ÉTUDE DE L'IMPACT SUR LA SÉCURITÉ DES API 2024

Comment les incidents liés aux API ont un impact sur vous et votre équipe

Akamai

Une publication affiliée aux
rapports d'Akamai sur l'état des lieux d'Internet (SOTI)

Table des matières

Synthèse

La troisième édition de l'étude de l'impact sur la sécurité des API (anciennement rapport Déconnexion de la sécurité des API) explore l'état de la protection des API, en se fondant sur une enquête menée auprès de 1 207 dirigeants et praticiens aux États-Unis, au Royaume-Uni et, pour la première fois en 2024, en Allemagne. L'étude examine comment les entreprises vivent les événements liés à la sécurité des API, leur fréquence, leurs causes et leurs impacts, et comment les services de sécurité abordent les API en tant que vecteur d'attaque.

Pour obtenir une vue d'ensemble, nous avons interrogé un ensemble équilibré de :

RSSI, DSI, CTO, professionnels seniors de la sécurité et membres d'équipes de sécurité des applications dans des entreprises dont la taille varie de moins de 500 à plus de 1 000 personnes

Huit secteurs d'activité : les services financiers, la vente au détail/le commerce électronique, la santé, le gouvernement/le secteur public, la fabrication, l'énergie/les services publics, et pour la première fois cette année, l'automobile et l'assurance

Introduction

Les API sont souvent considérées comme un *nouveau* vecteur d'attaque, même si les données montrent qu'elles sont répandues et nuisibles. Considérons ces statistiques :

- 108 milliards d'attaques d'API ont été enregistrées entre janvier 2023 et juin 2024, selon un récent rapport État des lieux d'Internet d'Akamai.
- « Les données actuelles indiquent qu'une violation des API entraîne en moyenne au moins 10 fois plus de fuites de données qu'une violation de sécurité moyenne de tout autre type », selon le Gartner®Market Guide for API Protection de mai 2024.
- Les attaques se multiplient également. Le rapport État des lieux d'Internet indique également que les attaques ciblant les applications Web et les API ont augmenté de 49 % entre le premier trimestre 2023 et le premier trimestre 2024.

Ces augmentations ne sont pas surprenantes. En coulisses, les API facilitent la communication et l'échange de données entre la quasi-totalité des technologies à l'origine de vos initiatives digitales : outils d'IA générative, applications orientées client, services cloud, et bien plus encore. Pourtant, de nombreuses API ne sont pas suffisamment protégées, qu'elles soient construites sans authentification, mal configurées ou totalement oubliées, ce qui en fait un vecteur d'attaque attrayant et rentable pour les cybercriminels. Il leur suffit de trouver une API vulnérable et, *hop*, ils accèdent directement à toutes les données qu'elle renvoie lorsqu'elle est appelée, ce qui peut représenter des milliers d'enregistrements.

De nombreuses API ne sont pas suffisamment protégées, ce qui en fait un vecteur d'attaque attrayant et rentable pour les cybercriminels.

À un niveau élevé, notre étude a montré que la sécurité des API n'est pas encore devenue un élément clé d'une stratégie de sécurité globale. Les entreprises traitent le plus souvent les menaces liées aux API comme émergentes, alors que les données relatives aux attaques montrent qu'elles sont de plus en plus nombreuses et efficaces, et que leur impact sur les finances et le stress induit aux équipes augmentent, comme le révèle notre étude. Nos conclusions pour 2024 offrent une perspective sur la façon dont les incidents de sécurité des API affectent vos pairs et leurs entreprises. Nous espérons que ces données aideront votre propre équipe à mieux évaluer la protection des API et à l'améliorer si nécessaire.

Résultats de haut niveau : les incidents liés aux API ont un impact sur l'entreprise et mettent les équipes sous pression

Les résultats de notre étude 2024 ont montré que les API sont un vecteur d'attaque qui se développe et crée des défis de sécurité considérables pour les équipes. Nos participants ont fait preuve d'un consensus remarquable sur les points suivants :

- Constater l'augmentation des incidents liés aux API pendant trois années consécutives
- Dépenser plus d'un demi-million de dollars en moyenne pour traiter les incidents liés aux API et s'en remettre (l'impact financier moyen s'élève à 943 162 $, selon nos participants américains)
- Les conséquences humaines des incidents liés aux API, l'impact causé par le stress et l'atteinte à la réputation sur les équipes (en particulier la surveillance interne accrue qui amplifie cette pression) ont été jugés plus préjudiciables encore que les coûts de résolution des incidents

Les participants ont exprimé des avis partagés sur l'exhaustivité de leurs inventaires d'API, et cette variabilité est encore plus prononcée lorsqu'elle est ventilée par rôle (voir page 11). Il est frappant de constater que les entreprises disposant d'inventaires d'API complets et qui savent également lesquelles de leurs API renvoient des données sensibles sont passées de 40 % en 2023 à seulement 27 % en 2024.

Les participants ont également indiqué que les outils traditionnels sur lesquels ils s'appuient pour protéger les API ne couvrent pas entièrement les risques. Ces outils, tels que les pare-feux d'application Web (WAF), les passerelles d'API et les pare-feux de réseau, sont souvent les premiers à blâmer en cas d'attaque réussie (voir la liste complète des causes à la page 17 et une note sur les WAF et WAAP à la page 12).

Les professionnels de la sécurité ressentent les conséquences humaines des incidents liés aux API, les impacts du stress et de l'atteinte à la réputation de leurs équipes étant encore plus importants que les coûts de réparation des incidents.

Les résultats de notre étude nous permettent également de déduire quelques raisons principales pour lesquelles les stratégies de sécurité des API ne sont pas encore prioritaires, malgré les preuves démontrant qu'elles méritent d'être mises en avant. L'un des principaux facteurs est le manque d'harmonisation entre les rôles clés en matière de sécurité sur le nombre, l'emplacement et les attributs de risque des API qui doivent être protégées, probablement en raison d'une faible visibilité des API et de l'absence d'une source fiable unique.

