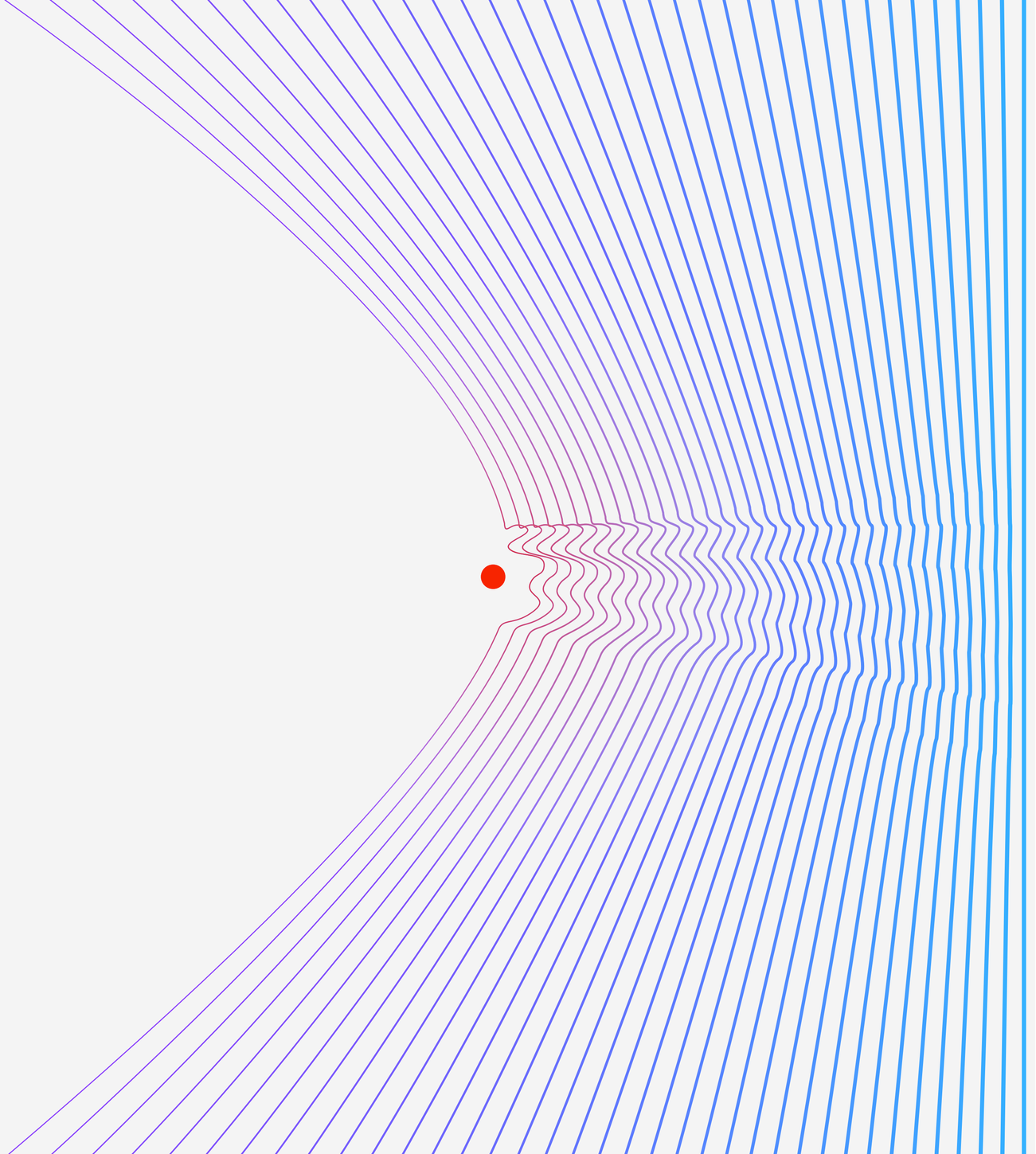
IBM **Security**

