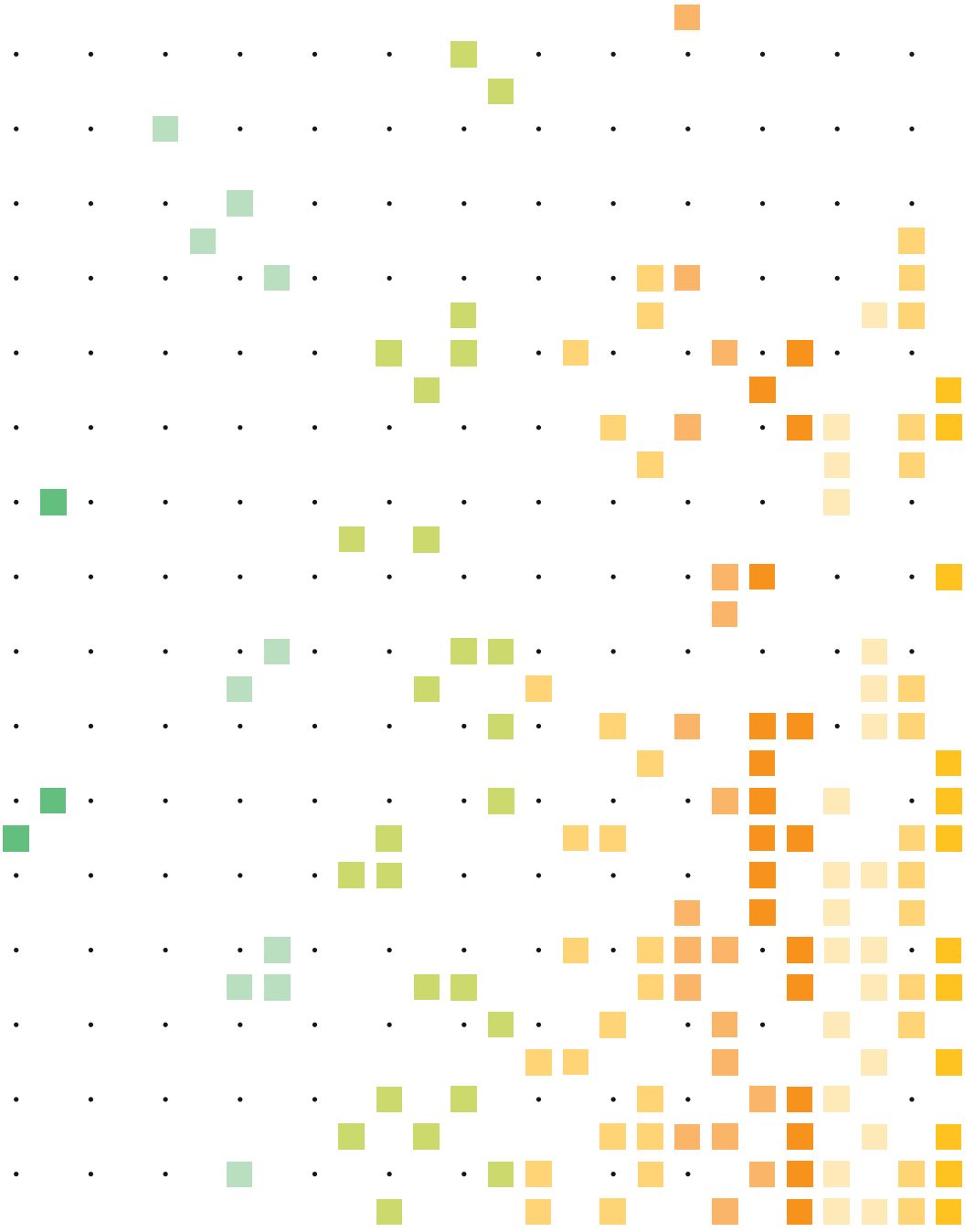
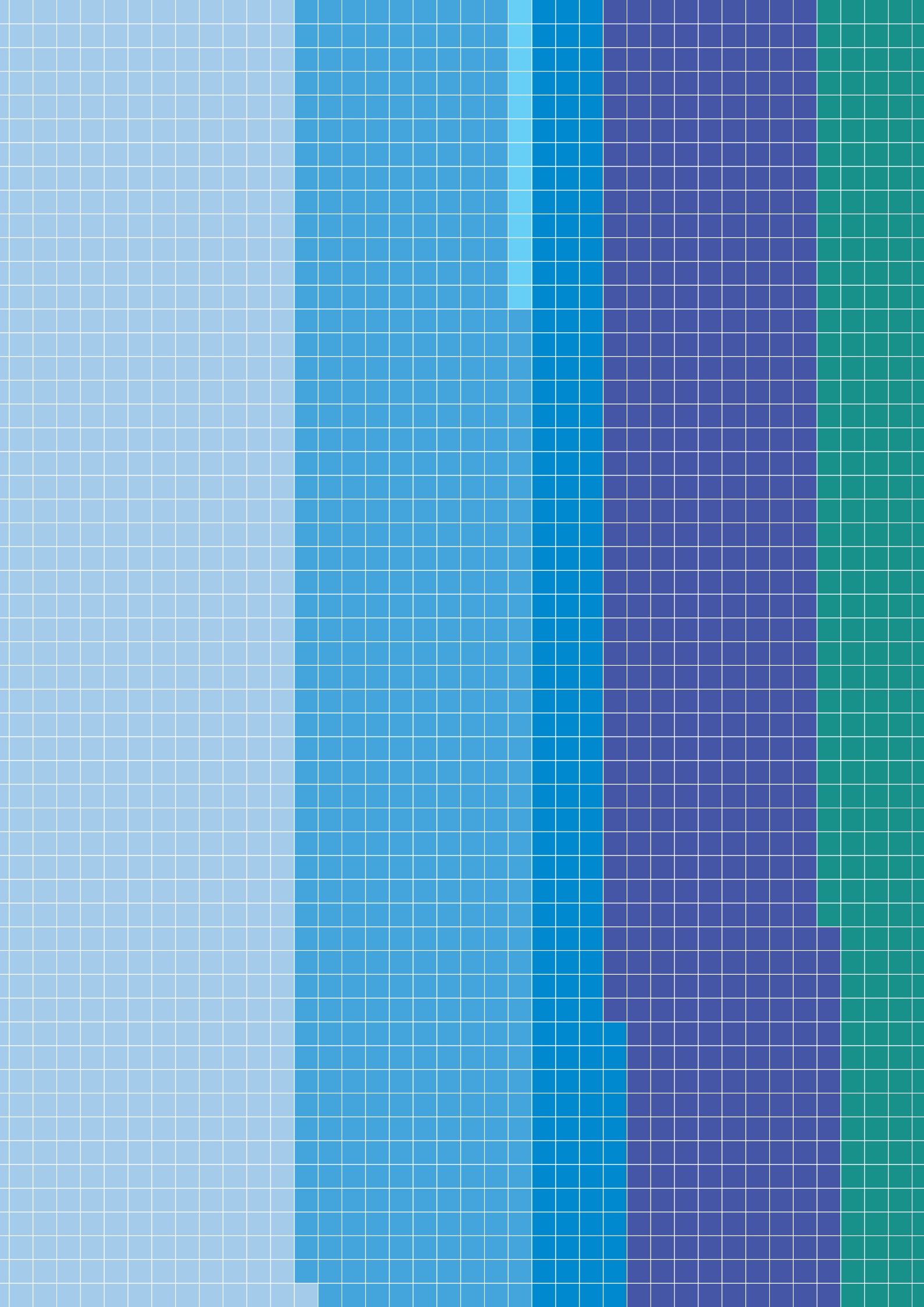
DBIR