Nous avons également observé un manque de consensus entre les responsables de la sécurité et les praticiens sur les causes des attaques visant les API. S'agit-il des outils qu'ils utilisent, des erreurs commises par leurs codeurs lors du développement, ou des attaques sur les failles dans les innovations de l'IA générative ? Cela dépend de la personne à qui vous posez la question.

Bien sûr, l'autre raison pour laquelle la sécurité des API n'a pas pris plus d'importance sur le plan stratégique est que les équipes sont déjà surmobilisées par d'autres menaces pressantes, qui concentrent également probablement la plus grande partie du budget, de l'attention et des efforts. Étudions plus en détail les résultats.

Étude de l'impact sur la sécurité des API - 2024
Aperçu des principales conclusions

84 % des participants ont subi un incident de sécurité des API au cours des 12 derniers mois

Coût moyen de résolution des incidents liés aux API au cours des 12 derniers mois :

États-Unis	Royaume-Uni	Allemagne
591 404 $	420 103 £	403 453 €

Faible visibilité

Seuls 27 % des entreprises disposant d'un inventaire d'API complet savent quelles API renvoient des données sensibles, contre 40 % en 2023.

Stress élevé

Impact n° 1 des incidents liés aux API RSSI : nuit à la réputation de notre service auprès des dirigeants/du conseil d'administration. *CIO* : augmente le stress et la pression pour l'équipe ou le service.

Peu de tests

Seulement 13 % et 18 % des participants testent leurs API en temps réel et quotidiennement, respectivement, depuis le développement de l'API jusqu'à la production.

Le coût financier des incidents de sécurité des API exacerbe l'impact sur les équipes et les dirigeants. Les violations coûteuses attirent l'attention et peuvent donner l'impression que les équipes ne font pas bien leur travail à des parties prenantes influentes, comme le conseil d'administration. C'est stressant. En fait, les participants, toutes zones géographiques confondues, ont cité le stress de leurs équipes comme le principal impact d'un incident lié à la sécurité des API.

État actuel de la sécurité des API

Au cours des trois dernières années, le nombre d'entreprises signalant des incidents de sécurité des API a constamment augmenté, atteignant un maximum de 84 % en 2024 (voir ci-dessous). Comment ces attaques contre les API affectent-elles les entreprises ? Que font-elles, ou ne font-elles pas encore, pour réduire les risques ? Nous avons structuré nos conclusions sous forme de réponses à ces questions.

Les attaques d'API ont-elles un impact significatif sur les entreprises et leurs équipes de sécurité ?

Pour faire court : oui. C'est la première année que nous avons recueilli des données sur l'impact financier d'un incident de sécurité des API, et il s'est avéré significatif : le coût, en moyenne, pour remédier aux incidents liés aux API (y compris les réparations du système, le temps d'arrêt, les frais juridiques, les amendes et toutes les autres dépenses associées) pour les 84 % qui en ont fait l'expérience au cours des 12 derniers mois s'est élevé à :

- **591 404 $** aux États-Unis
- **420 103 £** au Royaume-Uni
- **403 453 €** en Allemagne

Certains rôles ont observé des coûts beaucoup plus élevés, en particulier les cadres supérieurs américains, qui ont déclaré 943 162 dollars, soit près de 60 % de plus que la moyenne de l'ensemble des participants aux États-Unis.

Avez-vous connu un incident de sécurité des API au cours des 12 derniers mois ?

Année	Total	États-Unis	Royaume-Uni	Allemagne
2022	76 %	75 %	77 %	–
2023	78 %	85 %	69 %	–
2024	84 %	83 %	83 %	84 %

Quel que soit le chiffre exact, le coût financier des incidents de sécurité des API exacerbe les impacts humains. Les violations coûteuses attirent l'attention et peuvent donner l'impression que les équipes ne font pas bien leur travail à des parties prenantes influentes, comme le conseil d'administration. C'est stressant. En fait, les participants de toutes les zones géographiques ont cité le « stress » (en particulier le stress de leurs équipes) comme le principal impact d'un incident de sécurité des API, suivi par « l'atteinte à la réputation du service auprès des dirigeants et/ou du conseil d'administration », les « coûts de réparation » arrivant en troisième position. En particulier, les impacts internes qui affectent le plus le moral des collaborateurs réapparaissent et dominent les trois derniers impacts, qui sont presque à égalité (voir ci-dessous).

Les résultats sont similaires lorsqu'ils sont ventilés par secteur d'activité : « L'augmentation du stress et/ou de la pression que subit l'équipe après une violation d'API » est également l'impact numéro un dans quatre des huit secteurs d'activité que nous avons étudiés (voir l'encadré à la page 9). Cela inclut les services financiers, qui ont notamment signalé l'impact financier le plus élevé de tous les secteurs d'activité, à savoir 832 801 $.

Principaux impacts cités des incidents de sécurité des API

1. Augmentation du stress et de la pression pour l'équipe ou le service – **27 %**
2. Atteinte à la réputation du service auprès des dirigeants et/ou du conseil d'administration – **26,6 %**
3. Coûts engagés pour résoudre le problème – **25,8 %**
4. Amendes des régulateurs – **25,4 %**
5. Perte de la bonne volonté de la clientèle et comptes perdus – **25 %**
6. Perte de productivité – **24,1 %**
7. Perte de confiance et atteinte à la réputation – **23,8 %**
8. Perte de la bonne volonté des collaborateurs – **23,8 %**
9. Surveillance accrue de notre équipe/service par l'entreprise – **23,5 %**

D'après la question : quels coûts et/ou impacts, le cas échéant, les incidents de sécurité des API ont-ils eu sur votre entreprise ? (sélectionnez jusqu'à 3 réponses) ; n=1207

Les réponses des responsables informatiques et des responsables de la sécurité sur les impacts des incidents ont mis en exergue la relation entre les coûts financiers et humains des attaques d'API (chaque participant pouvait choisir jusqu'à trois impacts). L'un des points sur lesquels toutes les professions et toutes les régions s'accordent est le fait que les principaux impacts des incidents de sécurité des API sont sur le personnel.