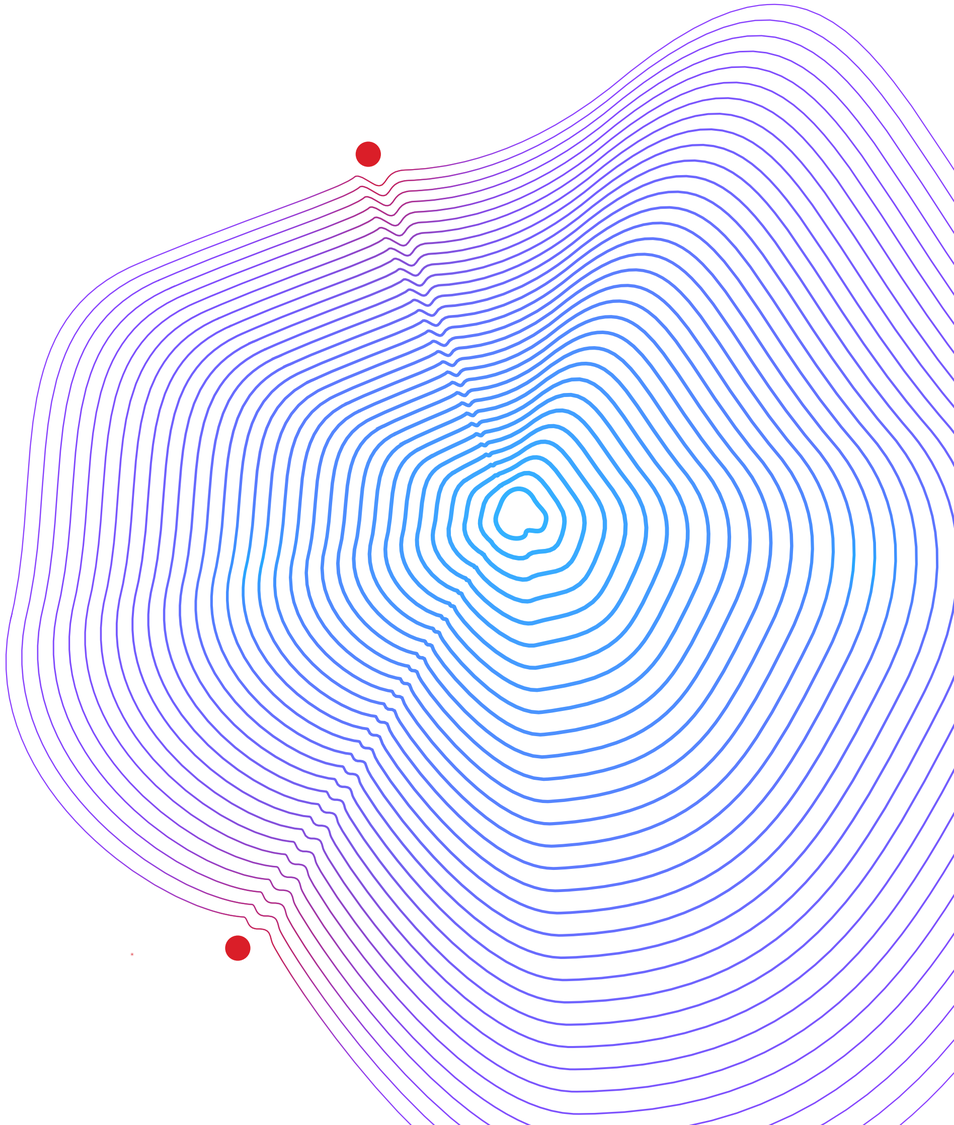
# Rapport sur le coût d'une violation de données 2023

