cibles des cyberattaques ne sont pas équitablement distribuées dans le monde. Si l'on examine chaque menace de manière individuelle, on constate souvent qu'elle vise clairement une zone géographique spécifique. Par exemple, jusqu'à aujourd'hui, Emotet a ciblé plus particulièrement les Amériques, l'Europe du Nord et l'Europe de l'Ouest, l'Australie et l'Inde, tandis que WannaCry a provoqué le plus de ravages en Ukraine.

Contrairement à la foudre, les cybermenaces frappent deux fois

Qui plus est, les entreprises victimes d'une cyberattaque l'ont été en moyenne à deux reprises. Et 10 % des interrogés déclarent avoir subi au moins quatre cyberattaques ou plus l'an dernier. Cela montre que bon nombre d'entreprises présentent de manière permanente des failles exploitables dans leurs systèmes de défense.

La plupart des attaques sont détectées sur le serveur ou le réseau

Si l'on examine où les entreprises découvrent les attaques au sein de leur environnement, on obtient un certain nombre d'informations intéressantes.



Endroit où les entreprises ont détecté/découvert la cyberattaque la plus virulente dont elles ont été victimes l'an dernier.
Question posée aux entreprises ayant été victimes d'une cyberattaque au cours de l'an dernier (2 109)

1. La plupart des menaces (36,7 %) sont découvertes sur le serveur

En général, les serveurs sont considérés comme « sûrs » par les administrateurs informatiques, car les utilisateurs ne s'y connectent pas. Cependant, les données montrent qu'ils sont les plus exposés. Les systèmes d'extrémité sont souvent le point d'entrée des attaques modernes, qui ensuite se déplacent vers les serveurs, les cibles les plus convoitées. Le fait que les entreprises détectent les menaces sur les serveurs plutôt que sur les systèmes d'extrémité indique un manque de visibilité sur ce qui se passe en amont de la chaîne des menaces, mais aussi des failles de sécurité au niveau des systèmes d'extrémité. Il est aussi probable que les attaques sur le serveur sont identifiées, car c'est là qu'elles peuvent alors le plus de répercussions sur l'entreprise.

2. Près d'une menace sur 10 est découverte sur les appareils mobiles

Avec 9,6 % des menaces détectées sur les portables, les informations recueillies montrent que les menaces mobiles représentent un danger important. Les entreprises doivent donc veiller à ce que tous les appareils ayant accès à leurs données soient correctement sécurisés.

3. En Inde, deux fois plus de menaces sur les mobiles

Alors que la moyenne mondiale des menaces détectées sur les mobiles est de 9,6 %, en Inde ce chiffre est presque multiplié par 2 avec 18,8 %. Ce phénomène s'explique à la fois par des facteurs technologiques et culturels. Dans ce pays, neuf portables sur dix fonctionnent sur Android, la plateforme de prédilection des auteurs de malwares. Les mobiles indiens sont donc particulièrement vulnérables aux menaces. De plus, l'Inde affiche l'un des taux les plus élevés d'installation de mauvaises applications, ce qui accroît leur propension aux infections mobiles. Enfin, il est beaucoup plus courant que dans d'autres pays de n'utiliser que des appareils mobiles pour les affaires. Pas étonnant donc que les mobiles se retrouvent davantage victimes d'attaques malveillantes.

https://economictimes.indiatimes.com/tech/software/the-critical-flaw-in-indias-mobile-security/articleshow/65085273.cms