- Les deux impacts les plus importants signalés par les RSSI, « l'atteinte à la réputation du service auprès des dirigeants et/ou du conseil d'administration » et « la perte de la bonne volonté de la clientèle et les comptes perdus », ont révélé une égalité exacte entre les impacts humains et financiers à 31 %.
- De même, les principaux impacts signalés par les DSI indiquent une égalité entre « l'augmentation du stress et/ou de la pression pour mon équipe/service » et « les coûts de réparation », à 34 %.

Ces résultats sont logiques pour les RSSI et les DSI : que se passe-t-il si les équipes qu'ils dirigent sont constamment en proie à des incidents de sécurité qui créent de mauvaises conditions de travail, font exploser les budgets et frustrent les clients ? Ces dirigeants ne veulent pas voir partir des talents de qualité ni voir la réputation de leur service s'effondrer. Ajoutez à cela des pressions financières telles que les coûts de résolution et/ou l'attrition des clients, et le stress des RSSI et des DSI s'accroît considérablement. Dans les faits, les participants des secteurs de l'assurance et de l'automobile ont classé la « perte de la bonne volonté de la clientèle et les comptes perdus » comme le principal impact d'un incident de sécurité des API (voir l'encadré à la page suivante pour plus de résultats par secteur d'activité).

Les réponses les plus fréquentes pour les autres postes sont les suivantes :

- CTO, 30 %, « perte de la bonne volonté des collaborateurs »
- Professionnel de la sécurité senior, 27 %, « atteinte à la réputation de notre service auprès de nos dirigeants/du conseil d'administration »
- Équipe de sécurité des applications, 31 %, « augmentation du stress ou de la pression subis par mon équipe/service »

Principaux impacts cités des incidents de sécurité des API par secteur d'activité	
Automobile	Perte de la bonne volonté de la clientèle et comptes perdus – **33 %**
Énergie/services publics	Atteinte à la réputation du service auprès des dirigeants et/ou du conseil d'administration – **36 %**
Services financiers	Égalité : Augmentation du stress/de la pression pour mon équipe/service + amendes réglementaires – les deux **29 %**
Gouvernement/ secteur public	Augmentation du stress/de la pression pour mon équipe/service – **29 %**
Santé	Égalité : Perte de confiance et de réputation + perte de productivité – les deux **29 %**
Assurance	Perte de la bonne volonté de la clientèle et comptes perdus – **28 %**
Fabrication	Augmentation du stress/de la pression pour mon équipe/service – **34 %**
Vente/e-commerce	Augmentation du stress et/ou de la pression pour mon équipe/service – **29 %**

D'après la question : quels coûts et/ou impacts, le cas échéant, les incidents de sécurité des API ont-ils eu sur votre entreprise ? (sélectionnez jusqu'à 3 réponses) ; n=1 207

Y a-t-il une visibilité suffisante sur les API et les risques potentiels ?

Non. Plus précisément, la situation a empiré. Cette année, le pourcentage de participants disposant d'un inventaire d'API complet et sachant quelles API échangent des données sensibles est passé de 40 % en 2023 à 27 % en 2024. (Ce constat pourrait avoir un côté positif, si l'on considère que davantage d'entreprises tentent d'entreprendre un inventaire complet. Toutefois, elles ne disposent pas des outils nécessaires pour localiser chaque API et identifier l'activité de chacune d'entre elles.)

Le pourcentage de participants disposant d'un inventaire d'API complet et sachant quelles API échangent des données sensibles **est passé de 40 % en 2023** à **27 % en 2024**.

État actuel des inventaires d'API et de la sensibilisation, tous les participants

	2024	2023
Oui, **et nous savons** lesquelles renvoient des données sensibles	27 %	40 %
Oui, **mais nous ne savons pas** lesquelles renvoient des données sensibles	43 %	32 %
Nous avons un inventaire d'API partiel **et nous savons** lesquelles renvoient des données sensibles	23 %	24 %
Nous avons un inventaire partiel, **mais nous ne savons pas** lesquelles renvoient des données sensibles	6 %	4 %
Non, **nous n'avons pas** d'inventaire	1 %	—

D'après la question : disposez-vous d'un inventaire d'API complet et savez-vous lesquelles renvoient des données sensibles ? (choisissez parmi cinq options) ; n=1 207

Si l'on considère les dirigeants des trois pays et des huit secteurs d'activité étudiés, les DSI ont tendance à penser, avec une marge significative par rapport aux RSSI, que leurs entreprises disposent d'un inventaire d'API complet. Au niveau des praticiens, les professionnels de la sécurité et les membres des équipes de sécurité des applications sont largement d'accord avec le point de vue du DSI moyen selon lequel toutes les API sont prises en compte.

Mais comment les cinq postes se comparent-ils en moyenne lorsqu'il s'agit de savoir (ou d'ignorer) lesquelles de leurs API renvoient des données sensibles lorsqu'elles sont appelées ? La réponse est importante, car nombre de ces appels proviennent de sources malveillantes qui cherchent à exploiter les vulnérabilités courantes des API.

Quatre types d'API non gérées que les hackers ciblent pour accéder aux données

1. Les **API fantômes** (alias API non documentées) existent et fonctionnent en dehors des canaux officiels surveillés au sein d'une entreprise.
2. Les **API indésirables** sont des API non autorisées ou malveillantes qui présentent un risque de sécurité pour un système ou un réseau.
3. Les **API zombies** englobent toute API qui continue de s'exécuter, même après avoir été remplacée en intégralité par de nouvelles versions ou d'autres API.
4. Les **API obsolètes** ne devraient plus être utilisées en raison de modifications qui leur ont été apportées.

Ces résultats offrent quelques pistes intéressantes sur la visibilité des risques liés aux API. La majorité des RSSI et des CTO ont répondu qu'ils disposaient soit d'un inventaire complet *sans* savoir quelles API renvoient des données sensibles (appelons cette notion « connaissance des données sensibles »), soit d'un inventaire partiel *avec* une connaissance des données sensibles.