2020 Rapport d'enquête sur les compromissions de données

Document de synthèse



verizon



3 950 compromissions

Les différentes couleurs du quadrillage que vous voyez sur cette page correspondent aux 16 secteurs d'activité et aux quatre régions du globe couverts par ce rapport. Chaque carré représente une compromission (ou 1,04 pour être précis) et le total s'élève à 4 675 carrés puisqu'une compromission peut apparaître à la fois pour un secteur et une région.

Nous avons également analysé un nombre record de 157 525 incidents, dont 32 002 étaient conformes aux exigences de notre étude. Les données recueillies cette année sont d'une exhaustivité telle qu'elles transparaissent à travers la couverture monochrome du rapport, comme une évocation imagée du rôle central de la data dans le DBIR. Parcourez-le sans plus attendre pour en découvrir les chiffres marquants.

Sommaire

Connaître les dangers pour mieux maîtriser les risques

Plus vous aurez une vision claire des menaces qui pèsent sur votre sécurité, plus vous multiplierez les chances de garder vos données et votre réputation intactes. C'est dans cet esprit que nous publions chaque année notre *rapport d'enquête sur les compromissions de données* (DBIR, Data Breach Investigations Report). Pour sa 13ème édition, ce document rassemble les contributions d'un nombre record de 81 organisations. Le rapport 2020 est le fruit d'une analyse de 32 002 incidents de sécurité, dont 3 950 compromissions de données confirmées. Cette année, nous avons élargi nos analyses sectorielles à davantage d'industries, tout en présentant pour la première fois des statistiques par zone géographique.

Découvrez les principales conclusions du DBIR 2020, envoyez cette synthèse à vos collègues et téléchargez le rapport complet pour une vue plus détaillée des menaces qui vous concernent.

32 002

incidents de sécurité analysés, dont 3 950 compromissions de données confirmées

Des améliorations continues

L'équipe de rédaction du DBIR 2020 s'appuie sur la structure VERIS (Vocabulary for Event Recording and Incident Sharing) pour classifier et analyser les incidents et compromissions. Cette année, nos équipes ont également développé des mappings avec le framework MITRE ATT&CK® et le Center for Internet Security's Critical Security Controls (CIS CSC). Ces nouveaux points de référence nous ont permis d'optimiser nos analyses et de les mettre à la disposition de toute la communauté de la sécurité.

Synthèse des résultats

Figure 1. Qui sont les victimes ?

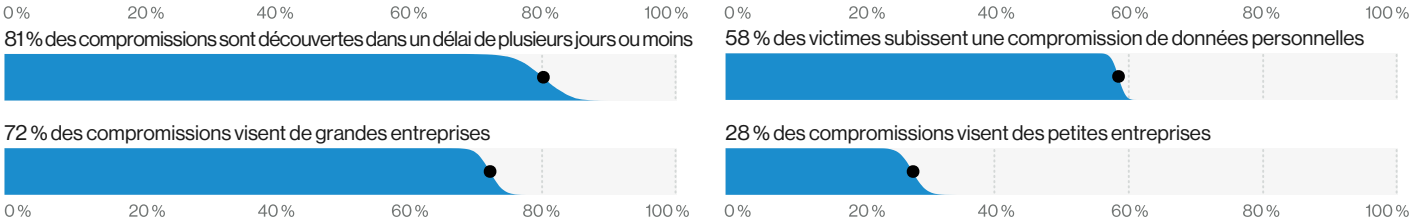


Figure 2. Qui sont les attaquants ?

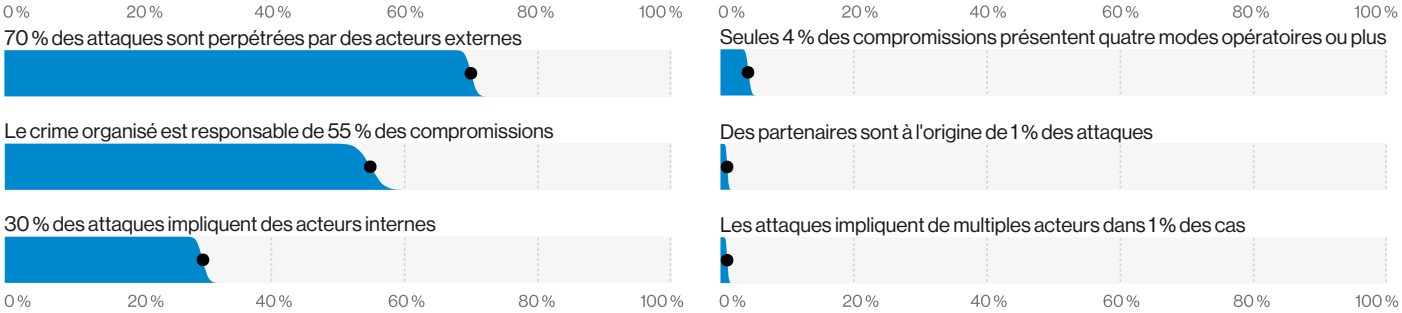
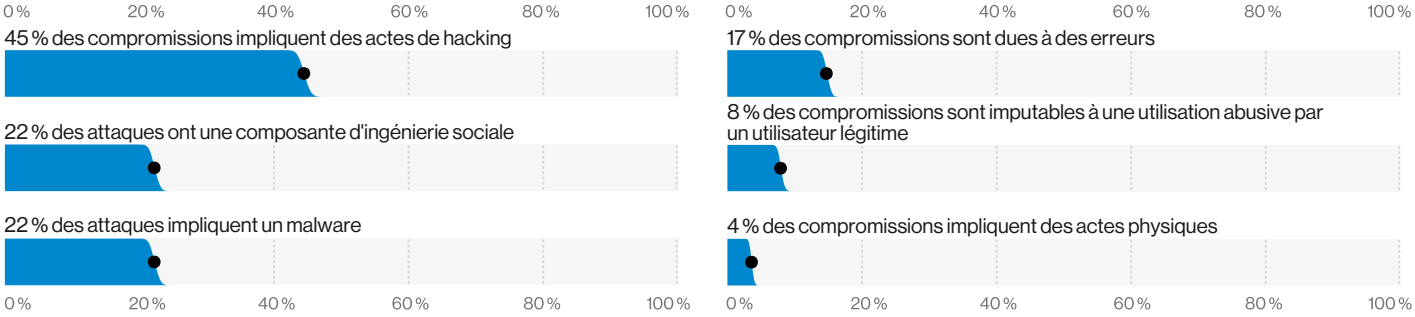


Figure 3. Quels sont les modes opératoires ?



