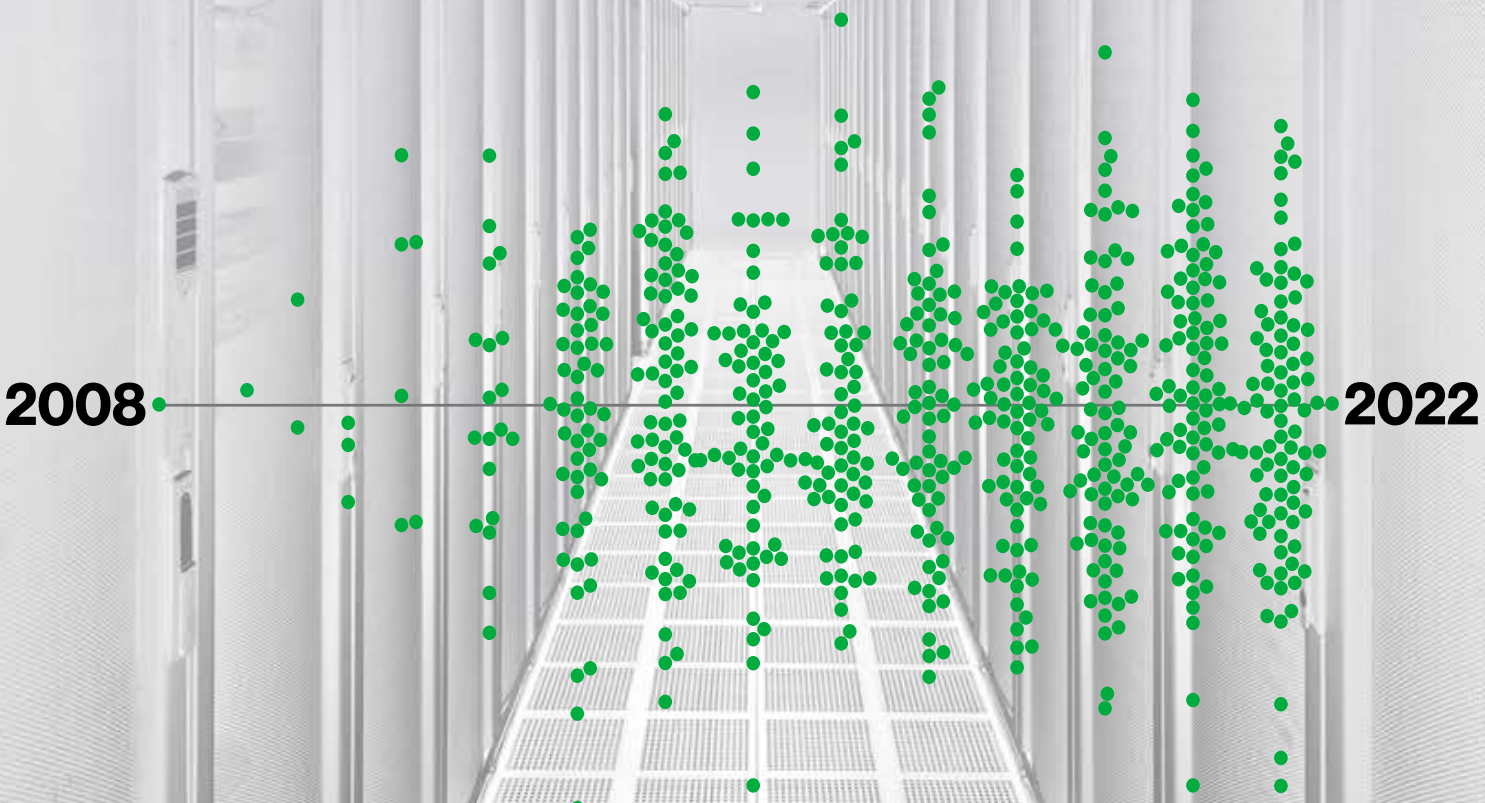
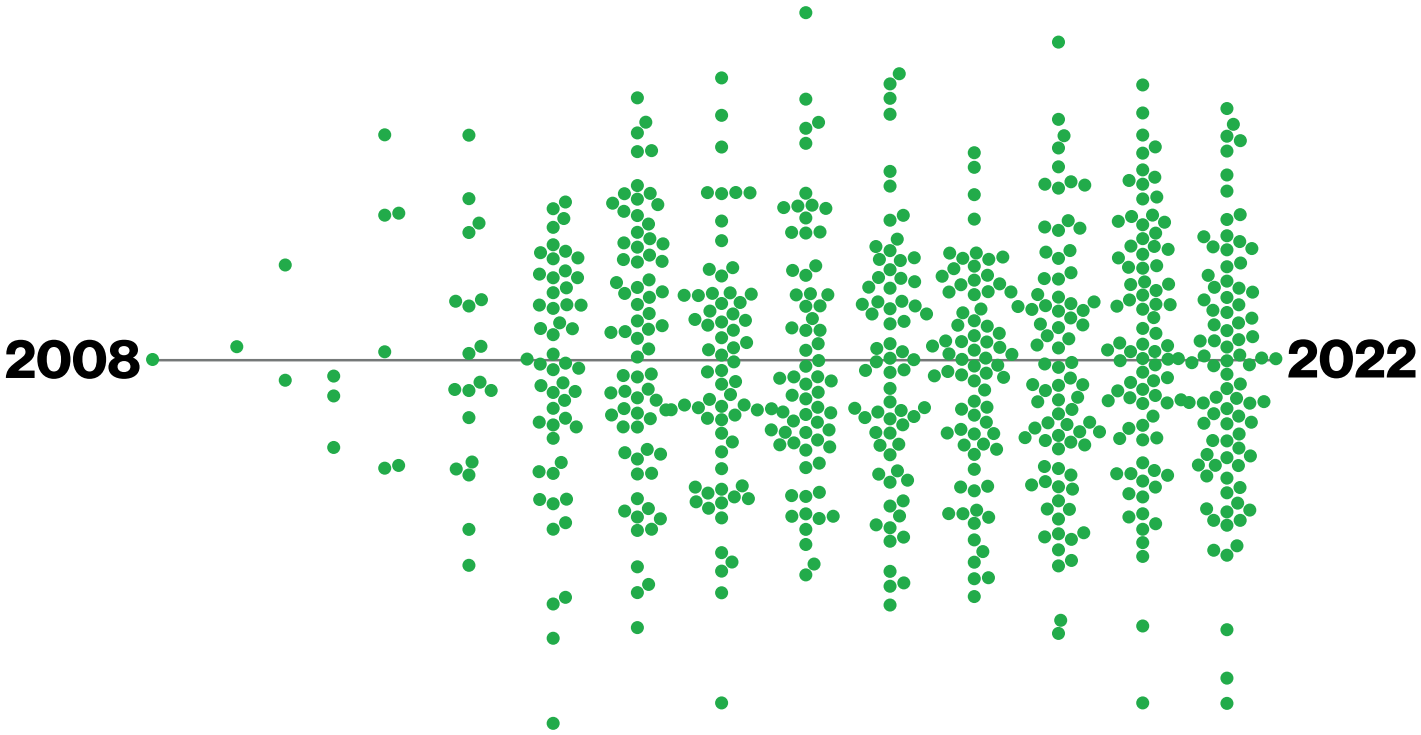
DBIR