## Synthèse



# Table des matières





01

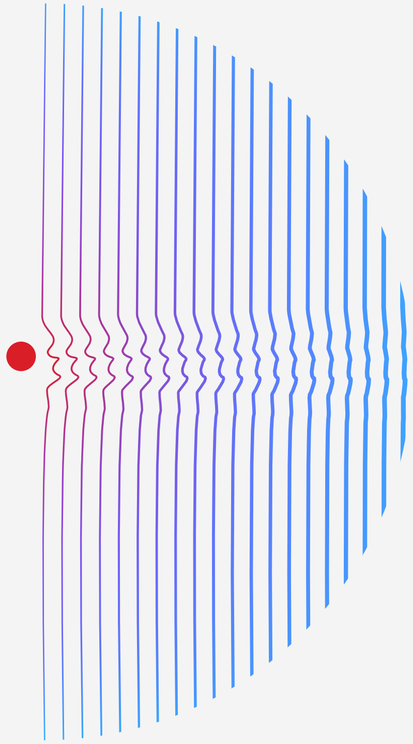
# Note de direction

Le rapport sur le coût d'une violation de données fournit aux responsables informatiques, de la gestion des risques et de la sécurité des preuves quantifiables qui les aident à mieux gérer leurs investissements en matière de sécurité, leur profil de risque et leurs processus décisionnels stratégiques. Ce rapport 2023 est présenté pour la 18e année consécutive.

Le rapport de cette année a été réalisé de manière indépendante par le Ponemon Institute et commandité, analysé et publié par IBM Security®. Il porte sur 553 organisations victimes de violations de données survenues entre mars 2022 et mars 2023.

Les années mentionnées dans ce rapport font référence à l'année de publication du rapport, pas nécessairement à l'année de la violation. Les violations étudiées ont eu lieu dans 16 pays et régions et dans 17 industries différentes.

Tout au long de ce rapport, nous examinerons les causes premières et les conséquences à court et à long terme des violations de données. Nous explorerons également les facteurs et les technologies qui ont permis aux sociétés de limiter leurs pertes, ainsi que ceux qui ont entraîné une augmentation des coûts.



# Nouveautés du rapport pour 2023

Chaque année, nous continuons à faire évoluer le rapport sur le coût d'une violation de données en prenant en compte des nouvelles technologies, des tactiques émergentes et des événements récents. Cette année, le rapport explore pour la première fois les éléments suivants :

- Comment les violations sont identifiées : que ce soit par les équipes de sécurité de l'organisation, par un tiers ou par l'agresseur informatique
- L'impact de l'implication des forces de l'ordre dans une attaque par ransomware
- L'effet des protocoles et des flux de travaux sur les ransomwares
- Coûts spécifiques associés aux amendes réglementaires
- Si et comment les sociétés prévoient d'accroître leurs investissements en matière de sécurité suite à une violation
- L'impact des stratégies d'atténuation suivantes :
  - Renseignements sur les menaces
  - Gestion des vulnérabilités et des risques
  - Gestion du périmètre de vulnérabilité
  - Prestataires de services de sécurité gérés (MSSPs)

Alors que le coût d'une violation continue d'augmenter, ce rapport fournit des analyses essentielles pour aider les équipes de sécurité et informatiques à mieux gérer les risques et à limiter les pertes potentielles. Le rapport contient les sections suivantes :

- La synthèse, avec les principales conclusions et les nouveautés de l'édition 2023
- Une analyse approfondie, incluant les coûts des violations par région géographique ou industrie
- Les recommandations de sécurité des experts d'IBM Security sur la base des résultats du rapport

02

# Principales conclusions

Les principales conclusions présentées ici sont basées sur l'analyse réalisée par IBM Security à partir des données compilées par le Ponemon Institute. Les montants dans ce rapport sont exprimés en dollars américains (USD).

## 4,45 millions USD

**Coût total moyen d'une violation**
Le coût moyen d'une violation de données a atteint 4,45 millions de dollars en 2023, un record. Cela représente une augmentation de 2,3 % par rapport au chiffre de 2022 (4,35 millions de dollars). Dans une perspective à long terme, le coût moyen a augmenté de 15,3 % par rapport aux 3,86 millions de dollars évoqués dans le rapport de 2020.

## 51 %

**Pourcentage d'organisations prévoyant d'augmenter leurs investissements en matière de sécurité à la suite d'une violation**
Alors que les coûts liés aux violations de données continuaient d'augmenter, les participants à l'étude étaient presque également répartis quant à savoir s'ils devaient augmenter leurs investissements dans la sécurité en raison d'une violation de données. Principaux domaines identifiés pour les investissements supplémentaires : la planification et les tests de réponse aux incidents (RI), la formation des employés, la détection des menaces et les technologies de riposte.