À retenir

Mythes et réalité

L'ennemi est à l'extérieur

Beaucoup persistent à croire que la majorité des compromissions sont le fruit de collaborateurs internes mal intentionnés. Or, le DBIR démontre une fois de plus que la menace se situe principalement au niveau des acteurs externes. Ainsi, 70 % des compromissions analysées venaient de l'extérieur.

L'argent est la principale motivation

S'il fait souvent la une des médias, l'espionnage ne représente que 10 % des compromissions recensées dans notre étude. Dans la majorité des cas (86 %), les cybercriminels sont attirés par l'appât du gain. Les techniques avancées – qui elles aussi font le buzz – ne représentent quant à elles que 4 % des compromissions.

Profil des attaquants et de leurs méthodes

Les vieilles recettes ont toujours la cote

Le vol d'identifiants, les attaques par ingénierie sociale (phishing, compromission de messageries professionnelles, etc.) et les erreurs humaines sont à l'origine de la majorité des compromissions de données (67% ou plus). Tant que ces méthodes fonctionnent, les cyberattaquants n'ont aucune raison d'en changer. C'est pourquoi la plupart des entreprises devraient y consacrer l'essentiel de leurs efforts.

Les ransomwares sont partout

Les ransomwares représentent 27 % des incidents, et 18 % des sociétés étudiées ont bloqué au moins un ransomware au cours de l'année écoulée. Aucune entreprise ne peut se permettre d'ignorer ce type de menace.

Le piège des applications web

Les attaques d'applications web représentent actuellement 43 % de toutes les compromissions, soit le double de l'année dernière. À l'heure où les entreprises migrent leurs workflows vers les services cloud, les cyberattaquants leurs emboîtent tout naturellement le pas. Les méthodes de compromission les plus courantes des applications web sont d'une part l'utilisation d'identifiants volés ou obtenus par attaque de type brute force (plus de 80 %), et d'autre part l'exploitation de vulnérabilités (moins de 20 %), l'objectif étant d'accéder aux données sensibles que ces applications recèlent.

Les données personnelles en ligne de mire

On assiste à une augmentation des compromissions de données personnelles. Toutefois, cette hausse peut être due aux obligations de notification imposées par les réglementations en vigueur. Quoi qu'il en soit, 58 % des compromissions concernent des données personnelles, un pourcentage presque deux fois supérieur à celui de l'an passé. Au rang des données exposées, on compte les adresses e-mail, les noms, les numéros de téléphone, les adresses postales, mais aussi d'autres types de données contenues dans les e-mails ou stockées dans des bases de données mal configurées.

Faites ce que je dis, pas ce que je fais

Le DBIR 2020 fait état d'un nombre élevé de compromissions liées à des erreurs internes (881 contre 424 l'an passé). Si les erreurs humaines restent un vrai problème, cette évolution s'explique certainement davantage par le resserrement du cadre juridique et réglementaire, plutôt que par une multiplication des erreurs commises par des acteurs internes.

Des tendances encourageantes

Un blocage plus efficace

Les outils de sécurité sont de plus en plus efficaces face aux malwares les plus courants. Le DBIR 2020 montre ainsi qu'après un pic à pratiquement 50 % de la totalité des compromissions en 2016, les chevaux de Troie sont passés à tout juste 6,5 % cette année. Les droppers, backdoors et autres keyloggers représentent quant à eux 45 % des malwares, Un chiffre certes élevé mais qui ne doit pas masquer l'efficacité croissante de la lutte contre ce type de menaces.

Des correctifs bien appliqués

D'après le DBIR 2020, moins de 5 % des compromissions résultent de l'exploitation d'une vulnérabilité. Même constat du côté des Security Information and Event Management (SIEM) : seuls 2,5 % des cas relevés mettent en cause l'exploitation d'une vulnérabilité. De manière encourageante, les entreprises font preuve, dans l'ensemble, d'une bonne assiduité dans l'installation des correctifs. Pourvu que cela dure !

Mais cette efficacité ne doit pas les détourner d'un problème potentiellement grave : la mauvaise gestion des ressources. Dans la majorité des entreprises, les ressources connectées à Internet sont disséminées sur cinq réseaux, voire plus. Inévitablement, certaines finissent par ne jamais être corrigées, et c'est d'elles que vient le danger.

27 %

Les ransomwares représentent 27 % des incidents causés par des malwares.

Le vol d'identifiants, les erreurs et les attaques par ingénierie sociale sont les trois causes principales de compromissions. Les salariés en télétravail sont particulièrement exposés à ce type d'attaque. D'où l'intérêt de jouer la carte de la prévention en cette période d'incertitudes.

Gros plan par secteur

Quelle que soit sa taille ou son activité, aucune entreprise n'est à l'abri d'une cyberattaque. Ce qui varie en revanche, c'est le type de menaces qui pèsent sur elle. Pour renforcer vos défenses et optimiser votre budget de sécurité, vous devez avoir une vision à la fois globale et sectorielle des menaces qui vous concernent. Cette année, nous avons élargi notre périmètre d'étude à 16 secteurs d'activité, avec en prime une analyse des différences entre PME et grandes entreprises. Notre classification sectorielle repose sur les codes du Système de classification des industries de l'Amérique du Nord (SCIAN).

Hôtellerie et restauration (SCIAN 72)

Contrairement aux années précédentes, les compromissions des systèmes de points de vente ne représentent plus la majorité des incidents. Le secteur est en revanche confronté à plusieurs types de menaces assez équitablement réparties entre malwares, erreurs humaines et vols d'identifiants. L'intérêt des hackers pour l'hôtellerie et la restauration est dû en grande partie aux données des cartes de paiement dont ces établissements sont les dépositaires.