2022 Data Breach Investigations Report

Document de synthèse





À propos de la couverture

En 2008, la couverture de notre tout premier rapport représentait une chaise vide dans une salle des serveurs. Les plus fidèles de nos lecteurs s'en souviendront peut-être. À l'époque, nous voulions attirer l'attention sur le manque de vigilance des entreprises quant à la sécurité de leurs données et de leurs équipements informatiques. La couverture du DBIR reprend le même thème, un peu par nostalgie mais surtout pour illustrer la difficulté des entreprises à garder un œil sur leurs collaborateurs et leurs systèmes. La frise chronologique tachetée de points verts représente le nombre de contributeurs à chaque édition du rapport ces quinze dernières années.

Sommaire

Verizon Data Breach Investigations Report (DBIR) 15e édition

Comme nous l'écrivions en 2018, le rapport DBIR fournit « aux professionnels de la sécurité des éclairages concrets sur les activités cybercriminelles qui menacent les entreprises ». Et cette 15e édition ne déroge pas à la règle. Vous y trouverez des informations sur les menaces qui pourraient impacter votre organisation aujourd'hui, ainsi que quelques références aux rapports précédents pour illustrer l'évolution du champ des menaces au fil des ans.

Si l'année passée sortait de l'ordinaire à bien des égards, elle a sans aucun doute marqué les esprits sur le plan des cyberattaques. Des attaques ultra-médiatisées contre des infrastructures critiques aux compromissions majeures contre la supply chain, les cybercriminels à motivation financière et les très redoutables groupes étatiques nous avaient rarement, voire jamais, habitués à une cadence aussi infernale que celle des douze derniers mois. Comme lors des éditions précédentes, nous analyserons nos données sur le sujet et sur d'autres types d'opérations régulièrement lancées contre les entreprises. Cette année, notre étude porte sur 23 896 incidents, dont 5 212 compromissions avérées. Ces données proviennent de compromissions et d'incidents sur lesquels le Verizon Threat Research Advisory Center (VTRAC) a enquêté, mais aussi de nos 87 généreux contributeurs à travers le monde, sans lesquels ce rapport n'aurait jamais pu exister. Nous espérons que le DBIR vous éclairera sur les tactiques les plus utilisées contre les entreprises en général et votre secteur en particulier, mais aussi sur les moyens de protection à votre disposition. L'angle éditorial du rapport consiste habituellement à comparer et contraster les tendances. Or, cette année, pour fêter les 15 ans de cette publication, nous nous sommes attachés à illustrer autant que possible l'évolution des tactiques au fil des ans (cf. figures 1 et 2 ci-dessous). Dans les pages qui suivent, vous découvrirez les principales conclusions du DBIR 2022. N'hésitez pas à envoyer cette synthèse à vos collègues et à télécharger le rapport complet pour une vue plus détaillée des menaces qui vous concernent. Bonne lecture !