## 1,76 million USD

**L'effet d'une sécurité étendue, de l'IA et de l'automatisation sur l'impact financier d'une violation**
En matière de sécurité, il a été prouvé que l'IA et l'automatisation étaient des investissements importants pour réduire les coûts et réduire le temps nécessaire pour identifier et contenir les violations. Les organisations qui ont utilisé ces fonctionnalités de manière systématique dans le cadre de leur approche ont bénéficié, en moyenne, d'un délai de 108 jours plus court pour identifier et contenir ladite violation. Ils ont également fait état de coûts de violation de données inférieurs de 1,76 million de dollars à ceux des entreprises qui n'utilisaient ni l'IA appliquée à la sécurité ni des fonctionnalités d'automatisation.

## 1 sur 3

**Nombre de violations identifiées par les équipes ou les outils de sécurité d'une organisation**
Seul un tiers des sociétés ont découvert la violation de données grâce à leurs propres équipes de sécurité, ce qui souligne la nécessité d'améliorer la détection des menaces. 67 % des violations ont été signalées par un tiers non hostile ou par les agresseurs eux-mêmes. Lorsque les agresseurs ont révélé une violation, cela a coûté aux organisations près d'un million de dollars de plus que si la violation avait été détectée en interne.

## 470 000 USD

**Coût supplémentaire constaté par les organisations qui ne faisaient pas appel aux forces de l'ordre en cas d'attaque par ransomware**
L'étude de cette année démontre que le fait de ne pas faire appel aux forces de l'ordre en cas d'attaque par ransomware a entraîné des coûts plus élevés. Alors que 63 % des personnes interrogées déclarent avoir contacté les forces de l'ordre, les 37 % qui ne l'ont pas fait ont également payé 9,6 % de plus et ont été confrontés à un cycle de vie de la violation équivalent à 33 jours supplémentaires.

## 53,3 %

**Depuis 2020, les coûts des violations de données du système de santé ont augmenté de 53,3 %**
Depuis 2020, la santé, un secteur soumis à de nombreuses réglementations, a subi une très forte augmentation des coûts de violation de données. Pour la 13e année consécutive, le secteur de la santé a enregistré les violations de données les plus coûteuses, le coût moyen étant de 10,93 millions de dollars.

## 82 %

**Le pourcentage de violations impliquant des données stockées dans le cloud (environnements publics, privés ou multiples)**
En 2023, les environnements cloud ont également été des cibles fréquentes pour les pirates informatiques. Les agresseurs ont souvent accédé à plusieurs environnements, avec 39 % des violations couvrant plusieurs environnements et un coût supérieur à la moyenne de 4,75 millions de dollars.

## 1,68 million de dollars

**Économies de coûts liées à des niveaux élevés d'adoption DevSecOps**
Les tests de sécurité intégrés dans le processus de développement logiciel (DevSecOps) se sont traduits par un ROI élevé en 2023. Les organisations ayant largement adopté la stratégie DevSecOps ont économisé 1,68 million de dollars par rapport à celles dont le niveau d'adoption était faible ou nul. Par rapport à d'autres facteurs d'atténuation des coûts, DevSecOps a généré des économies de coûts plus conséquentes.

## 1,49 million de dollars

**Économies de coûts réalisées par les organisations ayant des niveaux élevés de planification et de tests RI**
En plus d'être un investissement prioritaire pour les organisations, la planification et les tests IR se sont révélés être une tactique très efficace pour contenir le coût d'une violation de données. Les organisations ayant un niveau élevé de planification et de tests RI ont économisé 1,49 million de dollars par rapport aux autres.

## 1,44 million de dollars

**Augmentation des coûts liés aux violations de données pour les organisations dont les systèmes de sécurité sont très complexes**
Les organisations ayant déclaré que la complexité de leur système de sécurité était faible ou inexistante ont subi un coût moyen de 3,84 millions de dollars américains en 2023 pour les violations de données. Ceux qui ont des niveaux élevés de complexité des systèmes de sécurité ont signalé un coût moyen de 5,28 millions de dollars, soit une augmentation de 31,6 %.