Volume	125 incidents, dont 92 compromissions de données confirmées
Principaux schémas	Les crimewares, les attaques d'applications web et l'infiltration des systèmes de points de vente représentent 61 % des compromissions de données.
Attaquants	Externes (79 %), internes (22 %), multiples (2 %), partenaires (1 %) (compromissions)
Motivations	Financières (98 %), secondaires (2 %) (compromissions)
Données compromises	Données de paiement (68 %), personnelles (44 %), identifiants (14 %), autres (10 %) (compromissions)
Principaux contrôles	Limitation et contrôle des ports, protocoles et services réseau (CSC 9), protection périmétrique (CSC 12), protection des données (CSC 13)

Arts, divertissements et loisirs (SCIAN 71)

Dans ces secteurs, les attaques d'applications web ont entraîné un nombre élevé de compromissions. De même, les attaques par déni de service (DoS) ont affiché un volume de bits par seconde supérieur à celui de la moyenne globale. L'ingénierie sociale et les erreurs humaine restent également monnaie courante.

Volume	194 incidents, dont 98 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 68 % des compromissions de données.
Attaquants	Externes (67 %), internes (33 %), multiples (1 %), partenaires (1 %) (compromissions)
Motivations	Financières (94 %), commodité (6 %) (compromissions)
Données compromises	Données personnelles (84 %), médicales (31 %), autres (26 %), de paiement (25 %) (compromissions)
Principaux contrôles	Protection périmétrique (CSC 12), sécurisation des configurations (CSC 5, CSC 11), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17)

BTP (SCIAN 23)

Ce secteur est en proie aux pratiques d'ingénierie sociale, aux attaques sur les applications web et aux vols d'identifiants. Signe encourageant, le BTP affiche un taux restreint de compromissions par phishing, de même qu'un nombre étonnamment faible d'erreurs humaines.

Volume	37 incidents, dont 25 compromissions de données confirmées
Principaux schémas	Les crimewares, les attaques d'applications web et tout ce qui n'entre pas dans les autres catégories représentent 95 % de tous les incidents.
Attaquants	Externes (95 %), internes (5 %) (incidents)
Motivations	Financières (84 à 100 %), représailles (0 à 16 %) (incidents)[1]
Données compromises	Données personnelles et identifiants
Principaux contrôles	Sécurisation des configurations (CSC 5, CSC 11), protection périmétrique (CSC 12), surveillance et contrôle des comptes (CSC 16)

Enseignement (SCIAN 61)

Le phishing est à l'origine de 28 % des compromissions de données, devant les accès non autorisés par vol d'identifiants (23 %). D'après nos observations, les ransomwares comptent pour environ 80 % des infections par malware dans cette branche. Peu enclins à signaler des attaques par phishing, les établissements d'enseignement perdent un temps précieux en cas de compromission.

Volume	819 incidents, dont 228 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 81 % des compromissions.
Attaquants	Externes (67 %), internes (33 %), multiples (1 %), partenaires (1 %) (compromissions)
Motivations	Financières (92 %), piratage récréatif (5 %), commodité (3 %), espionnage (3 %), secondaires (2 %) (compromissions)
Données compromises	Données personnelles (75 %), identifiants (30 %), autres (23 %), internes (13 %) (compromissions)
Principaux contrôles	Mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection périmétrique (CSC 12), sécurisation des configurations (CSC 5, CSC 11)

Finance et assurance (SCIAN 52)

Les attaques sont ici perpétrées par des acteurs extérieurs qui cherchent à détourner des données facilement monnayables (63 %), mais aussi des collaborateurs internes mus par un intérêt financier (18 %). Dans 9 % des cas, les compromissions sont liées à des erreurs humaines commises en interne. Ce secteur est également la cible d'attaques sur ses applications web au moyen d'identifiants volés. Du côté des compromissions d'origine interne, on observe un recul des actes de malveillance et une augmentation des erreurs bénignes, qui n'en présentent pas moins des risques pour les entreprises concernées.

Volume	1509 incidents, dont 448 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 81 % des compromissions.
Attaquants	Externes (64 %), internes (35 %), partenaires (2 %), multiples (1 %) (compromissions)
Motivations	Financières (91 %), espionnage (3 %), représailles (3 %) (compromissions)
Données compromises	Données personnelles (77 %), autres (35 %), identifiants (35 %), bancaires (32 %) (compromissions)
Principaux contrôles	Mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection périmétrique (CSC 12), sécurisation des configurations (CSC 5, CSC 11)

Santé (SCIAN 62)

Ce secteur reste une cible de choix pour les attaques par ransomware à visées financières. Les vols ou pertes d'appareils continuent également de poser problème, tandis que les erreurs humaines restent une plaie qui semble ne pas vouloir se refermer. Parmi elles, les erreurs de livraison arrivent en tête, tandis que les abus internes sont en baisse.

Volume	798 incidents, dont 521 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 72 % des compromissions.
Attaquants	Externes (51 %), internes (48 %), partenaires (2 %), multiples (1 %) (compromissions)
Motivations	Financières (88 %), piratage récréatif (4 %), commodité (3 %) (compromissions)
Données compromises	Données personnelles (77 %), médicales (67 %), autres (18 %), identifiants (18 %) (compromissions)
Principaux contrôles	Mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection périmétrique (CSC 12), protection des données (CSC 13)

Information (SCIAN 51)

Les attaques par applications web par exploitation de vulnérabilités et utilisation d'identifiants volés sont les menaces les plus répandues dans ce secteur. Les erreurs – mauvaise configuration des bases de données cloud en tête – restent une problématique courante. Enfin, le secteur de l'information est de plus en plus souvent la cible d'attaques DoS.

Volume	5 741 incidents, dont 360 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 88 % des compromissions de données.
Attaquants	Externes (67 %), internes (34 %), multiples (2 %), partenaires (1 %) (compromissions)
Motivations	Financières (88 %), espionnage (7 %), piratage récréatif (2 %), représailles (2 %), autres (1 %) (compromissions)
Données compromises	Données personnelles (69 %), identifiants (41 %), autres (34 %), internes (16 %) (compromissions)
Principaux contrôles	Sécurisation des configurations (CSC 5, CSC 11), gestion continue des vulnérabilités (CSC 3), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17)

Industrie (SCIAN 31-33)

Les industriels sont généralement exposés aux attaques d'acteurs externes. Pour pirater les systèmes et faire main basse sur des données, ceux-ci recourent à des malwares de récupération de mots de passe et au vol d'identifiants. Si les motivations restent avant tout financières, le cyber-espionnage est également à prendre en considération. Enfin, l'utilisation abusive des droits d'accès en interne représente aussi une source de préoccupation.