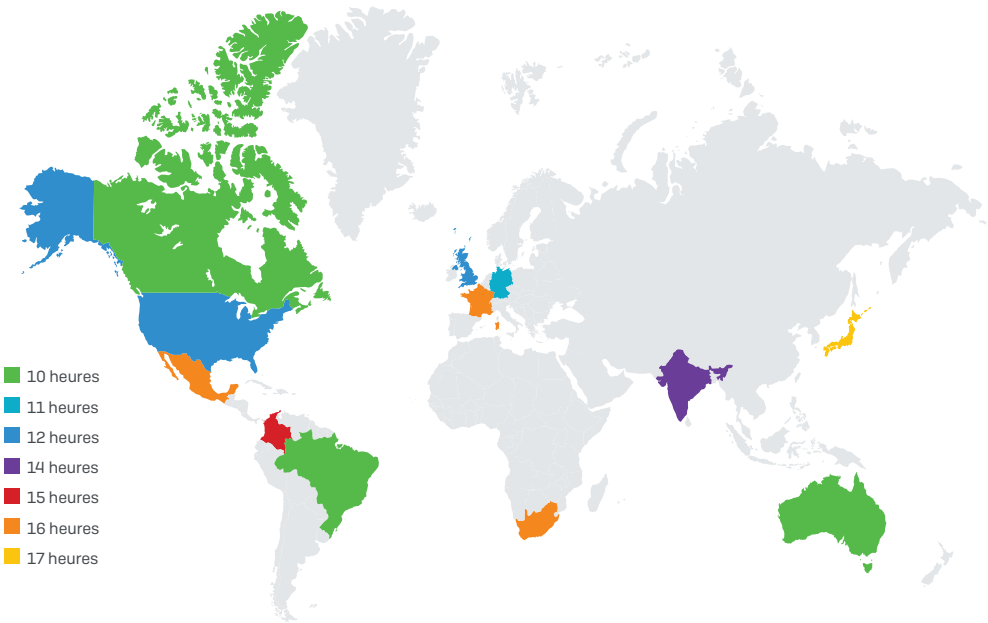
Vérité nº 2 : Les équipes informatiques manquent de visibilité sur le délai d'action de l'attaquant

Nous avons demandé aux entreprises combien de temps il leur avait fallu pour découvrir la cyberattaque la plus virulente pour elles l'an dernier. Pour celles qui connaissaient la réponse, la moyenne était de 13 heures.

Durée moyenne pendant laquelle la menace la plus virulente résidait dans leur environnement avant d'être détectée

Cela représente évidemment une durée colossale pour un pirate informatique qui dispose d'un accès ininterrompu à vos systèmes et à vos données. Dans ce laps de temps, un cybercriminel peut causer des dommages très importants, en s'emparant par exemple de données sensibles, en volant des identifiants de connexion, en installant des chevaux de Troie pour dérober des fonds, en installant des ransomwares, etc.

Le temps nécessaire à la détection des menaces varie d'un pays à l'autre : l'Australie, le Brésil et le Canada sont les plus rapides à réagir, avec 10 heures en moyenne tandis que les équipes informatiques japonaises ont elles besoin de 17 heures en moyenne.



Durée moyenne pendant laquelle la menace la plus importante était présente dans l'entreprise avant sa détection. Question posée à tous les responsables qui savaient depuis combien de temps la menace était présente dans leur environnement (1 744 participants)

Treize heures n'est que le sommet de l'iceberg

Si 13 heures représentent une durée importante, rappelons qu'il s'agit là du meilleur des cas.

Ce délai d'action moyen de 13 heures, cité par les 1 744 interrogés qui savaient depuis combien de temps la menace résidait dans leur environnement avant d'être détectée, peut sembler à première vue erroné par rapport à d'autres références, telles que le rapport d'enquête sur la violation des données de Verizon qui indique que 68 % des violations de données prennent plusieurs mois, voire plus, avant d'être découvertes. Cette différence de données est très révélatrice et permet de mieux comprendre les réalités auxquelles sont confrontées les entreprises qui ne disposent pas d'une équipe robuste dédiée à la détection et à la réponse aux menaces.

Pour 17 % des menaces, les entreprises ignorent depuis combien de temps elles étaient présentes dans leur environnement avant d'être détectées.

Les entreprises ne voient qu'une partie de l'iceberg. Comme nous l'avons vu précédemment, la plupart des menaces sont découvertes sur le serveur, ce qui suggère un manque de visibilité sur les systèmes d'extrémité. Il est donc fort probable que les entreprises ne voient qu'une partie du circuit de la menace, et par conséquent sous-estiment sa durée au sein de leur environnement. Leurs décisions de sécurité sont donc basées sur des informations partielles et une compréhension incomplète des risques.

Les entreprises ne disposent pas des outils requis pour évaluer avec précision le délai d'action. Pour la grande majorité des petites et moyennes entreprises, pour bien évaluer la durée d'une menace dans leur système, il faut du temps, des outils et des compétences qu'elles n'ont pas.