## 1,02 million de dollars

**Différence du coût moyen entre les violations identifiées et résolues en plus de 200 jours et celles qui ont pris moins de 200 jours**
Le délai nécessaire à l'identification et à l'endiguement des violations, connu sous le nom de cycle de vie d'une violation, continue de faire partie intégrante de l'impact financier global. Les violations dont le temps d'identification et d'endiguement est inférieur à 200 jours coûtent aux organisations 3,93 millions de dollars américains. Celles de plus de 200 jours coûtent 4,95 millions de dollars, soit une différence de 23 %.

03

# Recommandations pour aider à réduire le coût d'une violation de données

Dans cette section, IBM Security décrit les mesures que les entreprises peuvent prendre pour réduire les coûts et les conséquences d'une violation de données sur leur réputation. Nos recommandations comprennent des approches de sécurité gagnantes associées à une réduction des coûts d'identification et d'endiguement des violations.

1. Intégrer la sécurité à chaque étape du développement et du déploiement de logiciels, et procéder à des tests réguliers
2. Moderniser la protection des données dans le cloud hybride
3. S'appuyer sur l'IA et l'automatisation de la sécurité pour gagner en vitesse et en précision
4. Renforcer la résilience en maîtrisant votre périmètre de vulnérabilité et en répétant les procédures de RI

# 1

**Intégrer la sécurité à chaque étape du développement et du déploiement de logiciels, et procéder à des tests réguliers**
Les exigences réglementaires continuent de se complexifier, d'autant plus que la technologie est de plus en plus étroitement liée aux activités quotidiennes et que les logiciels sont de plus en plus riches et complexes en termes de fonctionnalités. Une approche DevSecOps, principal facteur d'atténuation des coûts selon une analyse spécifique recensant 27 facteurs et présentée dans le rapport 2023, sera essentielle pour intégrer la sécurité dans tous les outils ou plateformes dont une organisation dépend pour mobiliser son personnel ou ses clients.

Les organisations de tous types doivent veiller à ce que la sécurité soit la priorité de chaque logiciel qu'elles développent, ainsi que des logiciels commerciaux prêts à l'emploi qu'elles déploient.
Les développeurs d'applications doivent continuer de renforcer l'adoption des principes de sécurité dès la conception et de sécurité par défaut pour s'assurer que la sécurité est une exigence fondamentale prise en compte lors de la phase de conception initiale des projets de transformation numérique et pas simplement abordée après coup.
Les mêmes principes s'appliquent aux environnements cloud pour prendre en charge le développement d'applications cloud natives qui font un maximum d'efforts pour protéger la vie privée des utilisateurs et minimiser les périmètres de vulnérabilité.

Les tests d'application ou de pénétration du point de vue d'un agresseur informatique peuvent également permettre aux organisations d'identifier et de corriger les vulnérabilités avant qu'elles n'ouvrent la voie à des violations. Jamais une technologie ou une application ne sera sécurisée à 100 % et l'ajout de nouvelles fonctionnalités accroît les risques.
Des tests constants au niveau des applications permettront aux organisations d'identifier de nouvelles vulnérabilités.

# 2

**Moderniser la protection des données dans le cloud hybride**

Dans les environnements multicloud, les données sont créées, partagées et accessibles dans des proportions jamais vues. L'adoption rapide de nouvelles applications et de nouveaux services cloud aggrave le risque de « données fantôme », c'est-à-dire de données sensibles qui ne sont ni suivies ni gérées, ce qui accentue les risques de sécurité et de conformité. La majorité (82 %) des violations de données présentées dans ce rapport concernent des données stockées dans des environnements cloud, et 39 % des violations incluent des données couvrant plusieurs types d'environnements. Le coût et le risque de ces violations de données sont aggravés par une matrice de réglementations en constante évolution et des sanctions sévères en cas de défaut de conformité.

Face à ces défis, la visibilité et le contrôle de la répartition de données dans le cloud hybride doivent être une priorité absolue pour les organisations de tous types et reposer sur un chiffrement renforcé et des politiques de sécurité et d'accès aux données. Les sociétés doivent rechercher des technologies de sécurité des données et de conformité qui fonctionnent sur toutes les plateformes, leur permettant ainsi de protéger les données lors des transferts entre les bases de données, les applications et les services déployés dans les environnements de cloud hybride.