Volume	922 incidents, dont 381 compromissions de données confirmées
Principaux schémas	Les crimewares, les attaques d'applications web et l'abus de privilège représentent 64 % des compromissions de données.
Attaquants	Externes (75 %), internes (25 %), partenaires (1 %) (compromissions)
Motivations	Financières (73 %), espionnage (27 %) (compromissions)
Données compromises	Identifiants (55 %), données personnelles (49 %), autres (25 %), données de paiement (20 %) (compromissions)
Principaux contrôles	Protection périmétrique (CSC 12), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection des données (CSC 13)

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

Si la répartition des attaques est relativement équilibrée dans ces secteurs, on observe cependant une certaine prédominance de l'ingénierie sociale, notamment le phishing et l'imposture (malgré l'absence de données confirmées). Le cyber-espionnage et les atteintes aux technologies opérationnelles (OT) sont également des sujets d'inquiétude sérieux dans ces secteurs.

Volume	194 incidents, dont 43 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, le cyber-espionnage et tout ce qui n'entre pas dans les autres catégories représentent 74 % des compromissions.
Attaquants	Externes (75 %), internes (28 %), multiples (2 %) (compromissions)
Motivations	Financières (63 à 95 %), espionnage (8 à 43 %), commodité/autres/secondaires (0 à 17 % chacun), intimidation/piratage récréatif/représailles/idéologiques (0 à 9 % chacun) (compromissions)[1]
Données compromises	Identifiants (41 %), données personnelles (41 %), autres (35 %), internes (19 %) (compromissions)
Principaux contrôles	Sécurisation des configurations (CSC 5, CSC 11), protection périmétrique (CSC 12), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17)

Autres services (SCIAN 81)

Les autres services comprennent des activités n'entrant dans aucune des autres catégories (services à la personne, réparation, monde associatif, etc.). Dans ce secteur très pluriel, l'appât du gain domine chez les attaquants. Côté vecteurs d'attaque, les applications web comptent pour 39 % des compromissions. Les erreurs des salariés représentent également une menace bien réelle, particulièrement les erreurs de configuration ou de livraison. Enfin, si le vol d'identifiants reste très présent, les cybercriminels s'intéressent surtout aux données personnelles dans ces secteurs.

Volume	107 incidents, dont 66 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 83 % des compromissions.
Attaquants	Externes (68 %), internes (33 %), multiples (2 %) (compromissions)
Motivations	Financières (60 à 98 %), espionnage (0 à 28 %), commodité/intimidation/piratage récréatif/représailles/autres/secondaires (0 à 15 % chacun) (compromissions)[1]
Données compromises	Données personnelles (81 %), autres (42 %), identifiants (36 %), internes (25 %) (compromissions)
Principaux contrôles	Protection périmétrique (CSC 12), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), sécurisation des configurations (CSC 5, CSC 11)

Services professionnels, techniques et scientifiques (SCIAN 54)

Dans ces branches du tertiaire, les cybercriminels privilégient les vols d'identifiants pour compromettre des applications web dans un but purement financier. L'ingénierie sociale (campagne de phishing, usurpation d'identité, etc.) fait également partie des méthodes répandues pour accéder aux données. Enfin, les acteurs de ces services sont victimes d'attaques DoS régulières.

Volume	7 463 incidents, dont 326 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs en tous genres et tout ce qui n'entre pas dans les autres catégories représentent 79 % des compromissions.
Attaquants	Externes (75 %), internes (22 %), partenaires (3 %), multiples (1 %) (compromissions)
Motivations	Financières (93 %), espionnage (8 %), idéologique (1 %) (compromissions)
Données compromises	Données personnelles (75 %), identifiants (45 %), autres (32 %), internes (27 %) (compromissions)
Principaux contrôles	Sécurisation des configurations (CSC 5, CSC 11), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection périmétrique (CSC 12)

Service public (SCIAN 92)

Le ransomware représente un danger omniprésent pour toutes sortes d'administrations. Les erreurs de livraison et de configuration constituent une autre menace importante.

Volume	6 843 incidents, dont 346 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 73 % des compromissions.
Attaquants	Externes (59 %), internes (43 %), multiples (2 %), partenaires (1 %) (compromissions)
Motivations	Financières (75 %), espionnage (19 %), piratage récréatif (3 %) (compromissions)
Données compromises	Données personnelles (51 %), autres (34 %), identifiants (33 %), internes (14 %) (compromissions)
Principaux contrôles	Mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection périmétrique (CSC 12), sécurisation des configurations (CSC 5, CSC 11)

Immobilier (achat, vente, location) (SCIAN 53)

Les compromissions d'applications web au moyen d'identifiants volés sont particulièrement fréquentes. Autres dangers majeurs : les attaques par ingénierie sociale caractérisées par une intrusion dans les processus de transfert de biens et une tentative de détournement de fonds vers des comptes bancaires détenus par les hackers. Enfin, ici aussi, les erreurs de configuration entraînent de nombreuses compromissions.

Volume	37 incidents, dont 33 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 88 % des compromissions de données.
Attaquants	Externes (73 %), internes (27 %) (compromissions)
Motivations	Financières (45 à 97 %), commodité/espionnage (0 à 40 % chacun), intimidation/piratage récréatif/représailles/idéologiques/autres/secondaires (0 à 21 % chacun) (compromissions)[1]
Données compromises	Données personnelles (83 %), internes (43 %), autres (43 %), identifiants (40 %) (compromissions)
Principaux contrôles	Sécurisation des configurations (CSC 5, CSC 11), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), protection périmétrique (CSC 12)

Retail (SCIAN 44-45)

Les attaques contre les applications e-commerce demeurent le fléau numéro 1. À l'heure où les acteurs du retail migrent leurs opérations sur le web, les cybercriminels n'ont pas tardé les suivre. Conséquence logique, les intrusions sur les systèmes de points de vente, autrefois prédominantes, restent à un niveau faible, semblable à celui de l'an passé. Si les données de paiement sont généralement prisées des cybercriminels, ces derniers montrent également un très vif intérêt pour les identifiants et données personnelles.

Volume	287 incidents, dont 146 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 72 % des compromissions.
Attaquants	Externes (75 %), internes (25 %), partenaires (1 %), multiples (1 %) (compromissions)
Motivations	Financières (99 %), espionnage (1 %) (compromissions)
Données compromises	Données personnelles (49 %), de paiement (47 %), identifiants (27 %), autres (25 %) (compromissions)
Principaux contrôles	Protection périmétrique (CSC 12), sécurisation des configurations (CSC 5, CSC 11), gestion continue des vulnérabilités (CSC 3)

Transport et logistique (SCIAN 48-49)

Ces entreprises sont exposées aux attaques via des applications web, généralement perpétrées par des organisations criminelles attirées par l'appât du gain. Les erreurs des salariés, notamment le manque de contrôle de bases de données volumineuses, représentent un autre danger. Ajoutez à cela l'ingénierie sociale (attaques par phishing, usurpation d'identité, etc.), et vous obtenez le tableau des attaques à l'origine de la majorité des compromissions.