La majorité des DSI ont déclaré disposer d'un inventaire d'API complet, et parmi eux, 42,9 % ont déclaré avoir également une connaissance complète des données sensibles, tandis que 36,3 % ont déclaré ne pas avoir cette connaissance. Les professionnels seniors de la sécurité sont en phase avec les DSI (75 % déclarent disposer d'un inventaire complet), mais la situation est *inversée* en ce qui concerne la connaissance des données sensibles : 32,5 % des professionnels seniors de la sécurité ont déclaré avoir des connaissances sur les données sensibles et 42,5 % ont déclaré ne pas en avoir.

Enfin, les membres des équipes de sécurité des applications, qui ont probablement l'expérience la plus pratique en la matière parmi tous les participants, ont été les plus unanimes. Près de la moitié d'entre eux ont déclaré disposer d'un inventaire complet sans connaissance des données sensibles ; l'autre moitié a répondu l'une des deux options suivantes :

- Inventaire complet avec connaissance complète des données sensibles
- Inventaire partiel avec connaissance complète des données sensibles de ces API

Nous pouvons constater que les inventaires de mesure n'ont pas encore été suffisamment normalisés pour produire un décompte des API à partir d'une source unique. Compte tenu de la variabilité, il est également probable que davantage d'entreprises disposant d'un inventaire complet *n'aient pas* une connaissance complète des données sensibles. Il est toujours important de savoir quelles API renvoient des données sensibles. Cependant, un inventaire partiel peut être le plus dangereux, car les API fantômes, indésirables, zombies et obsolètes sont très ciblées, mal protégées et échappent généralement aux outils de sécurité traditionnels.

État actuel des inventaires d'API et de la sensibilisation, ventilé par poste

	RSSI	CIO	CTO	Professionnels de la sécurité senior	Sécurité des applications
Nous avons un inventaire complet, **et nous savons** lesquelles renvoient des données sensibles	17,2 %	42,9 %	16,5 %	32,5 %	26,4 %
Nous avons un inventaire complet, **mais nous ne savons pas** lesquelles renvoient des données sensibles	41,4 %	36,3 %	34,8 %	42,5 %	47,4 %
Nous avons un inventaire d'API partiel **et nous savons** lesquelles renvoient des données sensibles	32,5 %	15,4 %	39,9 %	18,3 %	20,4 %
Nous avons un inventaire partiel, **mais nous ne savons pas** lesquelles renvoient des données sensibles	8,3 %	5,5 %	8,2 %	5,8 %	5,2 %

D'après la question : disposez-vous d'un inventaire d'API complet et savez-vous lesquelles renvoient des données sensibles ? (choisissez parmi cinq options) ; n=1 207

Alors que les API non gérées se sont multipliées et se sont révélées imperceptibles pour les outils de sécurité traditionnels, ces résultats révèlent une faille de sécurité commune qui rend le vecteur d'attaque des API plus attrayant pour les acteurs malveillants.

Bien entendu, les API non gérées ne sont qu'un des cinq attributs d'API qu'une équipe de sécurité doit voir et évaluer. Ces attributs sont les suivants :

- Les **API présentant des vulnérabilités connues** qui n'ont pas été corrigées
- Les **API non gérées ou oubliées** (fantôme, indésirable, zombie, obsolète)
- Les **API exposées à des risques externes** (tels que les informations d'identification, les clés et les variables échappant à votre contrôle)
- Les **API présentant des erreurs** d'opérateur (mauvaises configurations de sécurité dans l'infrastructure et les services)
- Les **API présentant des vulnérabilités non détectées** et des bugs que les acteurs malveillants identifient et exploitent

Au minimum, les différentes réponses concernant les inventaires d'API et la visibilité sur les vulnérabilités des API suggèrent que :

- Les entreprises s'appuient encore sur des produits de sécurité qui ne sont pas conçus spécifiquement pour identifier et sécuriser les API, en particulier les API à haut risque et non gérées.
- Les services de sécurité doivent encore définir les attributs de risque d'une API qui doivent être vus et évalués, ou établir un consensus entre leurs nombreuses unités commerciales, équipes de développeurs et fournisseurs sur leur stratégie de découverte et d'inventaire des API.

La résolution de ces divergences peut constituer une première étape importante dans l'élaboration d'un argumentaire efficace en faveur de l'investissement dans des capacités renforcées de sécurisation de toutes les API (voir « Comment évoluer vers une posture plus mature en matière de sécurité des API » à la page 18). En l'état actuel des choses, l'attention et le plaidoyer nécessaires pour recevoir une allocation budgétaire ne sont souvent pas en place pour la sécurité des API, ce qui rend difficile la priorisation et le financement d'initiatives qui pourraient faire progresser non seulement les défenses des API et des applications Web, mais aussi la posture de sécurité globale d'une entreprise.

Plus performants ensemble : protections spécifiques WAAP + API

Conçue pour identifier et atténuer rapidement les menaces provenant de multiples vecteurs d'attaque, la protection des applications Web et des API (WAAP) étend les protections traditionnelles d'un WAF. **Une solution de sécurité des API (avec fonctionnement en tandem) étend les protections au-delà du pare-feu pour créer la défense la plus robuste possible**.

Les API sont-elles testées suffisamment souvent pour réduire le risque d'abus ou de violation ?

Non, pas assez souvent. Les API publiques mal configurées, dépourvues de contrôles d'authentification, contenant des erreurs de codage ou présentant d'autres risques évitables sont exactement ce que les hackers recherchent, et ces derniers sont de plus en plus doués pour les trouver.

Ainsi, chaque fois que votre équipe de développement envoie des API de ce type en production, sans les avoir préalablement testées de manière exhaustive, c'est comme si elle planifiait involontairement une future charge de travail pour votre équipe de sécurité (une charge de travail qui sera sans aucun doute urgente et allant dans le sens de ce que nos résultats révèlent sur le stress).

Mais notez que nous avons parlé de risques *évitables*.

Si vous testez les API en phase de développement, fréquemment et efficacement par le biais de l'automatisation, *avant* qu'elles ne soient mises en production, vous donnez un avantage à votre entreprise, à vos développeurs et à votre équipe de sécurité. Et cet avantage est immédiat en matière de réduction du stress causé par des vulnérabilités inconnues et de la certitude que les erreurs ne seront pas rencontrées en production alors qu'elles sont exponentiellement plus difficiles et plus coûteuses à corriger.

