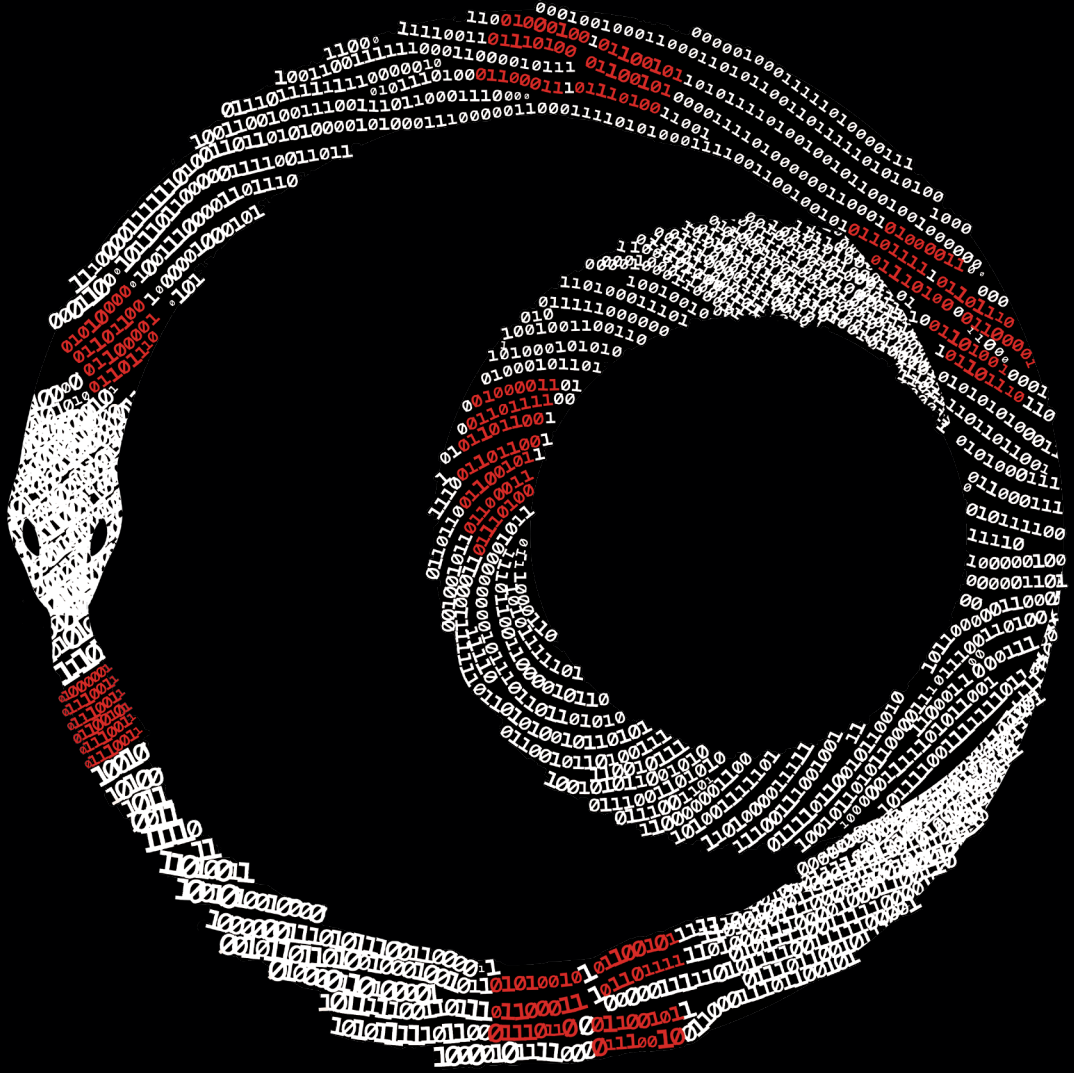
Document de synthèse

Rapport de préparation et de réponse à incident

Compromissions de données : comment ne pas tomber dans la spirale infernale !