Volume	112 incidents, dont 67 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 69 % des compromissions.
Attaquants	Externes (68 %), internes (32 %) (compromissions)
Motivations	Financières (74 à 98 %), espionnage (1 à 21 %), commodité (0 à 15 %) (compromissions)[1]
Données compromises	Données personnelles (64 %), identifiants (34 %), autres (23 %) (compromissions)
Principaux contrôles	Protection périmétrique (CSC 12), mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17), sécurisation des configurations (CSC 5, CSC 11)

Zoom sur les PME

En dépit de la persistance de certaines différences liées à la taille des entreprises, la transition vers le cloud et sa myriade d'outils web, mais aussi la hausse continue des attaques par ingénierie sociale, ont estompé la frontière entre PME, ETI et grands groupes. L'ajustement des business models des PME a incité les cybercriminels à s'adapter et repenser leurs actions pour parvenir plus rapidement et facilement à leurs fins.

	Petite et moyenne (moins de 1 000 salariés)	Grande (plus de 1 000 salariés)
Volume	407 incidents, dont 221 compromissions de données confirmées	8 666 incidents, dont 576 compromissions de données confirmées
Principaux schémas	Les attaques d'applications web, les erreurs diverses et tout ce qui n'entre pas dans les autres catégories représentent 70 % des compromissions.	Les crimewares, l'abus de privilège et tout ce qui n'entre pas dans les autres catégories représentent 70 % des compromissions de données.
Attaquants	Externes (74 %), internes (26 %), partenaires (1 %), multiples (1 %) (compromissions)	Externes (79 %), internes (21 %), partenaires (1 %), multiples (1 %) (compromissions)
Motivations	Financières (83 %), espionnage (8 %), piratage récréatif (3 %), représailles (3 %) (compromissions)	Financières (79 %), espionnage (14 %), piratage récréatif (2 %), représailles (2 %) (compromissions)
Données compromises	Identifiants (52 %), données personnelles (30 %), autres (20 %), internes (14 %), médicales (14 %) (compromissions)	Identifiants (64 %), autres (26 %), données personnelles (19 %), internes (12 %) (compromissions)

Résultats par région

Pour la première fois cette année, le DBIR offre une présentation des statistiques par région du globe.

Figure 4. Amérique du Nord

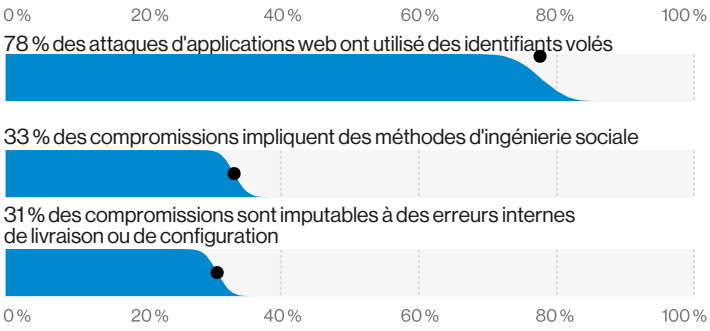


Figure 5. Europe, Moyen-Orient et Afrique

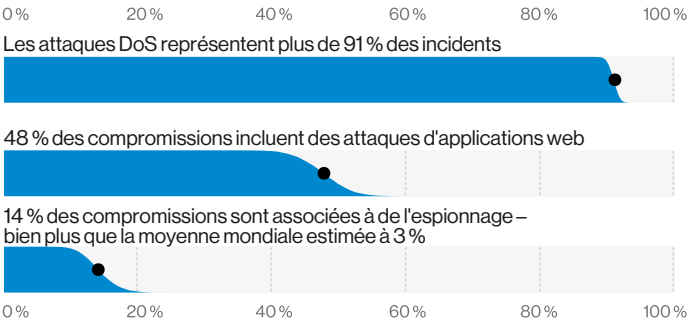


Figure 6. Asie-Pacifique

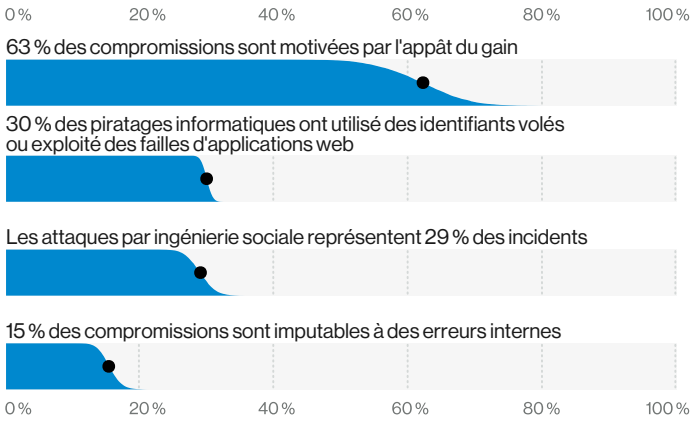
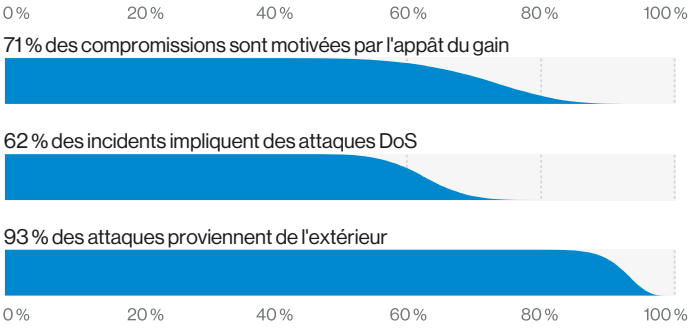


Figure 7. Amérique latine et Caraïbes



Bonnes pratiques

Cette année, 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.

Gestion continue des vulnérabilités (CSC 3)

Utilisez cette méthode pour détecter et corriger les vulnérabilités du code et les erreurs de configuration.

Sécurisation des configurations (CSC 5, CSC 11)

Vérifiez que vos systèmes sont configurés de manière à n'accéder qu'aux services strictement nécessaires.

Protection des messageries électroniques et navigateurs web (CSC 7)

Verrouillez les clients e-mail et navigateurs afin de réduire les risques d'attaques face à la jungle d'Internet.

Limitation et contrôle des ports, protocoles et services réseau (CSC 9)

Après en avoir défini l'étendue, limitez l'accès aux seuls services et ports nécessaires.