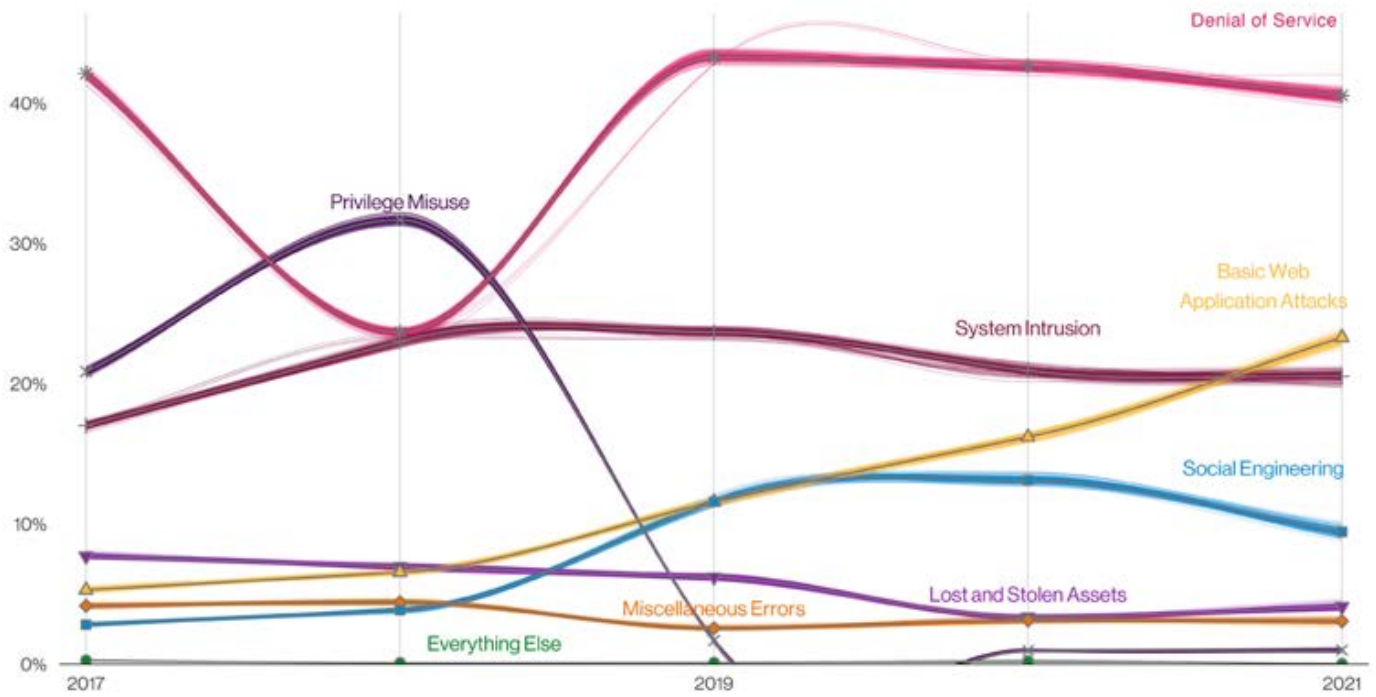


Figure 1. Évolution chronologique des incidents

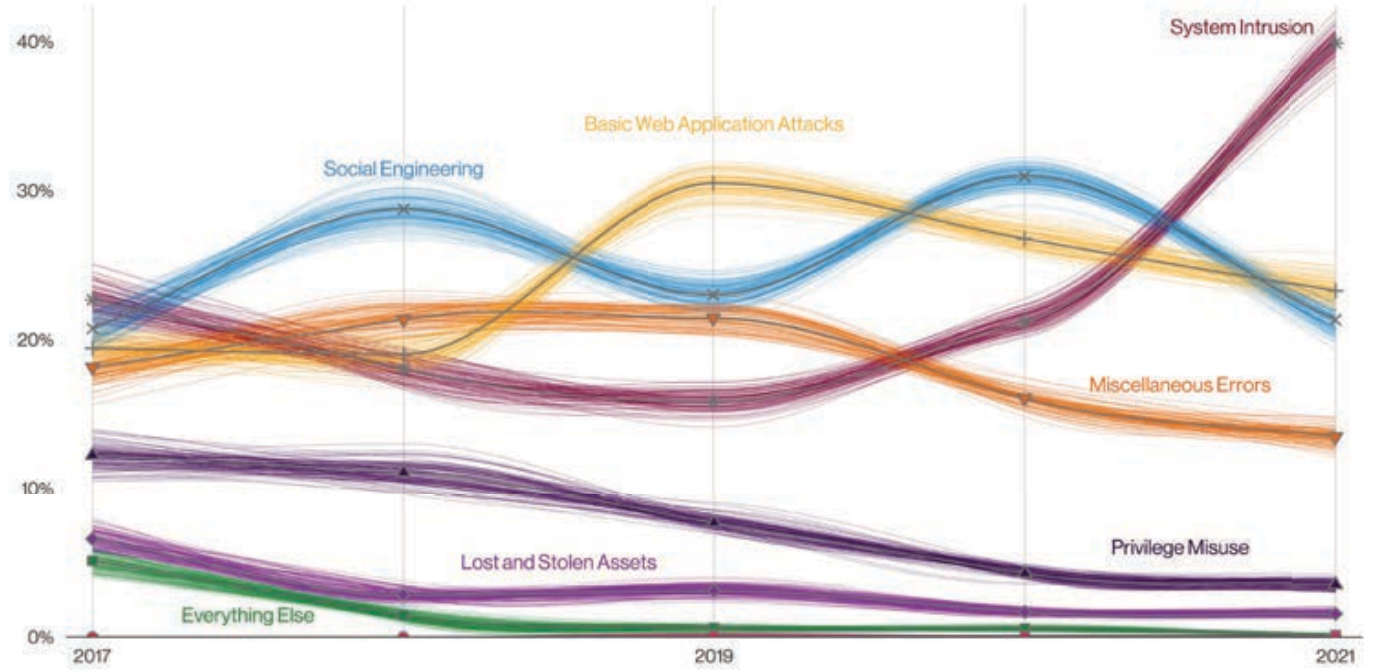


Figure 2. Évolution chronologique des compromissions

À retenir

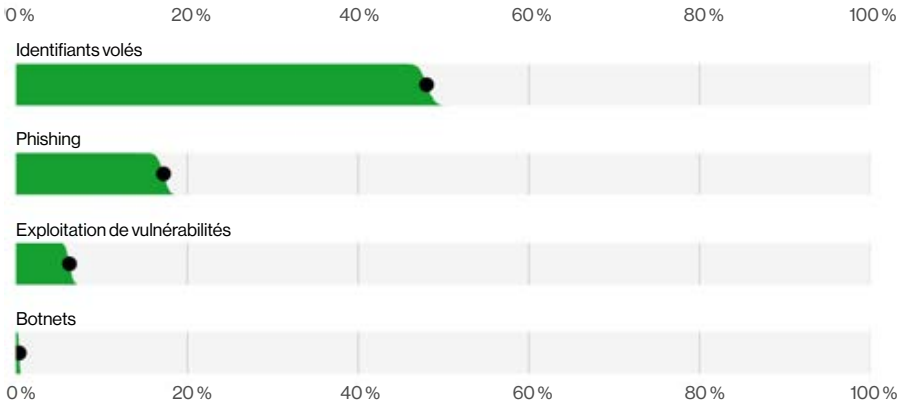


Figure 3. Part des quatre grands vecteurs dans les compromissions hors erreurs et abus de privilèges (n = 4 250)

Les attaquants disposent de quatre grands vecteurs pour infiltrer votre environnement : les identifiants volés, le phishing, l'exploitation de vulnérabilités et les botnets. Tous les quatre sont omniprésents dans le rapport DBIR. Chaque entreprise a donc besoin d'un plan pour s'en prémunir.