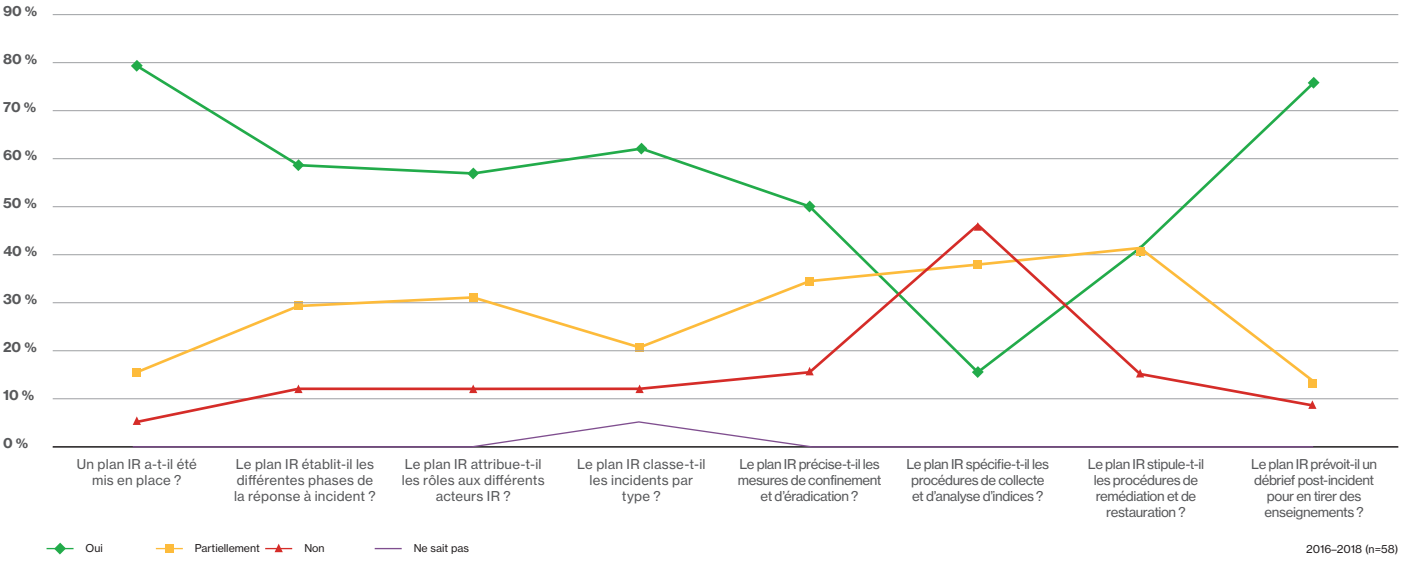
verizon

Réunion de crise

Bien se préparer et surtout bien répondre aux compromissions de données et autres incidents de sécurité n'est jamais chose facile. Il faut d'abord connaître son environnement et les menaces auxquelles il est exposé, il faut ensuite une collaboration efficace entre les équipes, et il faut enfin un plan de réponse à incident (IR, Incident Response) bien rodé.

C'est dans cette optique que nous avons rédigé ce rapport de préparation et de réponse à incident, ou VIPR (Verizon Incident Preparedness and Response). Basé sur des données et des scénarios concrets, il synthétise trois années (2016–2018) d'évaluations de plans IR et de simulations de compromission de données effectuées pour nos clients.

Évaluations de plan IR
Phases 1 à 6 : sélection des éléments d'un plan IR



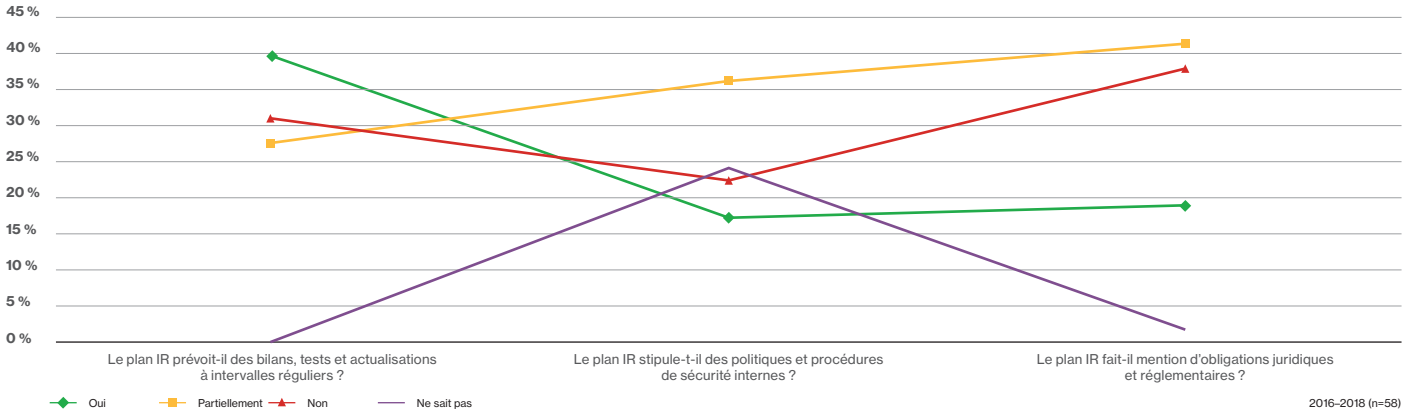
Cette nouvelle édition du rapport VIPR vous invite à vous mettre dans la peau des différents acteurs d'un plan IR pour vous aider à améliorer vos propres procédures de réponse à incident.