Les solutions de surveillance de l'activité des données peuvent contribuer à garantir la mise en place de contrôles appropriés, tout en imposant activement ces politiques, par exemple en détectant rapidement toute activité suspecte et en bloquant les menaces en temps réel pour les magasins de données critiques.

En outre, les nouvelles technologies, telles que la gestion de la sécurité des données, peuvent permettre de trouver des données inconnues et sensibles dans le cloud, notamment des actifs structurés et non structurés au sein des fournisseurs de services de cloud, des propriétés SaaS (logiciel en tant que service) et des lacs de données. Cela peut aider à identifier et à atténuer les vulnérabilités dans les configurations, les autorisations d'utilisation et les flux de données sous-jacents des magasins de données. Alors que les organisations continuent de s'orienter vers des opérations hybrides multicloud, il est essentiel de déployer de solides stratégies de gestion des identités et des accès (IAM) qui intègrent des technologies telles que l'authentification multi-facteur (MFA), en mettant particulièrement l'accent sur la gestion des comptes d'utilisateurs privilégiés disposant d'un niveau d'accès élevé.

# 3

**S'appuyer sur l'IA et l'automatisation de la sécurité pour gagner en vitesse et en précision**

Dans le rapport de 2023, seulement 28 % des organisations déclarent utiliser largement l'IA et l'automatisation pour la sécurité dans leurs opérations, ce qui signifie que de nombreuses organisations ont l'opportunité unique d'améliorer leur vitesse, leur précision et leur efficacité. Une utilisation intensive de l'IA et de l'automatisation appliquées à la sécurité a permis de réaliser près de 1,8 million de dollars d'économies sur les coûts liés aux violations de données et de réduire le temps d'identification et d'endiguement d'une violation de plus de 100 jours par rapport aux organisations qui ne l'utilisent pas.

Les équipes de sécurité peuvent bénéficier de l'intégration de l'IA et de l'automatisation de la sécurité dans l'ensemble de leurs outils. Par exemple, l'utilisation de l'IA et de l'automatisation dans les outils de détection des menaces et les outils de réponse peut permettre aux analystes de détecter les nouvelles menaces avec plus de précision et de contextualiser et trier les alertes de sécurité plus efficacement. Ces technologies peuvent également automatiser certaines parties du processus d'examen des menaces ou recommander des actions pour accélérer la réponse. En outre, les solutions d'identité et de sécurité des données basées sur l'IA peuvent aider à renforcer une posture de sécurité proactive en identifiant les transactions à haut risque, en les protégeant avec un minimum de friction pour les utilisateurs et en corrélant plus efficacement les comportements suspects.

Lorsque vous intégrez l'IA à vos opérations de sécurité, recherchez des technologies qui offrent des cas d'utilisation fiables et matures avec une précision, une efficacité et une transparence démontrées afin d'éliminer les risques de parti pris, les zones d'ombre ou les dérives. Dans le cas de l'IA, les organisations doivent planifier un modèle opérationnel qui favorise l'apprentissage continu au fil de l'évolution des menaces et des capacités technologiques.

Les organisations peuvent également bénéficier d'une approche qui intègre étroitement les technologies de sécurité de base pour des flux de travail plus fluides et la possibilité de partager des analyses dans des pools de données communs. Les responsables de la sécurité des systèmes d'information (CISO) et les responsables des opérations de sécurité (SecOps) peuvent également utiliser des rapports de renseignement sur les menaces pour améliorer la reconnaissance des modèles et la visibilité des menaces émergentes.

# 4

**Renforcer la résilience en maîtrisant votre périmètre de vulnérabilité et en répétant les procédures de RI**
Maîtrisez votre exposition aux attaques les plus probables dans votre secteur et votre organisation, et priorisez votre stratégie de sécurité en conséquence. Des outils tels que ASM ou des techniques telles que la simulation adversaire peuvent aider les organisations à disposer d'une perspective mieux documentée sur les agresseurs dans leur profil de risque et leurs vulnérabilités uniques, y compris les vulnérabilités les plus facilement exploitables.