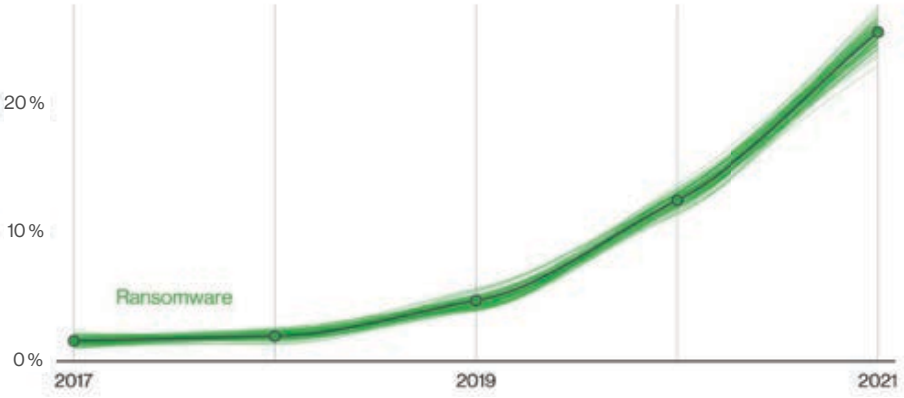


Figure 4. Évolution chronologique de la part des ransomwares dans les compromissions

Cette année, la prolifération des ransomwares s'est poursuivie avec une hausse de près de 13 % pour atteindre 25 % du total des compromissions – soit une croissance égale à celle des cinq dernières années réunies. Aussi inévitables et dévastateurs soient-ils, les ransomwares restent, par essence, un système de monétisation de l'accès à une organisation. Éliminer les quatre grands vecteurs évoqués plus haut vous aidera à bloquer les principales voies d'accès de ce type de menaces à votre réseau.

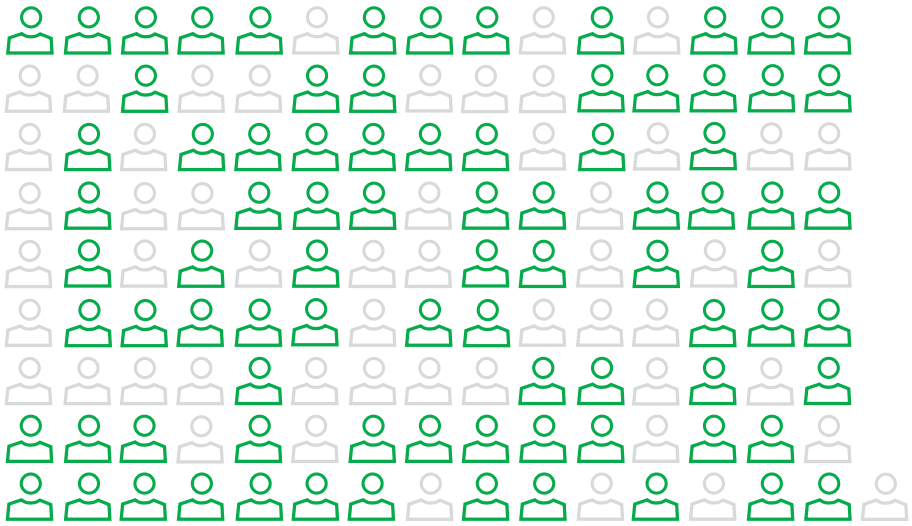
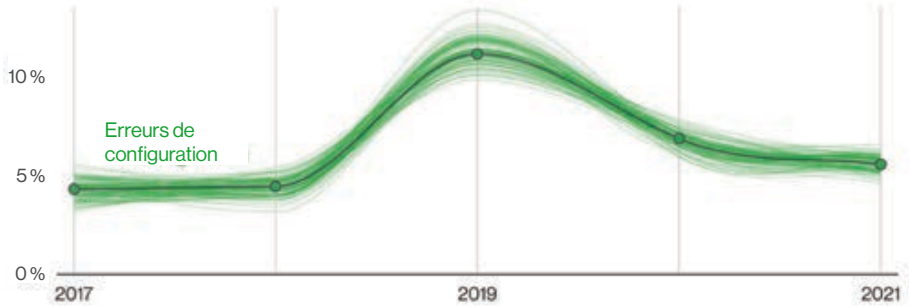


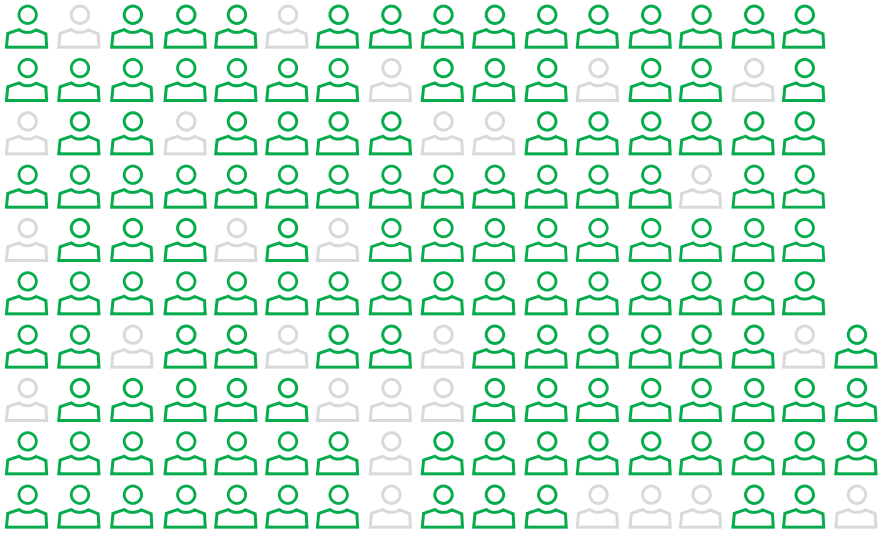
Figure 5. La part des partenaires dans les incidents par intrusion système (n = 3 403). Chaque glyphe représente 25 incidents.

En 2021, nous avons pu constater qu'une seule compromission majeure de la supply chain pouvait avoir des répercussions énormes, à tel point que cette supply chain a été impliquée dans 62 % des incidents en 2021. Pour les attaquants, il suffit de compromettre le bon partenaire pour démultiplier leur capacité de nuisance. Contrairement aux groupes à visées financières, les groupes d'attaque à la solde d'États sautent parfois l'étape de la compromission et se contentent d'exploiter l'accès fourni.



Les erreurs, autre tendance majeure, restent souvent liées à des systèmes de stockage cloud mal configurés. Si cette tendance se stabilise légèrement depuis deux ans, il ne faudrait surtout pas sous-estimer la faillibilité des collaborateurs de l'entreprise.

Figure 6. Évolution chronologique de la part des erreurs de configuration dans les compromissions



En clair, le facteur humain reste une source de compromission importante. En 2021, 82 % des compromissions ont impliqué le facteur humain. Vol d'identifiants, phishing, perte d'ordinateur portable… le facteur humain reste à l'origine de nombreux incidents et compromissions.