Si vous testez les API en phase de développement, fréquemment et efficacement par le biais de l'automatisation, *avant* qu'elles ne soient mises en production, vous donnez un avantage à votre entreprise, à vos développeurs et à votre équipe de sécurité.

Jusqu'à présent, cependant, les tests restent insuffisants, d'après les participants. Les tests fréquents d'API, en temps réel et au quotidien, ont diminué par rapport à l'année dernière, tout au long du cycle de vie de l'API, y compris en production.

- En 2023, 18 % des participants américains et britanniques ont déclaré effectuer des tests en temps réel. Dans le même groupe de personnes **en 2024, ce chiffre est tombé à 13 %**.
- En 2023, 37 % des participants américains et britanniques ont déclaré effectuer des tests au moins une fois par jour. **En 2024, ils n'étaient plus que 13 % à faire des tests à cette fréquence**, bien que 26 % des participants allemands aient fait des tests une fois par jour.

Les tests d'API hebdomadaires sont les plus courants pour les participants dans toutes les zones géographiques, mais ils n'atteignent 50 % dans aucune. En outre, la fréquence des tests d'API varie considérablement d'une zone géographique à l'autre, allant des tests en *temps réel* à l'*absence* de tests. Il convient de noter que seulement 6 % des participants ont répondu « nous ne testons la sécurité des API qu'avant de les mettre en production ». Dans l'idéal, les équipes devraient procéder à des tests continus tout au long du cycle de vie de l'API.

Que signifie tester continuellement les API ?

Des vulnérabilités peuvent être introduites dans les API à tout moment de leur cycle de vie, qu'il s'agisse d'erreurs de codage commises lors du développement ou de lacunes de sécurité qui apparaissent une fois que les utilisateurs commencent à interagir avec l'API. C'est pourquoi, dans l'idéal, les tests d'API sont effectués en phase de développement (shift-left) et en continu pendant la phase de production (shift-right).

Exemples de tests d'API en phase de développement :

- Exécuter des tests automatisés qui simulent le trafic malveillant.
- Inspecter les spécifications des API par rapport aux politiques de gouvernance établies.
- Tester les API à la demande ou dans le cadre d'un pipeline CI/CD.

Exemples de tests d'API en phase de production :

- Surveiller en permanence le trafic des API et évaluer les métadonnées du trafic.
- Identifier les modifications apportées à vos API existantes par le biais d'une analyse automatisée.
- Trouver les problèmes en temps réel et y remédier avant que les hackers ne s'en aperçoivent.

Vos protocoles de sécurité des API répondent-ils aux exigences de conformité ?

Dans de nombreuses réglementations en matière de protection des données, les API ne sont pas mentionnées nommément, mais les exigences sont clairement axées sur la sécurisation des applications et de l'infrastructure au sein desquelles les API fonctionnent. Les mandats de conformité sont en constante évolution et de nouvelles réglementations sont en cours d'élaboration avec des répercussions sur les API, notamment la loi américaine sur les droits à la vie privée (actuellement en projet de loi) et le règlement européen sur la cyberrésilience.

Les réglementations et les cadres ayant des implications directes et actuelles pour la sécurité des API sont les suivants :

- PCI DSS (actuellement v4.0.1)
- Règlement général sur la protection des données (RGPD)
- Loi sur la résilience opérationnelle numérique (DORA)
- Loi HIPAA (Health Insurance and Portability and Accountability Act)
- Directive sur la sécurité des réseaux et des systèmes d'information (NIS2)

La sécurité des API reçoit une certaine attention, mais reste secondaire

Si les attaques contre les API sont coûteuses et entraînent des amendes, si elles contribuent à la perte de confiance des clients, si elles provoquent une augmentation du stress chez le personnel et une perte de crédibilité auprès des conseils d'administration des entreprises, pourquoi les équipes ne prennent-elles pas des mesures plus décisives ? Les réponses aux questions suivantes nous aident à comprendre la situation.

Quelle priorité les différents postes de l'entreprise accordent-ils à la sécurité des API ?

Nous avons demandé à nos participants d'identifier leurs principales priorités en matière de cybersécurité pour les 12 prochains mois, en leur permettant d'en sélectionner jusqu'à trois parmi une liste exhaustive (voir encadré). Les six premières priorités ne différaient que de 2 % et les six dernières de 1 %, ce qui suggère que les priorités sont similaires d'un pays à l'autre et d'un secteur d'activité à l'autre, et que les équipes sont souvent obligées de jongler avec toutes ces priorités.

Dans certains secteurs d'activité, cependant, les différences de classement au cœur des API racontent une tout autre histoire. Par exemple, le secteur de l'énergie et des services publics classe la sécurité des API comme la priorité la plus faible par rapport à tous les autres secteurs, à 13,2 % (et en dessous de la moyenne de 18 % de tous les participants à l'enquête). Dans le même temps, le secteur de l'énergie et des services publics est celui qui signale le plus d'incidents liés à la sécurité des API, avec 91 %, soit le taux le plus élevé des huit secteurs d'activité et un taux supérieur à la moyenne de 84 %. Qu'est-ce qui explique cette situation ? Le faible degré de priorité accordé à la sécurité des API et le taux d'attaque élevé.