Protection périmétrique (CSC 12)

Outre le déploiement de pare-feu, pensez à utiliser des dispositifs de surveillance du réseau, des proxys et une authentification multifacteur.

Protection des données (CSC 13)

Contrôlez l'accès aux informations sensibles à travers leur inventaire, leur chiffrement et la restriction des accès aux seuls fournisseurs cloud et e-mail autorisés.

Surveillance des comptes (CSC 16)

Verrouillez les comptes utilisateurs dans toute l'entreprise afin d'empêcher l'utilisation d'identifiants volés. Envisagez l'utilisation d'une authentification multifacteur.

Mise en place d'un programme de sensibilisation et de formation à la sécurité (CSC 17)

Sensibilisez vos utilisateurs aux cybermenaces et aux compromissions accidentelles.

S'informer, c'est se préparer.

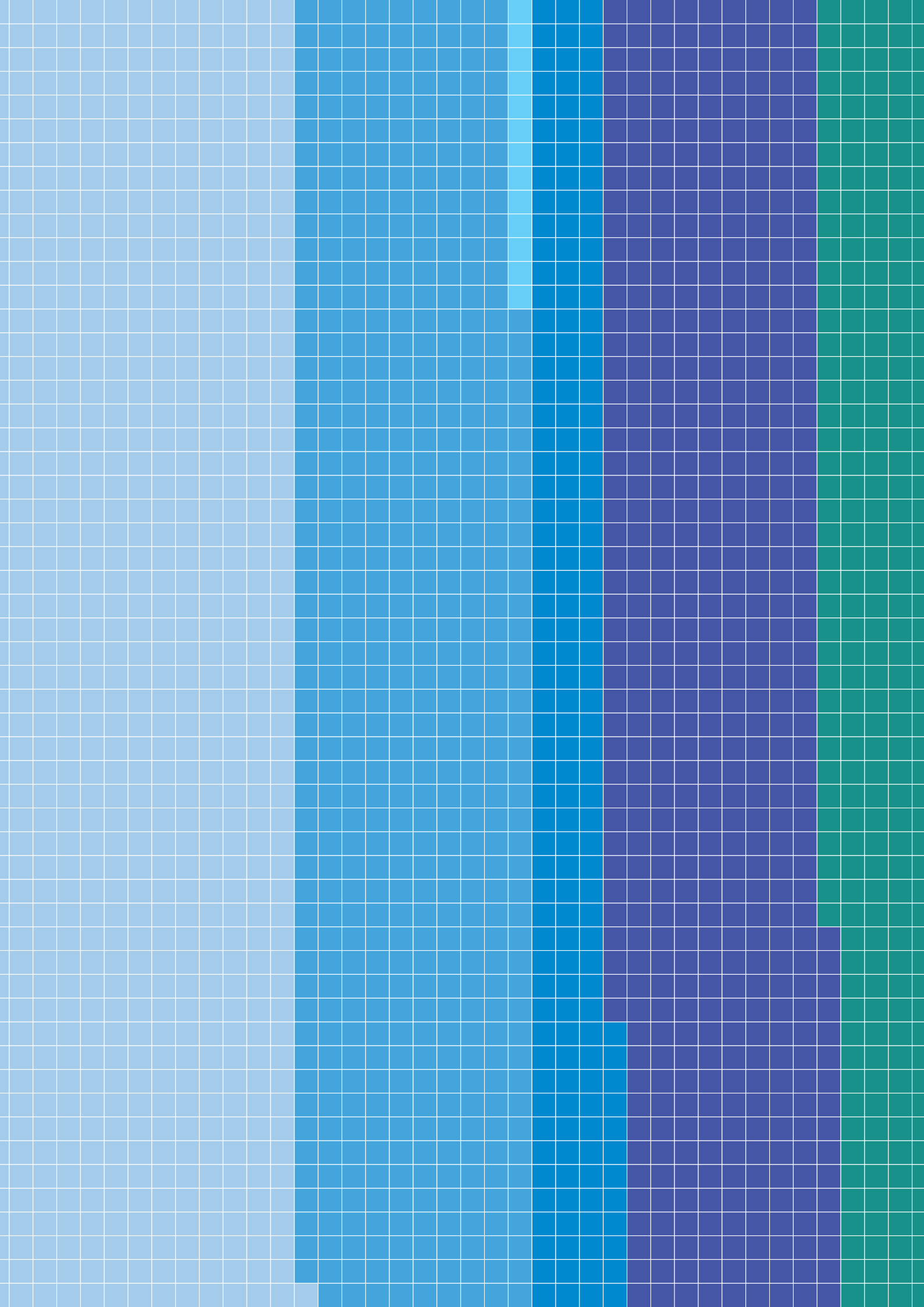
Pour faire face aux menaces actuelles, vous devez pouvoir compter sur une information fiable. Le rapport DBIR vous présente les acteurs, tendances et modes opératoires qui pèsent sur votre activité pour vous aider à mieux vous protéger et sensibiliser vos utilisateurs.