Figure 7. La part de l'humain dans les compromissions (n = 4 110). Chaque glyphe représente 25 compromissions.

Gros plan par secteur

Quels que soient votre secteur et la taille de votre entreprise, la cybercriminalité constitue un risque à ne pas prendre à la légère. Toutefois, le type et la fréquence des attaques peuvent varier en fonction de la taille, de la fonction et de l'implantation géographique de votre organisation. Pour mettre en place un système de défense efficaces, vous devez non seulement examiner le champ des menaces dans son ensemble, mais aussi celles qui vous concernent le plus. Cette année encore, nous proposons un état des lieux de 11 grands secteurs. Pour la première fois, nous avons également ajouté une section simple et claire à l'intention des très petites entreprises (de 10 salariés maximum). Enfin, nous vous proposons un tour d'horizon des schémas d'attaques dans différentes régions du globe afin d'observer les spécificités de chacune d'elles. Comme toujours, notre classification sectorielle repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN).

Hôtellerie et restauration (SCIAN 72)

S'il connaît une baisse du nombre d'intrusions système depuis 2016, le secteur de l'hôtellerie et de la restauration demeure la cible de malwares propagés par e-mail et de compromissions d'applications web à l'aide d'identifiants volés.

Volume	156 incidents, dont 69 compromissions de données confirmées
Principaux schémas	L'intrusion système, le déni de service et les attaques d'applications web de base représentent 84 % de tous les incidents.
Attaquants	Externes (90 %), internes (10 %) (compromissions) Externes (95 %), internes (5 %) (tous les incidents)
Motivations	Financières (91 %), espionnage (9 %) (compromissions) Financières (64 %), espionnage (36 %) (tous les incidents)
Données compromises	Identifiants (45 %), données personnelles (45 %), données de paiement (41 %), autres (18 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4)
Ce qui n'a pas changé	Ce secteur demeure la cible d'attaquants à visées financières, friands d'informations personnelles et de données de paiement.

Arts, divertissements et loisirs (SCIAN 71)

Si les intrusions système et les attaques d'applications web de base ont échangé leur place dans le top 3 des schémas d'attaque, les erreurs diverses continuent d'occuper la dernière marche de ce triste podium. Côté incidents, les attaques par déni de service constituent encore un problème de taille pour le secteur, surtout sur le marché des jeux d'argent.

Volume	215 incidents, dont 96 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web de base, l'intrusion système et les erreurs diverses représentent 80 % des compromissions.
Attaquants	Externes (74 %), internes (26 %) (compromissions)
Motivations	Financières (97 %), représailles (3 %) (compromissions)
Données compromises	Données personnelles (66 %), identifiants (49 %), autres (23 %), données médicales (15 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4)
Ce qui n'a pas changé	Les catégories restent les mêmes. Seul l'ordre change. La compromission des données médicales reste un risque majeur dans ce secteur.

Enseignement (SCIAN 61)

Comme la plupart des autres secteurs, l'enseignement connaît une explosion du nombre d'attaques par ransomware, qui représentent aujourd'hui plus de 30 % des compromissions. En outre, les établissements doivent se protéger contre le vol d'identifiants et les attaques de phishing susceptibles d'exposer les données personnelles de leurs salariés et de leurs étudiants.

Volume	1 241 incidents, dont 282 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et les erreurs diverses représentent 80 % des compromissions.
Attaquants	Externes (75 %), internes (25 %) (compromissions)
Motivations	Financières (95 %), espionnage (5 %) (compromissions)
Données compromises	Données personnelles (63 %), identifiants (41 %), autres (23 %), internes (10 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4)
Ce qui n'a pas changé	Surtout ciblé par des acteurs externes à visées financières, ce secteur continue de subir des attaques contre son infrastructure externe. Toutefois, les erreurs restent aussi l'une des principales causes de compromission.

Finance et assurance (SCIAN 52)

Le secteur financier continue de subir les assauts du crime organisé, attiré par la manne qu'il représente. Ses armes de prédilection : l'ingénierie sociale (phishing), le hacking (utilisation d'identifiants volés) et les malwares (ransomwares). Enfin, les erreurs diverses (souvent des erreurs d'adressage) sont très courantes depuis trois ans.

Volume	2 527 incidents, dont 690 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web de base, l'intrusion système et les erreurs diverses représentent 79 % des compromissions.
Attaquants	Externes (73 %), internes (27 %) (compromissions)
Motivations	Financières (95 %), espionnage (4 %), représailles (1 %) (compromissions)
Données compromises	Données personnelles (71 %), identifiants (40 %), autres (27 %), bancaires (22 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4), Protection des données (CSC 3)
Ce qui n'a pas changé	Comme l'année dernière, les erreurs et les attaques d'applications web de base restent une source majeure de compromission dans ce secteur.

Santé (SCIAN 62)

Dans ce secteur, les attaques d'applications web de base ont pris le pas sur les erreurs diverses comme cause de compromissions. Toutefois, les erreurs constituent encore un problème de taille.

Volume	849 incidents, dont 571 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web de base, les erreurs diverses et l'intrusion système représentent 76 % des compromissions.
Attaquants	Externes (61 %), internes (39 %) (compromissions)
Motivations	Financières (95 %), espionnage (4 %), commodité (1 %), représailles (1 %) (compromissions)
Données compromises	Données personnelles (58 %), médicales (46 %), identifiants (29 %), autres (29 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4), Gestion du contrôle des accès (CSC 6)
Ce qui n'a pas changé	Les trois principaux schémas restent les mêmes. Seul l'ordre change. La répartition entre les différents types d'attaquants est identique à celle de l'année dernière (au point de pourcentage près).

Information (SCIAN 51)

Cette année, l'intrusion système devance les erreurs et les attaques d'applications web de base sur le podium des causes de compromissions. Côté incidents, les attaques DDoS conservent la première place. Ces deux dernières années ont été le théâtre d'une hausse significative du nombre de malwares, tandis que les erreurs semblent reparties à la baisse depuis leur hausse d'il y a cinq ans.

Volume	2 561 incidents, dont 378 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et les erreurs diverses représentent 81 % des compromissions.
Attaquants	Externes (76 %), internes (24 %) (compromissions)
Motivations	Financières (78 %), espionnage (20 %), idéologiques (1 %), représailles (1 %) (compromissions)
Données compromises	Données personnelles (66 %), autres (35 %), identifiants (27 %), internes (17 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4), Gestion du contrôle des accès (CSC 6)
Ce qui n'a pas changé	Comme l'année dernière, les erreurs et les attaques d'applications web de base restent une source majeure de compromission dans ce secteur.