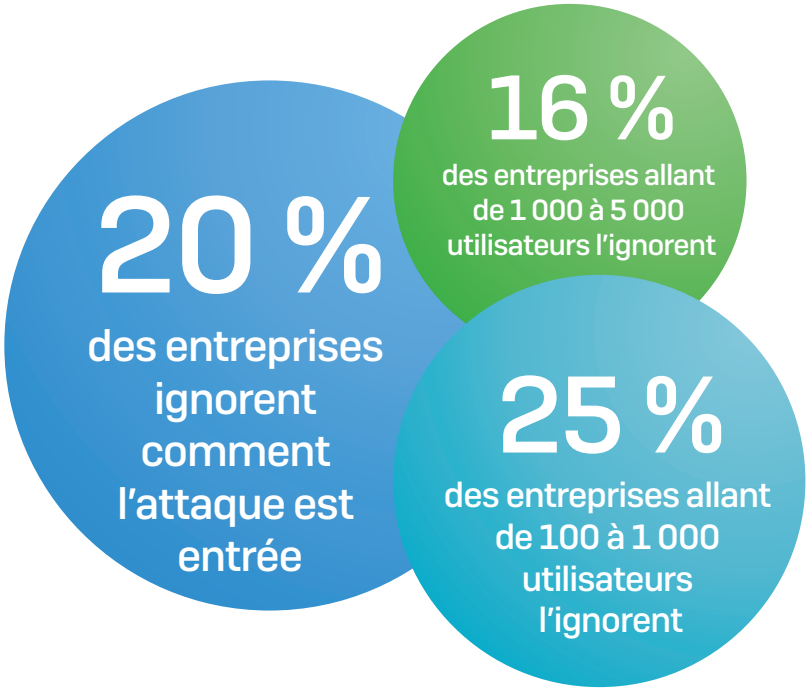
Certains types de menaces sont plus faciles à détecter que d'autres. Ils varient considérablement en termes de méthodes de distribution, de techniques utilisées et d'objectifs. Les menaces génériques de type « spray-and-pray » qui réussissent en partie grâce à leur volume (leur principe : si j'envoie suffisamment d'attaques, l'une d'elles passera) sont généralement moins bien déguisées que les attaques discrètes, sophistiquées et très ciblées. Et en réalité, beaucoup de ces menaces de masse sont détectées et stoppées en quelques secondes.

Le rapport de Verizon portait uniquement sur les violations de données, tandis que les participants à l'enquête Sophos ont répondu sur la base d'un éventail plus large de cyberattaques. Les menaces causant le plus d'impact et de dommages sont souvent les plus sophistiquées, avec le plus long délai d'action.

Les cybercriminels étant devenus des professionnels du camouflage, les décideurs informatiques savent parfaitement qu'ils doivent pouvoir identifier les attaques complexes et sophistiquées occasionnant les plus gros dégâts. Les participants à l'enquête ont en effet déclaré que la fonctionnalité la plus importante d'une solution EDR (Endpoint Detection and Response) était sa capacité à identifier des événements suspects.

Vérité nº 3 : Les équipes informatiques ne peuvent pas combler leurs lacunes en matière de sécurité, car elles ne les connaissent pas

L'un des objectifs premiers d'une stratégie de sécurité efficace est d'empêcher les menaces de pénétrer au sein de l'entreprise. Pourtant, un décideur informatique sur cinq avoue ne pas savoir comment la cyberattaque la plus grave qu'ils aient subie est entrée dans leur système. Ils ne peuvent donc pas protéger ces points d'entrée de manière adéquate.



Pourcentage d'interrogés qui ne savent pas comment la cyberattaque la plus virulente a pénétré leur entreprise. Question posée à tous les participants ayant été victimes d'une cyberattaque au cours des douze derniers mois (2 109)

Les grandes entreprises sont plus à même que les petites de savoir comment les menaces sont entrées. Cela s'explique à la fois par des ressources plus qualifiées et des solutions de cybersécurité plus complètes que les PME. Souvent, les plus petites entreprises n'ont tout simplement pas les ressources ni les compétences pour rechercher ce qui s'est passé lors d'une attaque. Elles se focalisent juste sur le nettoyage. Les cybercriminels visent les organisations de toutes tailles, mais l'incapacité des petites entreprises à identifier leurs failles de sécurité font qu'elles sont plus vulnérables.