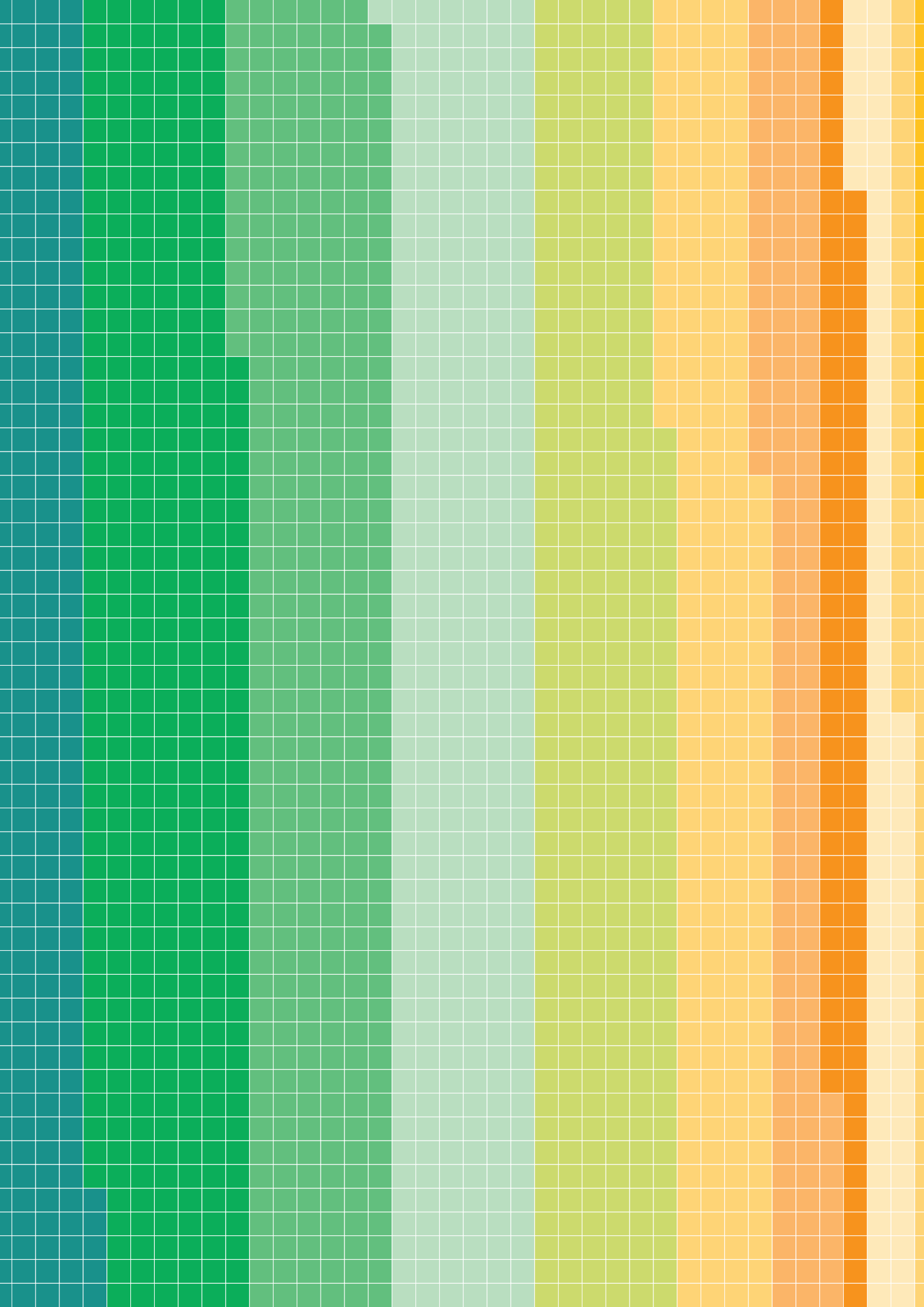
Lisez le rapport DBIR 2020 complet sur https://enterprise.verizon.com/fr-fr/resources/reports/dbir

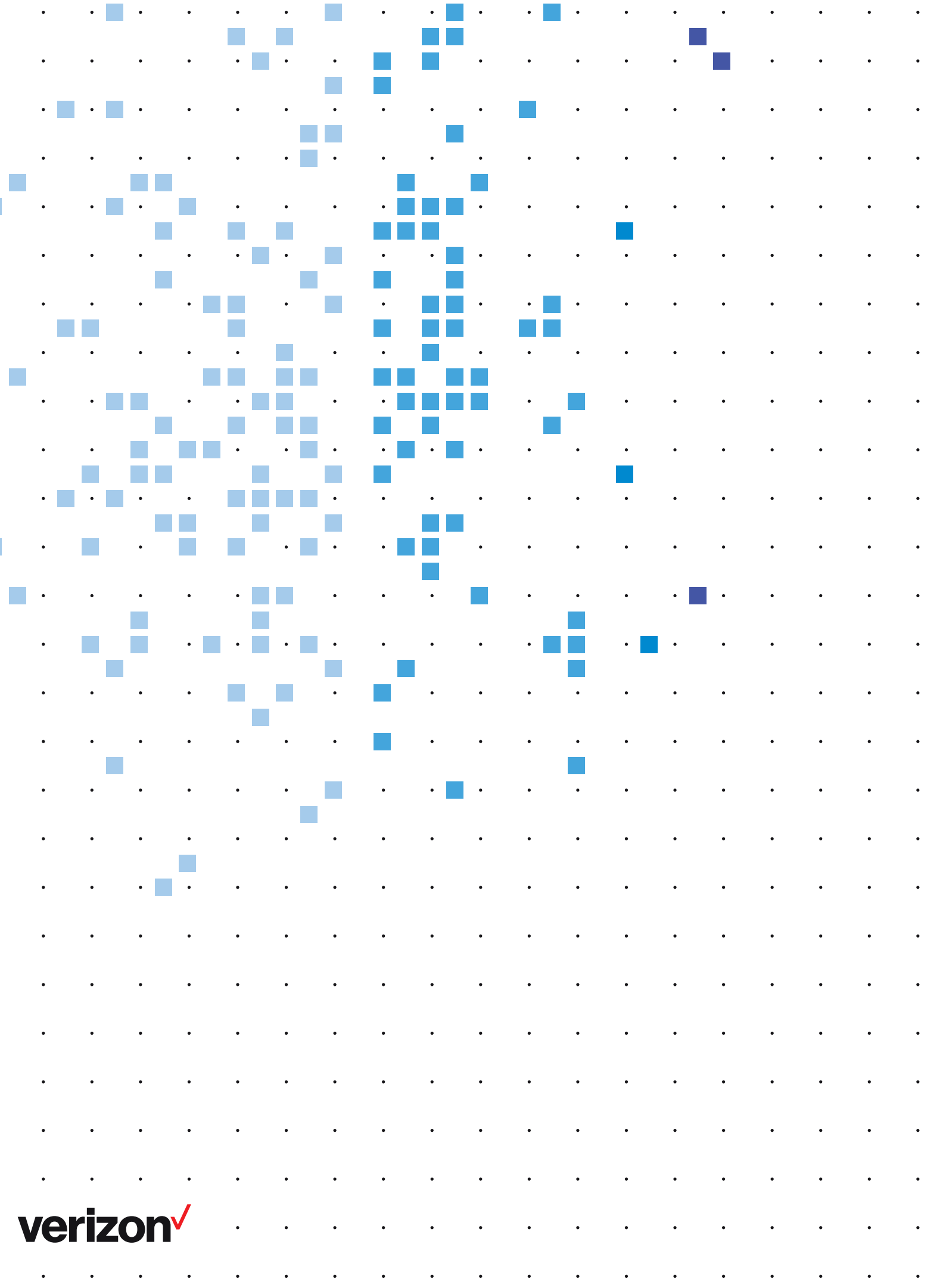
Vous aussi, vous voulez œuvrer pour un monde digital plus sûr ?

Le DBIR s'appuie sur la contribution de dizaines d'entreprises. Pourquoi ne pas apporter votre pierre à l'édifice ? Apportez votre contribution au rapport 2021 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.

1 Étant donné le faible volume d'échantillon, nous indiquons ici une fourchette de pourcentages pour refléter la marge de variabilité dans cette catégorie. Pour en savoir plus, lisez le rapport complet.






verizon