En outre, il a été démontré que le fait de disposer d'une équipe qui maîtrise déjà les bons protocoles et outils pour répondre à un incident réduit considérablement les coûts et le temps nécessaire pour identifier et endiguer la violation.

La planification et les tests RI figuraient déjà parmi les 3 principaux facteurs d'atténuation des coûts dans le rapport de 2023, mais les données ont également montré que les organisations qui avaient effectué une mise en place robuste de ces contre-mesures ont réduit le coût lié aux violations de données de 1,49 million de dollars par rapport aux organisations ayant un niveau d'adoption faible ou nul de ces mêmes mesures. Enfin, les incidents ont été résolus dans un délai plus court de 54 jours. Constituez une équipe RI dédiée, rédigez des protocoles RI et testez régulièrement les plans RI avec des exercices théoriques ou des simulations, par exemple sous forme de « cyber range ». Le fait d'avoir un fournisseur RI sous contrat peut également aider à réduire le délai de réponse à une violation.

Enfin, les organisations doivent adopter des pratiques de segmentation du réseau pour limiter la propagation des attaques et l'étendue des dommages qu'elles peuvent causer, renforcer la résilience globale et réduire les efforts de reprise.

*Les pratiques de sécurité recommandées sont fournies à des fins de formation sans garantie de résultat.*

04

# À propos du Ponemon Institute et d'IBM Security

**Ponemon Institute**
Fondée en 2002, le Ponemon Institute est un institut indépendant spécialisé dans la recherche et la formation, dont le but est de promouvoir des pratiques responsables de gestion de l'information et de la confidentialité dans le secteur public et privé. Notre mission est de réaliser des études empiriques de haute qualité portant sur des questions critiques affectant la gestion et la sécurité des informations sensibles sur les personnes et les organisations.

Dans le cadre de ses enquêtes commerciales, le Ponemon Institute respecte strictement la confidentialité des données et des personnes et les règles éthiques propres aux études et ne collecte pas d'informations personnelles identifiables auprès de personnes, ni d'informations identifiant une société.

De plus, nous respectons des normes de qualité très strictes qui garantissent qu'aucune question superflue, non pertinente ou inappropriée ne sera posée aux participants.

**Le logiciel IBM Security**
IBM Security contribue à la sécurité des gouvernements et des grandes entreprises du monde grâce à un portefeuille intégré de produits et de services de sécurité dotés de fonctionnalités dynamiques reposant sur l'IA et l'automatisation. Le portefeuille, soutenu par la recherche IBM Security X-Force®, permet aux organisations d'anticiper les menaces, de protéger les données en cas de transferts et de réagir avec rapidité et précision sans freiner l'innovation métier. Des milliers d'organisations collaborent en toute confiance avec IBM pour évaluer, mettre en œuvre et gérer les transformations des mesures de sécurité.

IBM gère l'une des plus grandes organisations de recherche, de développement et de distribution de services de sécurité au monde. L'entreprise surveille également plus de 150 milliards d'événements de sécurité chaque jour dans plus de 130 pays et a déposé plus de 10 000 brevets de sécurité à travers le monde.

Si vous avez des questions ou des commentaires au sujet de ce rapport, y compris pour obtenir la permission de citer ou de reproduire son contenu, veuillez nous contacter par courrier, téléphone ou e-mail aux coordonnées suivantes :

Ponemon Institute LLC
Attn : Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA
1.800.887.3118
research@ponemon.org

## En savoir plus sur l'amélioration de votre stratégie de sécurité

Visitez ibm.com/security.

Prenez part à la conversation au sein de la communauté IBM Security.

# Passez à l'étape suivante

**Solutions d'IA pour la cybersécurité**
Réduisez les temps de réponse de votre sécurité et boostez la productivité.
En savoir plus

**Solutions de détection et de réponse aux menaces**
Donnez aux équipes de sécurité les moyens de surmonter les menaces de manière rapide, précise et efficace.
En savoir plus

**Solutions de sécurité cloud**
Intégrez la sécurité dans votre parcours vers le multicloud hybride.
En savoir plus

**Solutions contre les ransomwares**
Gérez les risques de cybersécurité et les vulnérabilités pour minimiser l'impact des ransomwares.
En savoir plus