Vérité nº 4 : Les entreprises perdent 41 jours par an à enquêter sur de faux problèmes

Les entreprises passent en moyenne quatre jours par mois à analyser des problèmes de sécurité potentiels, soit 48 jours par an. Mais seulement 15 % se révèlent être de véritables infections. Elles consacrent donc 85 % de leur temps à enquêter sur de faux problèmes, ce qui revient à environ 41 jours par an. Cette situation a évidemment des implications importantes en matière de budget et de productivité.

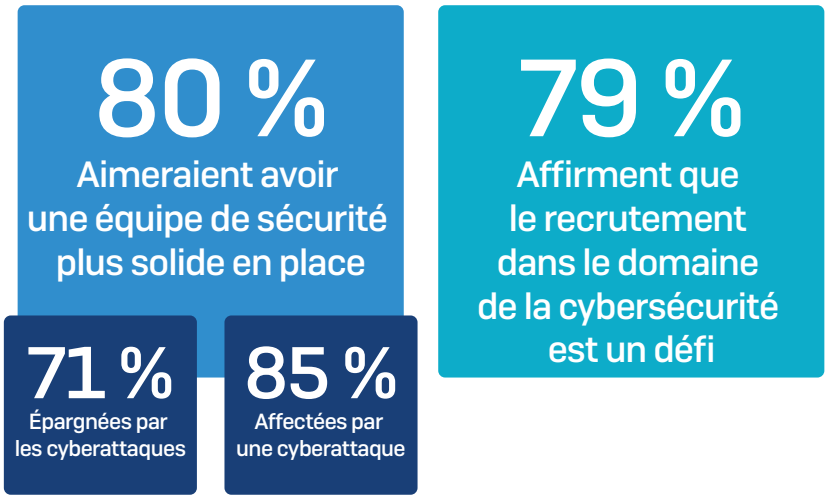
- Coût direct : le temps perdu à enquêter sur de faux problèmes a des répercussions sur les finances et sur les ressources.
- Coût d'opportunité : le personnel informatique qui doit enquêter sur de faux problèmes ne peut pas se consacrer à d'autre tâches.

Cette énorme perte de productivité explique également pourquoi l'identification d'événements suspects est la fonctionnalité EDR la plus recherchée. En mettant en place des outils efficaces pour identifier ce qui est suspect, les entreprises peuvent concentrer leurs ressources limitées aux bons endroits, au lieu de chercher des « aiguilles dans une botte de foin ». Mieux identifier les événements suspects permettra aux entreprises de :

- Améliorer leur efficacité, en utilisant plus efficacement leurs ressources limitées
- Réduire leur exposition, en localisant et en réagissant aux incidents de sécurité plus rapidement
- Minimiser les risques, en focalisant leurs ressources sur les événements suspects susceptibles de mettre l'entreprise en danger

Vérité nº 5 : Quatre entreprises sur cinq ont du mal à détecter les menaces et à réagir, car elles manquent d'expertise en matière de sécurité

Le manque d'expertise en sécurité face à ces menaces constitue un problème majeur. Avec 80 % des décideurs informatiques affirmant vouloir une équipe plus solide pour détecter, analyser et répondre correctement aux incidents de sécurité, il est clair que les entreprises opèrent à l'aveugle par manque de compétences en cybersécurité.



Il existe un écart marqué dans le souhait d'avoir une équipe plus solide entre les entreprises victimes d'une cyberattaque (85 % souhaitent une équipe plus solide) et celles qui ne l'étaient pas (71 % souhaitent une équipe plus solide). Cela indique que les entreprises ayant subi une attaque montrent une plus grande prise de conscience, à la fois de leur propre manque d'expertise en sécurité (elles ont appris à leurs dépens que les menaces peuvent pénétrer leurs défenses), mais aussi des défis à relever pour stopper les attaques avancées actuelles et des compétences en cybersécurité requises pour les contrer.