Principales priorités citées en matière de sécurité pour les 12 prochains mois

1. Défense contre les attaques alimentées par l'IA générative – **21,2 %**
2. Défense contre les ransomwares – **20,5 %**
3. Sécurisation de l'authentification pour les utilisateurs faisant partie du personnel – **19,7 %**
4. Gestion et sécurisation des secrets des développeurs – **19,6 %**
5. Sécurisation des points de terminaison – **19,2 %**
6. Solutions de sécurité dans le cloud – **19,1 %**
7. Sécurisation des accès informatiques privilégiés – **18,6 %**
8. Prévention des pertes de données – **18,6 %**
9. Sécurisation des API contre les acteurs malveillants – **17,9 %**
10. Sécurisation des applications – **17,7 %**
11. Gestion des informations et des événements de sécurité – **17,6 %**
12. Réponse et gestion des incidents – **17,6 %**

D'après la question : quelles sont les principales priorités de votre entreprise en matière de cybersécurité pour les 12 prochains mois ? (veuillez en sélectionner 3 au maximum) ; n=1 207

La répartition des réponses par poste de travail a permis de dégager des données plus évocatrices :

- Les RSSI ont cité les attaques assistées par l'IA générative et la protection des API en tête de liste, avec respectivement **25,5 %** et **24,8 %**.
- Le personnel de la sécurité des applications a rejoint les RSSI en citant les attaques assistées par l'IA générative comme leur plus grande priorité, à **22,5 %**.
- Les DSI et les CTO se sont tous concentrés sur l'accès privilégié, les CTO ajoutant la réponse aux incidents à égalité.
- Les professionnels seniors de la sécurité sont les seuls à avoir placé les ransomwares en tête de leurs priorités.

Ces différences nous amènent à nouveau à nous poser des questions telles que les suivantes : pourquoi les différentes couches de l'organisation de la sécurité informatique semblent-elles fonctionner avec différents plans d'action ? Et pourquoi les hauts responsables de la sécurité et les collaborateurs de première ligne semblent-ils s'accorder sur le rôle important que jouent les API, et leurs risques, dans les attaques assistées par l'IA générative, alors que d'autres postes ne le sont pas ?

Peut-être parce qu'eux seuls connaissent l'étendue des inconnues concernant les vulnérabilités des composants de l'IA (comme les LLM) qui touchent des données sensibles, tandis que les unités commerciales des RSSI mettent en œuvre à la hâte des innovations telles que des applications alimentées par l'IA générative pour répondre à la demande, de même que les membres de l'équipe de sécurité des applications. En outre, cette équipe est aux premières loges pour observer les nombreux signes avant-coureurs indiquant que les hackers intègrent l'IA générative à leurs méthodes d'attaque.

Mais la raison principale est peut-être la plus simple : les communications descendantes et ascendantes ne sont pas assez fréquentes, en particulier dans les grandes entreprises, ce qui entraîne un décalage entre les priorités au sommet et ce que les équipes *doivent* gérer au jour le jour.

Enfin, comparons les principales priorités des participants en matière de cybersécurité avec les causes qu'ils ont données pour expliquer les incidents liés à la sécurité des API. Comme le montre la page 17, trois des causes les plus citées concernent les outils traditionnels de sécurité des applications qui n'ont pas été en mesure de détecter les problèmes liés aux API. Cette comparaison est l'occasion d'ouvrir une discussion sur la manière dont les solutions de découverte et de test des API pourraient améliorer non seulement la sécurité des API, mais aussi la quasi-totalité de leurs autres priorités en matière de sécurité.

En d'autres termes, si les bons outils de sécurité des API peuvent non seulement protéger les API, mais aussi améliorer la sécurité dans des domaines tels que les données, le cloud et les applications, la sécurité des API n'apparaîtra plus comme un domaine de niche cloisonné aux yeux de vos parties prenantes. Le fait de parler de la situation dans son ensemble peut faciliter l'obtention d'un accord pour hisser les API en haut de la liste des priorités.

Si les bons outils de sécurité des API peuvent non seulement protéger les API, mais aussi améliorer la sécurité dans des domaines tels que les données, le cloud et les applications, la sécurité des API n'apparaîtra plus comme un domaine de niche cloisonné aux yeux de vos parties prenantes.

L'absence d'alignement sur les incidents de sécurité des API indique-t-elle qu'il n'existe pas une source fiable unique ?

Nous avons mis en évidence les différences entre les dirigeants et le personnel de première ligne en ce qui concerne leurs priorités globales en matière de sécurité, et ces différences subsistent dans les questions plus spécifiques aux menaces liées aux API. Par exemple, les DSI sont en phase avec l'équipe de sécurité des applications en termes de sensibilisation aux attaques d'API (environ 88 % dans chaque poste déclarent avoir subi des incidents). En revanche, environ 80 % des RSSI, des CTO et des professionnels senior de la sécurité déclaraient avoir subi des incidents, une différence de 8 points de pourcentage.

La cause principale des incidents liés à la sécurité des API varie également en fonction du poste, la plupart des RSSI et des professionnels seniors de la sécurité citant le fait que la passerelle API n'a pas détecté l'incident, tandis que les trois autres postes désignent chacun un coupable différent :

- RSSI : la passerelle d'API ne l'a pas détecté – **26,8 %**
- CIO : exposition involontaire à Internet – **28,6 %**
- CTO : le WAF ne l'a pas détecté – **25,9 %**
- Professionnel senior de la sécurité : la passerelle d'API ne l'a pas détecté – **23,3 %**
- Équipe de sécurité des applications : erreur de configuration de l'API – **23,2 %**

Principales causes citées des incidents de sécurité des API, tous les participants

1. L'API a été exposée involontairement à Internet – 21,8 %
2. Le pare-feu d'application Web ne l'a pas détecté – 21,8 %
3. La passerelle d'API ne l'a pas détecté – 20,2 %
4. API dans les outils/technologies de l'IA générative, par exemple les LLM – 20 %
5. Erreur de configuration de l'API – 19,9 %
6. Le pare-feu réseau ne l'a pas détecté – 19,6 %
7. Outil/service technologique bien connu, par exemple Microsoft – 19,2 %
8. Vulnérabilité due à des erreurs de codage de l'API – 19,1 %
9. API non gérées, par exemple, API dormantes ou zombies – 18,9 %
10. Absence de contrôles d'authentification de l'API – 18,8 %
11. Vulnérabilités en matière d'autorisation – 18,7 %
12. Solution logicielle téléchargée depuis Internet – 17,6 %
13. Solution logicielle de niveau intermédiaire, par exemple, Slack – 16,3 %

D'après la question : selon vous, quelles sont les causes des incidents de sécurité des API que votre entreprise a connus ? (sélectionnez jusqu'à 3 réponses) ; n=1 207

Le coût déclaré des incidents de sécurité liés aux API a également montré un manque d'alignement des hauts responsables, bien qu'il soit important de noter que la répartition des données par poste *et* par région entraîne naturellement une réduction de la taille de l'échantillon. Néanmoins, les différences entre ces sous-ensembles méritent d'être soulignées, en particulier aux États-Unis, où les DSI et les CTO ont déclaré que le coût des incidents s'élevait à environ 1 million de dollars et les RSSI à environ 737 000 dollars, tandis que les professionnels seniors de la sécurité et le personnel de la sécurité des applications ont déclaré des coûts d'environ 375 000 et 444 000 dollars, respectivement.