Industrie (SCIAN 31-33)

Si l'industrie constitue toujours une cible lucrative pour les groupes d'espionnage, elle subit de plus en plus souvent les assauts d'autres cybercriminels dans le cadre d'attaques par déni de service, par identifiants volés et par ransomware.

Volume	2 337 incidents, dont 338 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 88 % des compromissions.
Attaquants	Externes (88 %), internes (12 %), partenaires (1 %) (compromissions)
Motivations	Financières (88 %), espionnage (11 %), représailles (1 %), secondaires (1 %) (compromissions)
Données compromises	Données personnelles (58 %), identifiants (40 %), autres (36 %), internes (14 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4)
Ce qui n'a pas changé	Les attaques d'applications web de base et par intrusion systèmes font encore partie des principaux schémas rencontrés dans ce secteur.

Exploitation minière, extraction de pétrole et de gaz (SCIAN 21) et compagnies d'énergie (SCIAN 22)

Les exploitations minières et les compagnies d'énergie subissent les mêmes types d'attaques que les autres secteurs étudiés, notamment le vol d'identifiants et l'exploitation de données à l'aide de ransomwares. Toutefois, elles sont également la cible d'un grand nombre d'attaques par ingénierie sociale comme le phishing.

Volume	403 incidents, dont 179 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, l'intrusion système et les attaques d'applications web de base représentent 95 % des compromissions.
Attaquants	Externes (96 %), internes (4 %) (compromissions)
Motivations	Financières (78 %), espionnage (22 %) (compromissions)
Données compromises	Identifiants (73 %), données personnelles (22 %), internes (9 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Gestion des comptes (CSC 5)
Ce qui n'a pas changé	Le secteur reste la cible d'attaquants à visées financières, mais aussi de groupes de cyberespionnage.

Services professionnels, scientifiques et techniques (SCIAN 54)

Dans ce secteur, les attaques par déni de service constituent un problème de taille. Si elles se soldent rarement par une compromission de données, leur impact reste parfois considérable. Cette année encore, l'intrusion système s'impose comme le principal schéma d'attaque. Bien que moins fréquente, l'ingénierie sociale fait malgré tout partie du trio de tête.

Volume	3 566 incidents, dont 681 compromissions de données confirmées
Principaux schémas	L'intrusion système, les attaques d'applications web de base et l'ingénierie sociale représentent 89 % des compromissions.
Attaquants	Externes (84 %), internes (17 %), multiples (1 %) (compromissions)
Motivations	Financières (90 %), espionnage (10 %) (compromissions)
Données compromises	Identifiants (56 %), données personnelles (48 %), autres (26 %), internes (14 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4)
Ce qui n'a pas changé	Même si leur classement a changé par rapport à l'année dernière, les trois principaux schémas d'attaque restent les mêmes (intrusion système, attaques d'applications web de base et ingénierie sociale).

Service public (SCIAN 92)

Dans ce secteur, l'intrusion système constitue désormais le principal schéma d'attaque. Les salariés des services publics demeurent une source de compromissions, même si ces dernières sont sept fois plus souvent le fruit d'une erreur que d'un acte de malveillance.

Volume	2 792 incidents, dont 537 compromissions de données confirmées
Principaux schémas	L'intrusion système, les erreurs diverses et les attaques d'applications web de base représentent 81 % des compromissions.
Attaquants	Externes (78 %), internes (22 %) (compromissions)
Motivations	Financières (80 %), espionnage (18 %), idéologiques (1 %), représailles (1 %) (compromissions)
Données compromises	Données personnelles (46 %), identifiants (34 %), autres (28 %), internes (28 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Gestion des comptes (CSC 5)
Ce qui n'a pas changé	Les erreurs diverses font encore partie du trio de tête des schémas d'attaque, à la même place que l'année dernière.

Retail (SCIAN 44-45)

Le retail subit les mêmes types d'attaques que l'année dernière : utilisation d'identifiants volés, phishing et ransomware.

Volume	629 incidents, dont 241 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 84 % des compromissions.
Attaquants	Externes (87 %), internes (13 %) (compromissions)
Motivations	Financières (98 %), espionnage (2 %) (compromissions)
Données compromises	Identifiants (45 %), données personnelles (27 %), autres (25 %), données de paiement (24 %) (compromissions)
Principaux contrôles de sécurité IG1	Programme de sensibilisation et de formation à la sécurité (CSC 14), Gestion du contrôle des accès (CSC 6), Configuration sécurisée des ressources et logiciels d'entreprise (CSC 4)
Ce qui n'a pas changé	Les entreprises de ce secteur sont encore et toujours la cible d'une grande variété d'attaquants dont les tactiques vont du phishing au déploiement de malwares pour collecter des données de cartes bancaires saisies dans des formulaires en ligne.

Très petites entreprises (TPE)

Lorsque les cybercriminels font les gros titres, c'est généralement parce qu'une grande entreprise est tombée dans leurs filets. Toutefois, contrairement aux idées reçues, les très petites structures constituent des cibles autant, voire plus attrayantes à certains égards.

Pour les cyberattaquants, tout est bon à prendre. À tel point qu'un seul cyberincident peut parfois contraindre les petites entreprises à déposer le bilan, comme on a pu le constater par le passé. Même pour les TPE de moins de 10 salariés, toutes les précautions doivent être prises.

D'après nos analyses, les ransomwares représentent le type d'attaque le plus courant contre ces structures. Un ransomware, ou rançongiciel, désigne un type de programme malveillant qui chiffre vos données pour vous empêcher de les consulter et de les utiliser. Une fois le ransomware déclenché, les attaquants demandent une somme d'argent (souvent conséquente) en échange du déchiffrement des données. Le deuxième schéma d'attaque le plus courant à l'encontre des TPE est l'utilisation d'identifiants volés. Pour obtenir votre nom d'utilisateur et votre mot de passe, les attaquants ont le choix des armes : les attaques par force brute (un attaquant a recours à l'automatisation pour tester de multiples combinaisons de lettres, de symboles et de chiffres et ainsi deviner vos identifiants), différents types de malwares (d'où l'intérêt d'avoir un antivirus à jour), ou encore la réutilisation de mots de passe d'un autre site. Les attaques par ingénierie sociale (phishing, pretexting, etc.) sont elles aussi assez courantes. Certaines peuvent d'ailleurs s'avérer très convaincantes (par exemple, une facture qui semble venir d'un fournisseur connu, où seules les coordonnées bancaires sont différentes). Si la plupart de ces attaques sont lancées par e-mail, les cybercriminels n'hésitent plus à décrocher leur téléphone pour convaincre leur cible de la légitimité de leur demande.