Malheureusement, trouver une solution à cette pénurie de compétences n'est pas une tâche facile. Même si les entreprises reconnaissent avoir besoin d'une plus grande assistance en la matière, la trouver est une autre affaire. En effet, pour 79 % des interrogés, recruter du personnel qualifié en cybersécurité reste un défi. C'est pourquoi les entreprises ont beaucoup de mal à mettre en place les équipes dont elles ont besoin et elles vont se pencher sur des technologies telles que l'intelligence artificielle pour combler ces lacunes.

Vérité nº 6 : Plus de la moitié des entreprises ne perçoivent pas les avantages de leur solution EDR

L'EDR est rapidement devenu une technologie incontournable. Plus de neuf décideurs informatiques sur dix (93 %) disposent ou envisagent d'acquérir une fonctionnalité EDR pour leur arsenal de sécurité. Parmi les interrogés qui ne possèdent pas d'outils EDR, 89 % prévoient de l'ajouter à leur système de défense et 61 % prévoient de le faire dans les six prochains mois. Si l'on considère les données précédentes sur le temps passé à analyser des incidents de sécurité et le manque de visibilité sur la chaîne des menaces, ces projets EDR sont parfaitement logiques.

93 %
souhaitent l'EDR dans leur arsenal de sécurité

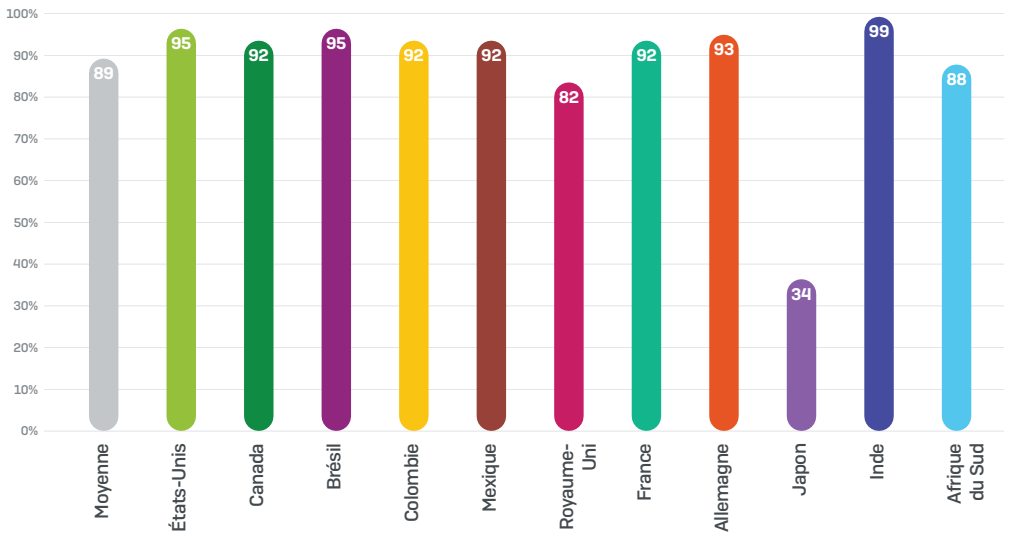
9 sur 10
sans EDR prévoient de l'ajouter

61 %
sans EDR prévoient de l'ajouter dans les six prochains mois

L'EDR pour tous
Demande identique pour les grandes et les petites entreprises

Fait intéressant, la demande pour l'EDR est presque identique chez les petites et les grandes entreprises. Elle n'est plus l'exclusivité des grandes entreprises, mais plutôt un outil destiné à tous.

Parmi les pays étudiés, le Japon reste à part dans ses projets d'adoption de l'EDR.



Pourcentage des interrogés qui envisagent d'ajouter la fonction EDR. Question posée à tous les participants qui ne disposent pas actuellement de l'EDR (1 990)

Dans tous les autres pays, au moins huit entreprises sur dix ne disposant pas de la technologie EDR prévoient de l'ajouter. L'Inde arrive en tête de la liste avec 99 % des entreprises n'ayant pas l'EDR qui prévoient de l'ajouter, suivie de près par l'Australie (97 %), les États-Unis et le Brésil (tous deux à 95 %). Au Japon, seule une entreprise sur trois (34 %) sans technologie EDR envisage de l'ajouter à sa stratégie de sécurité.