Au Royaume-Uni, les coûts étaient généralement plus alignés sur les sous-ensembles de postes spécifiques, bien que les membres de l'équipe de la sécurité des applications aient déclaré le montant le plus élevé, à savoir 749 000 £, et les RSSI le montant le plus bas, à savoir 190 000 £. (Les postes intermédiaires s'échelonnent de 374 000 à 222 000 £). En Allemagne, la disparité des coûts déclarés est similaire à celle du Royaume-Uni, l'estimation la plus élevée provenant du personnel le moins qualifié et le plus opérationnel, soit 345 000 euros, et le coût le plus bas étant celui des RSSI les plus qualifiés, soit 197 000 £ (résultats opposés à ceux des États-Unis). L'un des points qui a fait l'objet d'un consensus général entre tous les postes dans toutes les régions est que les incidents liés à la sécurité des API ont un impact majeur sur le personnel (voir Impacts à la page 7).

Comment évoluer vers une posture plus mature en matière de sécurité des API

Comme nous l'avons mentionné, nos résultats montrent clairement que les membres des équipes de sécurité à différentes strates de l'entreprise n'envisagent pas la sécurité des API sous le même angle. D'un autre côté, il est également clair qu'ils ont un terrain d'entente sur lequel s'appuyer. Ils connaissent les coûts (financiers et humains) et reconnaissent que les outils sur lesquels ils s'appuient ne sont pas suffisants.

La sécurité des API ayant un impact aussi important sur les entreprises, vos prochaines étapes pourraient consister à décider ce sur quoi il faut s'appuyer, ce qu'il faut changer, et à montrer aux dirigeants comment la sécurisation des API peut contribuer à la rentabilité de l'entreprise. Un bon point de départ est d'obtenir un alignement au sein de votre service de sécurité, du RSSI à l'équipe de sécurité des applications, sur la façon de donner la priorité à la sécurité des API, puis de promouvoir une communication ouverte entre la direction et les membres de l'équipe de sécurité des applications de première ligne, ainsi que les strates de gestion situées entre les deux.

Mesures que vous pouvez prendre

Pour clore notre étude, nous avons élaboré une série d'étapes à suivre pour que votre équipe de sécurité puisse lancer ou développer votre stratégie de sécurité des API et évoluer vers une protection mature des API.

1 Commencez par la découverte et la visibilité des API

Pour réaliser un inventaire complet de votre portefeuille d'API, recherchez des outils dotés d'une approche automatisée de la découverte des API et des microservices qu'elles prennent en charge. L'étendue de la couverture est essentielle, car les API non gérées (voir l'encadré à la page 10) sont une cible de choix pour les acteurs malveillants.

2 Investissez dans les tests

Choisissez une solution de sécurité des API qui vous permet de vérifier facilement si les API sont codées correctement pour remplir la fonction prévue. Idéalement, les tests sont effectués avant le déploiement, mais il est également important de tester toutes les API déjà en production avec une analyse en temps réel du trafic et des vulnérabilités potentielles.

3 Procédez à une documentation complète des API

Il est essentiel d'auditer l'ensemble de votre environnement API pour identifier celles qui sont mal configurées ou toutes autres erreurs. Vos capacités d'audit doivent également garantir une documentation adéquate de toutes les API et indiquer si elles contiennent des données sensibles ou si elles ne disposent pas des contrôles de sécurité appropriés. Cela vous aide également à vous préparer aux obligations de conformité qui impliquent la sécurité des API, de manière implicite ou explicite (voir page 14).

4 Utilisez la détection d'exécution

Une solution de sécurité des API dotée d'une détection automatisée de l'exécution vous permet de faire la différence entre une activité API « normale » et une activité API « anormale ». En surveillant ainsi les interactions des API, vous êtes en mesure de détecter les comportements indiquant une menace en temps réel et d'agir.

5 Réagissez aux comportements suspects

En intégrant une solution de sécurité des API à votre système de sécurité existant (par exemple, WAF ou WAAP), vous serez en mesure de repérer les comportements à haut risque et de bloquer le trafic suspect avant qu'il n'accède à des ressources critiques.

6 Enquêtez et recherchez les menaces

Au stade le plus avancé de la sécurité des API, vous utiliserez une analyse cybercriminelle des données des menaces antérieures pour savoir si les alertes ont correctement identifié les menaces et si des modèles permettant une recherche proactive des menaces ont émergé en combinant des outils sophistiqués et l'intelligence humaine.