Pour une liste détaillée de recommandations pratiques et pour savoir qui contacter en cas de suspicion d'attaque, lisez la section consacrée aux très petites entreprises dans notre rapport complet.

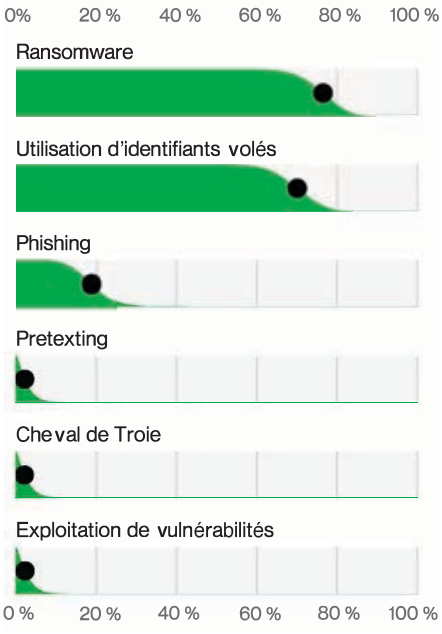


Figure 8. Vecteurs de compromission dans les TPE (n = 61)

Résultats par région

Cette édition du DBIR est la troisième à vous proposer une analyse des incidents par région. Nous espérons que nos lecteurs trouveront dans cette perspective globale des informations utiles et instructives. Comme nous l'avons mentionné par le passé, notre visibilité sur une région donnée dépend de multiples facteurs : la présence de contributeurs, les obligations de notification régionales, nos propres investigations, etc.

Asie-Pacifique (APAC)

En Asie-Pacifique, on constate un grand nombre d'attaques par hacking et par ingénierie sociale. En revanche, la proportion de ransomwares est bien inférieure à celle d'autres régions.

Volume	4 114 incidents, dont 283 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, les attaques d'applications web de base et l'intrusion système représentent à elles trois 98 % des compromissions.
Attaquants	Externes (98 %), internes (2 %) (compromissions)
Motivations	Financières (54 %), espionnage (46 %), secondaires (1 %) (compromissions)
Données compromises	Identifiants (72 %), internes (26 %), secrets (18 %), autres (11 %) (compromissions)
Ce qui n'a pas changé	Les attaques d'applications web de base et l'ingénierie sociale restent des menaces persistantes dans cette région.

Europe, Moyen-Orient et Afrique (EMEA)

Ici, l'augmentation des cas d'ingénierie sociale met en lumière le besoin de contrôles pour détecter rapidement ce type d'attaques. Quant à la persistance des attaques d'applications web de base en zone EMEA, elle montre bien que le vol d'identifiants reste également un problème de taille.

Volume	1 093 incidents, dont 307 compromissions de données confirmées
Principaux schémas	L'ingénierie sociale, l'intrusion système et les attaques d'applications web de base représentent 97 % des compromissions.
Attaquants	Externes (97 %), internes (3 %) (compromissions)
Motivations	Financières (79 %), espionnage (21 %) (compromissions)
Données compromises	Identifiants (67 %), internes (67 %), secrets (20 %), autres (18 %) (compromissions)
Ce qui n'a pas changé	Les principaux schémas d'attaque restent les mêmes. Seul l'ordre change. Dans cette région, les attaquants externes sont encore et toujours à l'origine de la grande majorité des compromissions.

Amérique du Nord (NA)

En Amérique du Nord, les intrusions système sont devenues le principal schéma d'attaque. Si l'ingénierie sociale a été supplantée par ce type de menaces, elle n'en reste pas moins un problème important dans cette région, à commencer par le phishing. Enfin, les attaques d'applications web de base continuent elles aussi de faire des victimes en entreprise.

Volume	4 504 incidents, dont 1 638 compromissions de données confirmées
Principaux schémas	L'intrusion système, l'ingénierie sociale et les attaques d'applications web de base représentent 90 % des compromissions.
Attaquants	Externes (90 %), internes (10 %), multiples (1 %) (compromissions)
Motivations	Financières (96 %), espionnage (3 %), représailles (1 %) (compromissions)
Données compromises	Identifiants (66 %), données internes (21 %), personnelles (20 %), autres (20 %) (compromissions)
Ce qui n'a pas changé	Les trois principaux schémas restent les mêmes. Seul l'ordre change. Dans cette région, les acteurs externes sont encore à l'origine d'un grand nombre de compromissions.

La force d'un collectif soudé

L'équipe de rédaction du DBIR continue de s'appuyer sur la structure VERIS (Vocabulary for Event Recording and Incident Sharing) pour classifier et analyser les incidents et compromissions. Nous avons développé des mappings en collaboration avec le framework MITRE ATT&CK et le Center for Internet Security's Critical Security Controls (CIS CSC) afin d'aider les entreprises à élaborer et maintenir un programme de cybersécurité basé sur des données précises et actualisées. Nous travaillons également avec d'autres acteurs du secteur au projet Attack Flow, dont le but est de disséquer l'enchaînement des événements associés à une attaque. Ces points de référence, ainsi que d'autres frameworks, nous ont permis d'optimiser nos analyses et de les mettre à la disposition de toute la communauté de la sécurité de l'information.

Bonnes pratiques

Cette année encore, nous avons aligné nos conclusions sur les contrôles du Center for Internet Security, l'idée étant de traduire les observations du DBIR en pratiques de sécurité concrètes. Nous vous présentons ici les principaux contrôles nécessaires à la réduction des risques pour la plupart des entreprises.

Contrôle 3 – Protection des données

Ce contrôle concerne les processus et les contrôles techniques destinés à identifier, classifier et traiter tous les types de données de l'organisation en toute sécurité. Il aide à prévenir les expositions accidentelles de données par e-mail et erreur de configuration.