La technologie EDR seule ne suffit pas

Même si l'EDR est un outil puissant capable de renforcer vos cyberdéfenses, vous devez disposer des ressources adéquates pour l'utiliser efficacement et tirer le meilleur parti de votre investissement. Malheureusement, plus de la moitié des interrogés ayant investi dans cette technologie ne savent pas l'utiliser. Pour 54 % des entreprises, l'EDR est en réalité un gaspillage financier, car elles n'arrivent pas en tirer profit.

54 %

n'arrivent pas exploiter tous les avantages de leur solution EDR

Fait intéressant : bien que l'on pourrait penser que les petites entreprises aient plus de mal à exploiter leur investissement dans la technologie EDR, les faits montrent que la taille de l'organisation n'est pas un facteur déterminant. Les réponses recueillies étaient quasiment identiques, quelle que soit la taille de l'entreprise.

Deux raisons principales expliquent ces résultats, qui s'appliquent probablement à toutes les entreprises interrogées :

Le manque de ressources en gestion de l'EDR. Les entreprises doivent déterminer qui administrera leur solution EDR pour pouvoir pleinement l'exploiter. Comme nous l'avons déjà vu, le manque de compétences en cybersécurité est un problème répandu.

La complexité et l'inadéquation des compétences Toute technologie ne présente de l'intérêt que si elle peut être utilisée de manière efficace. Il est donc impératif de tenir compte de la facilité d'utilisation de la solution EDR, mais aussi de son adéquation avec les compétences et les ressources disponibles.

Vérité n° 7 : Chat échaudé craint l'eau froide — Les victimes apprennent à leurs dépens.

L'enquête a révélé des différences très nettes dans certains domaines entre les entreprises qui avaient été victimes d'une cyberattaque et celles qui avaient su éviter les pirates. Ce qui caractérise les victimes d'une cyberattaque l'an dernier :

- Elles sont plus vigilantes : elles examinent deux fois plus d'incidents que les autres entreprises.
- Elles consacrent plus de temps à la cybersécurité : elles passent en moyenne quatre jours par mois à analyser des incidents potentiels, au lieu de trois jours pour les non-victimes.

x 2
investigations sur les incidents

1/3
de leur temps perdu en plus

Plusieurs facteurs sont en jeu ici :

1. **Elles ont renforcé leur sécurité après l'incident.** Les victimes ont probablement une bien meilleure idée de l'impact des cyberattaques et sont disposées à consacrer plus de temps, d'efforts et de ressources pour les stopper.
2. **Elles ont une visibilité limitée sur leur environnement.** Une cybersécurité médiocre signifie qu'un plus grand nombre de menaces pénètrent leur système et qu'elles ont moins de possibilités de les examiner. Elles ont donc plus d'incidents potentiels à analyser, avec moins d'outils pour le faire, ce qui nécessite plus de temps.
3. **Elles sont davantage conscientes de ce qu'il faut rechercher.** Les entreprises qui ont subi une attaque sont davantage conscientes des signes qui doivent les alerter.

La vérité sur l'EDR

Cette enquête a révélé un certain nombre de défis auxquels sont confrontées les entreprises du monde entier en matière de sécurité des systèmes, mais aussi de technologie EDR. Alors que pouvons-nous conclure sur l'EDR et comment s'intègre-t-elle dans la protection Endpoint ?

Les faits montrent que l'EDR peut aider à résoudre bon nombre des problèmes mis en avant par l'enquête. À commencer par mieux comprendre les cyberattaques. Deux entreprises sur trois ont subi une cyberattaque l'année dernière. Or 17 % des responsables informatiques ne savent pas depuis combien de temps la menace résidait dans leur environnement et 20 % ne savent pas comment elle est entrée. Les outils EDR peuvent apporter des réponses à ces questions, permettant aux entreprises d'identifier la cause première de l'attaque, son temps passé dans le système et son impact potentiel. Grâce à ces informations, elles peuvent mettre en place les défenses dont elles ont besoin et combler leurs failles de sécurité.