Conclusion

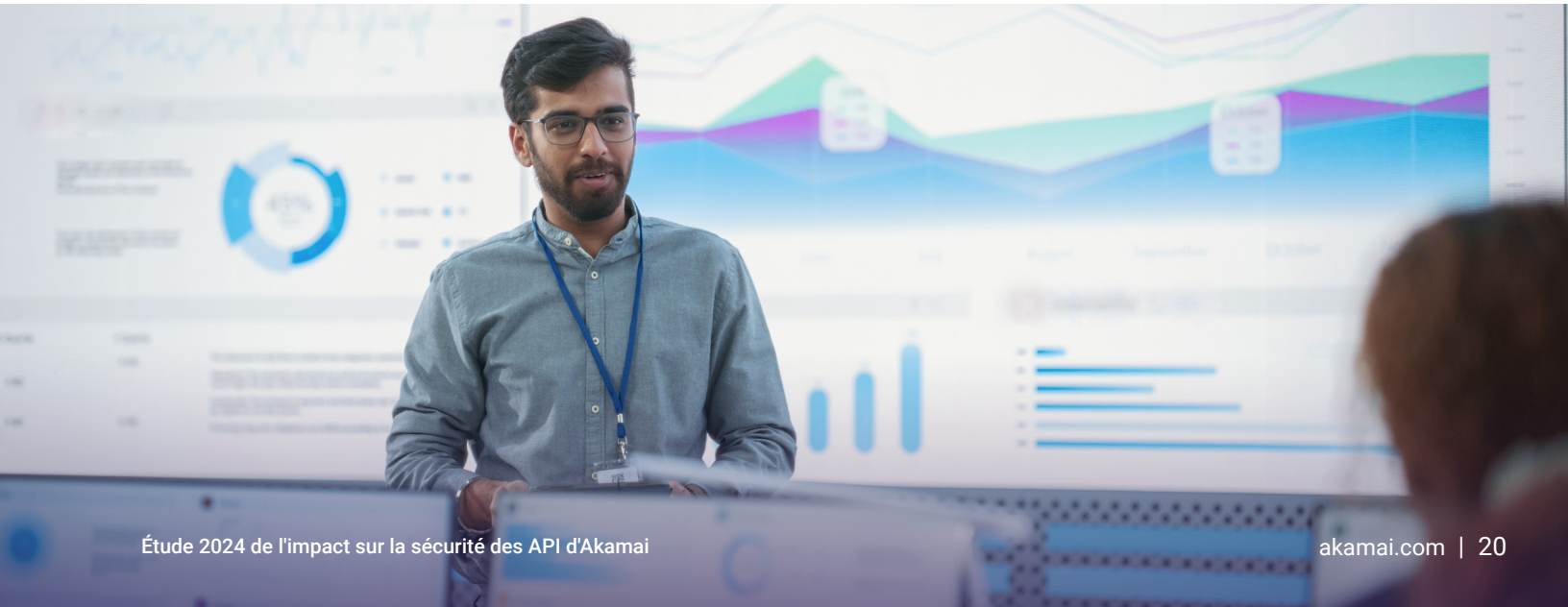
Le rapport de cette année a clairement montré que la sécurité, en l'occurrence la sécurité des API, n'est pas seulement une question de listes de menaces ou d'outils ; c'est une question de personnes.

Notre étude confirme que les équipes de sécurité sont surchargées et que l'idée d'ajouter un tout nouveau vecteur d'attaque à la charge de travail de votre équipe peut sembler décourageante. Mais la prolifération des API ne va pas s'arrêter là, et prendre des mesures pour sécuriser vos API a un fort effet d'entraînement sur plusieurs autres priorités, telles que les vulnérabilités liées à l'IA générative (pour protéger les API qui échangent des données avec les LLM) et la sécurité dans le cloud (pour réduire le risque dans chaque API incluse dans les charges de travail que vous migrez).

Nous sommes convaincus que la proactivité en matière de sécurité des API ne protège pas seulement votre entreprise, mais permet également à votre équipe de devenir beaucoup plus crédible et fiable dans sa vision de ce vecteur d'attaque critique, parmi les pairs, les dirigeants et le conseil d'administration. Cela présente l'énorme avantage de réduire le niveau de stress de votre équipe, dont notre étude a montré qu'elle est très affectée par les incidents de sécurité des API et par la surveillance et la perte de confiance qu'ils engendrent, tant chez les collaborateurs que chez les clients.

En prenant des mesures dès maintenant, vous facilitez également la planification de la conformité et l'établissement de rapports, sans parler de la prévention opportune des amendes réglementaires. Alors pourquoi ne pas commencer ?

- Si vous êtes prêt à envisager les prochaines étapes de votre démarche vers une posture de sécurité des API mature, nous vous recommandons de commencer par notre livre blanc, Principes fondamentaux de la sécurité des API.
- Si vous êtes prêt à discuter de vos défis et de la manière dont nous pouvons vous aider, il vous suffit de demander une démonstration personnalisée d'Akamai API Security.



À propos de l'étude de l'impact sur la sécurité des API

L'étude 2024 de l'impact sur la sécurité des API d'Akamai a été réalisée par Opinion Matters entre le 12 juin 2023 et le 7 juillet 2024. L'équipe a interrogé un total de 1 207 participants, répartis comme suit en fonction du siège social de l'entreprise : 404 au Royaume-Uni, 402 aux États-Unis et 401 en Allemagne. Un tiers des participants étaient des DSI ou des RSSI, un tiers des professionnels seniors de la sécurité et un tiers des membres d'équipes de sécurité des applications travaillant dans des entreprises de moins de 500 à plus de 1 000 salariés, dans huit secteurs d'activité clés : l'automobile, les services financiers, la vente au détail/l'e-commerce, la santé, l'assurance, le gouvernement/le secteur public, l'industrie manufacturière et l'énergie/les services publics.

Opinion Matters emploie des membres de la Market Research Society et respecte le code de conduite de la MRS ainsi que les principes d'ESOMAR. Opinion Matters est également membre du British Polling Council.

Crédits

Rédactrice principale
Annie Brunholzl

Managing editor
John Natale

Directeur de recherche
Mitch Mayne

Copy editor
Randi Kravitz

Promotions
Barney Beal

Marketing et publication
Georgina Morales Hampe

Révision et expertise
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

État des lieux d'Internet/Sécurité

Lisez les numéros précédents et surveillez les prochaines parutions du célèbre rapport État des lieux d'Internet/Sécurité d'Akamai, **akamai.com/soti**

Recherches sur les menaces d'Akamai

Tenez-vous au courant des dernières analyses d'informations sur les menaces, des rapports de sécurité et des recherches sur la cybersécurité sur **akamai.com/threatresearch**

Akamai API Security

Découvrez comment Akamai protège les API tout au long de leur cycle de vie, du développement à la production, grâce à des fonctionnalités essentielles de découverte des API, de gestion de la posture, de protection de l'exécution et de test de la sécurité des API. **https://www.akamai.com/products/api-security**

La solution de sécurité d'Akamai protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 11/24.