**Solutions de gestion des identités et des accès**
Connectez chaque utilisateur, API et unité à toutes les applications en toute sécurité.
En savoir plus

**Services de réponse aux incidents et de détection des menaces**
Gérez et répondez de manière proactive aux menaces de sécurité.
En savoir plus

**Solutions de sécurité et de protection des données**
Protégez les données et simplifiez la conformité dans les clouds hybrides.
En savoir plus

**Gestion du périmètre de vulnérabilité**
Gérez l'évolution de votre empreinte numérique et améliorez rapidement la cyber-résilience de votre organisation.
En savoir plus

**Solutions Unified endpoint management**
Faites évoluer votre personnel mobile en sécurisant et en gérant n'importe quelle unité.
En savoir plus

**Services de gouvernance, de gestion des risques et de conformité**
Améliorez la maturité de votre cybersécurité grâce à une approche de gouvernance, de gestion des risques et de conformité intégrée.
En savoir plus

**Planifier une consultation individuelle**
Rencontrez un spécialiste IBM Security X-Force pour évaluer vos besoins.
En savoir plus

**Participez à un atelier IBM Security Framing and Discovery**
Obtenez de l'aide pour moderniser votre programme de sécurité.
En savoir plus

Compagnie IBM France
17 avenue de l’Europe
92275 Bois-Colombes Cedex
IBM Corporation
New Orchard Road
Armonk, NY 10504

Réalisé aux
États-Unis d'Amérique
Juillet 2023



Les informations contenues dans le présent document étaient à jour à la date de sa publication initiale et peuvent être modifiées sans préavis par IBM. Les offres mentionnées dans le présent document ne sont pas toutes disponibles dans tous les pays où la société IBM est présente.

Toutes les références clients mentionnées ou décrites illustrent la façon dont certains clients ont utilisé les produits IBM et précisent les résultats qu'ils ont pu obtenir. Les chiffres réels en termes de coûts environnementaux et de performances peuvent varier d'un client à l'autre en fonction de la configuration et des conditions de fonctionnement. En général, les résultats attendus ne peuvent pas être garantis, car les résultats de chaque client dépendent entièrement des systèmes du client et des services commandés. LES INFORMATIONS CONTENUES DANS LE PRÉSENT DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT SANS AUCUNE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET AUCUNE GARANTIE OU CONDITION D'ABSENCE DE CONTREFAÇON. Les produits IBM sont garantis conformément aux dispositions des contrats qui régissent leur utilisation.

Déclaration de bonnes pratiques de sécurité : la sécurité des systèmes informatiques consiste à protéger les systèmes et les informations par la prévention, la détection et la réponse aux accès non autorisés depuis l'intérieur et l'extérieur de votre entreprise. Tout accès non autorisé peut conduire à la modification, à la destruction, au détournement ou à l'utilisation abusive d'informations, ainsi qu'à l'endommagement ou à l'utilisation abusive de vos systèmes, y compris pour attaquer d'autres personnes. Aucun système ou produit informatique ne doit être considéré comme entièrement sécurisé, et aucun produit ou mesure de sécurité ne peut être totalement efficace pour empêcher des accès ou utilisations non autorisés. Les systèmes, produits et services d'IBM sont conçus pour fonctionner dans le cadre d'une stratégie de sécurité globale et conforme à la loi qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produits ou services pour optimiser leur efficacité. IBM NE GARANTIT PAS QUE LES SYSTÈMES, PRODUITS OU SERVICES SONT PROTÉGÉS CONTRE LES AGISSEMENTS MALVEILLANTS OU ILLÉGAUX D'UN TIERS OU QU'ILS PROTÉGERONT VOTRE ENTREPRISE CONTRE DE TELS AGISSEMENTS.

Il incombe au client de respecter les lois et réglementations qui lui sont applicables. IBM ne fournit pas de conseils juridiques et ne déclare ni ne garantit que ses services ou produits garantiront que le client est en conformité avec la législation ou la réglementation en vigueur. Toutes les déclarations relatives à l'orientation et aux intentions futures d'IBM sont susceptibles d'être modifiées ou retirées sans préavis et ne représentent que des objectifs.