Contrôle 4 – Configuration sécurisée des ressources et logiciels d'entreprise

Outre son intitulé relativement long, ce contrôle comprend des mesures qui proposent des solutions de sécurité à intégrer dès le départ, et non à ajouter après coup. Ses avantages sont substantiels puisqu'il permet d'activer la fonction d'effacement à distance sur les équipements mobiles afin de réduire les compromissions dues à des erreurs, notamment de configuration, et à des pertes d'appareils.

Contrôle 5 – Gestion des comptes

Ce contrôle a pour principal objectif d'aider les entreprises à gérer les accès aux comptes et s'avère efficace contre les attaques par force brute et de « credential stuffing ».

Contrôle 6 – Gestion du contrôle des accès

Ce contrôle gère les droits et privilèges des utilisateurs. Il implémente l'authentification multifacteur pour l'accès à des zones sensibles de l'environnement, un dispositif essentiel contre l'utilisation d'identifiants volés.

Contrôle 14 – Programme de sensibilisation et de formation à la sécurité

Ce contrôle est un grand classique et son intitulé suffit à le décrire. Étant donné que nos analyses révèlent une prédominance des erreurs et des attaques par ingénierie sociale, il semble judicieux d'investir dans la sensibilisation et la formation technique des équipes à la sécurité pour les aider à évoluer dans un environnement semé d'embûches.

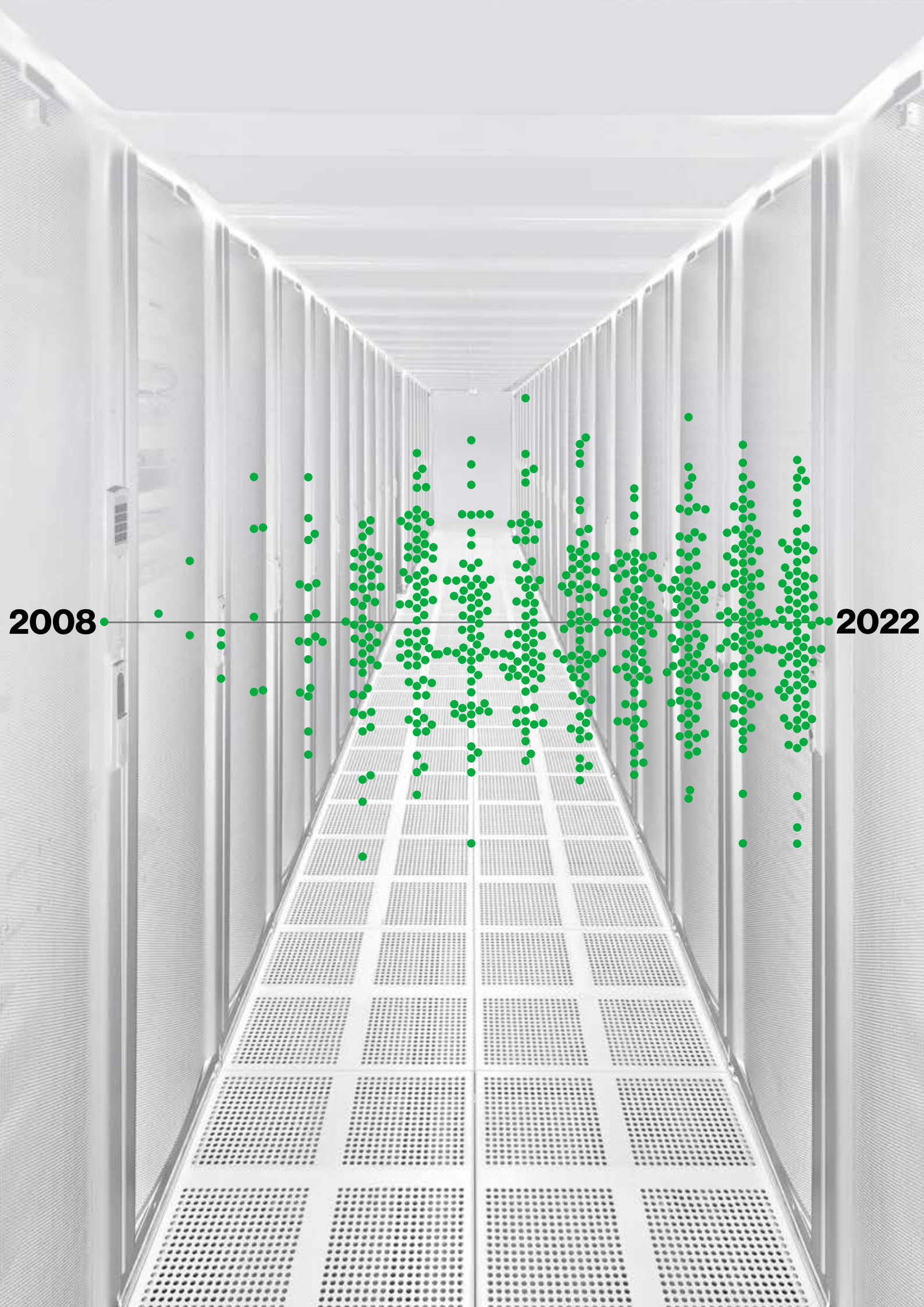
S'informer, c'est se préparer

Pour faire face aux menaces actuelles, vous devez pouvoir compter sur une information fiable.
Le rapport DBIR vous présente les acteurs, tendances et modes opératoires qui pèsent sur votre activité pour vous aider à mieux vous protéger et sensibiliser vos utilisateurs. Bénéficiez de tous les éclairages concrets dont vous avez besoin pour sécuriser votre entreprise.

Lisez le rapport DBIR 2022 complet sur https://www.verizon.com/business/fr-fr/resources/reports/dbir/

Envie d'œuvrer pour un monde digital plus sûr ?

Le DBIR s'appuie sur les contributions de dizaines d'entreprises. Pourquoi ne pas apporter votre pierre à l'édifice ? Apportez votre contribution au rapport 2023 ou faites-nous part de vos commentaires afin de nous aider à améliorer la prochaine édition. Écrivez-nous à dbir@verizon.com, contactez-nous par twitter à @VZDBIR et consultez la page VERIS GitHub : https://github.com/vz-risk/veris.


2008
2022