Nous avons également constaté qu'il faut en moyenne 13 heures aux entreprises pour détecter une menace. L'EDR peut également identifier de manière proactive les événements suspects, ce qui permet aux équipes informatiques de détecter les attaques passées inaperçues depuis longtemps. L'EDR permet donc de prendre des mesures efficaces pour réduire les risques de devenir une nouvelle victime.

Autre chiffre important qui ressort également de l'enquête : les entreprises passent en moyenne 48 jours par an à analyser des incidents de sécurité potentiels. La technologie EDR peut vraiment alléger cette durée en proposant des analyses approfondies et des investigations guidées sur les incidents potentiels que les équipes de sécurité, de tous niveaux, peuvent comprendre et prendre en charge. Cela réduit considérablement le temps passé à détecter et à répondre aux incidents.

Mais nous avons également constaté que 54 % des entreprises disposant de la fonctionnalité EDR ne savent pas comment l'utiliser pour en tirer pleinement profit. C'est pourquoi il est impératif de choisir une solution EDR qui convienne à votre organisation plutôt qu'une solution qui ne fera qu'ajouter une charge de travail supplémentaire. Une solution EDR correctement mise en œuvre peut aider les entreprises à utiliser plus efficacement leurs ressources limitées.

Conclusion

La cybersécurité est un défi permanent pour les entreprises de toutes tailles à travers le monde. Dans ce contexte, les expériences des 3 100 responsables informatiques interrogés dans douze pays sur les six continents nous permettent de tirer plusieurs conclusions importantes :

Premièrement, lors de la planification de leur stratégie de sécurité, les entreprises doivent partir du principe qu'une menace finira par réussir à passer leurs défenses. Ce faisant, elles doivent également être conscientes de leur visibilité très limitée sur les menaces et de leur incapacité à identifier — et à combler — leurs failles dans leur dispositif de sécurité.

Deuxièmement, la grande majorité des entreprises considèrent la fonctionnalité EDR comme une partie intégrante de leur stratégie de sécurité. Ce n'est pas surprenant. L'EDR est un outil efficace capable de répondre à de nombreux problèmes présentés dans cette enquête. Alors qu'aujourd'hui, les compétences en matière de cybersécurité sont rares, une solution EDR intelligente peut apporter les informations clés et l'expertise nécessaires pour garder une longueur d'avance sur les menaces.

Néanmoins, comme l'a révélé l'enquête, le simple fait d'acquérir la technologie EDR ne suffit pas. Pour beaucoup trop d'entreprises, leur investissement dans l'EDR se révèle être un gaspillage, car elles ne sont pas en mesure d'exploiter pleinement leur solution. Pour éviter de tomber dans ce piège, chaque entreprise doit prendre en compte à la fois les fonctionnalités et la simplicité d'utilisation de la solution EDR avant de l'ajouter à son arsenal de sécurité.

À propos de Sophos

Sophos est un leader mondial de la sécurité des réseaux et des systèmes. Plus de 100 millions d'utilisateurs dans 150 pays ont retenu Sophos comme la meilleure protection contre les menaces complexes et les risques de pertes de données. **Intercept X Advanced with EDR** permet aux entreprises de comprendre la portée et l'impact des incidents de sécurité, de détecter les attaques passées inaperçues, d'analyser les fichiers pour déterminer s'ils constituent une menace et de rendre compte de manière fiable de l'état de leur sécurité à tout moment. Le Machine Learning intégré et l'intelligence sur les menaces des SophosLabs vous permettent d'élargir vos compétences sans avoir à recruter. Pour en savoir plus et bénéficier d'un essai gratuit de 30 jours, visitez notre pagewww.sophos.fr/intercept-x.

À propos de Vanson Bourne

Vanson Bourne est un cabinet d'études de marché indépendant spécialisé dans le secteur des technologies. Sa réputation d'analyste solide et crédible repose sur des principes de recherche rigoureux et sur sa capacité à solliciter l'avis des décideurs de haut niveau dans les domaines techniques et commerciaux, dans tous les secteurs d'activité et sur l'ensemble des marchés dominants. Pour en savoir plus, consultez leur site www.vansonbourne.com.

Pour commencer votre essai EDR gratuit de 30 jours, rendez-vous sur notre page www.sophos.fr/intercept-x

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

2019-02-26 WPFR (RP)

SOPHOS