Le document s'articule autour de cinq scénarios de compromission de données (voir la partie Utilisation des kits de simulation d'incident), chacun correspondant à une phase déterminée d'un plan IR et des éléments qui la composent. Ce modèle pourra vous servir de matrice pour élaborer ou mettre à jour votre propre plan IR et ses guides de réponse à incident. Les scénarios développés pourront également étoffer vos contenus pour organiser vos exercices de simulation et autres « grandes manœuvres ».

Planification et préparation

Une réponse à incident efficace passe par une bonne planification et une bonne préparation. Cette phase porte sur la construction du plan IR, notamment l'attribution des rôles en interne, la désignation des intervenants de première ligne et l'identification des différents acteurs externes (prestataires de services, autorités de régulation et consultants).

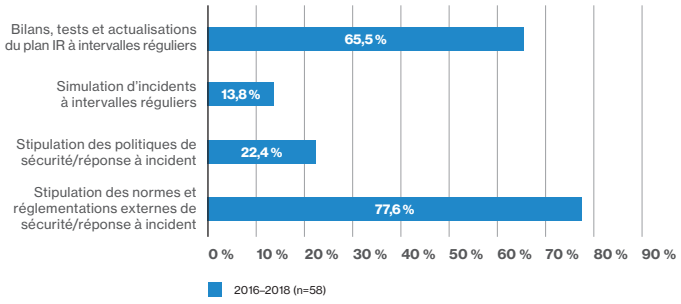
Évaluations de plan IR
Phase 1 : adéquation du plan



Résultats d'évaluation

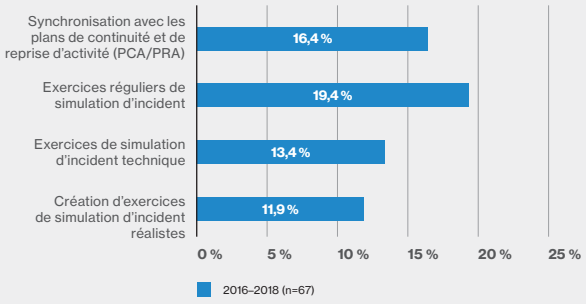
Seuls 40 % des plans IR évalués entre 2016 et 2018 prévoient explicitement des bilans, tests et actualisations à intervalles réguliers, tandis que 31 % n'en parlent même pas. Parmi les plans IR évalués, 22 % ne se réfèrent à aucune politique ou procédure de sécurité interne (30 % partiellement), tandis que 38 % ne font mention d'aucune obligation juridique ou réglementaire (41 % partiellement) relevant du domaine de la cybersécurité, de la réponse à incident ou de la notification des autorités de contrôle en cas d'incident.

Recommandations post-évaluation



En première place des recommandations figure la référence aux normes et règlementations externes, telles que le RGPD, ISO 27001, etc., (78 %), devant les bilans, tests et actualisations périodiques du plan IR (66 %).

Recommandations de simulation



Les recommandations de simulation émises entre 2016 et 2018 préconisent majoritairement la réalisation de simulations d'incident (20 %) et de simulations d'incident technique (13 %).

Détection et validation

Plus un incident de cybersécurité est détecté tôt, plus la réponse est efficace.

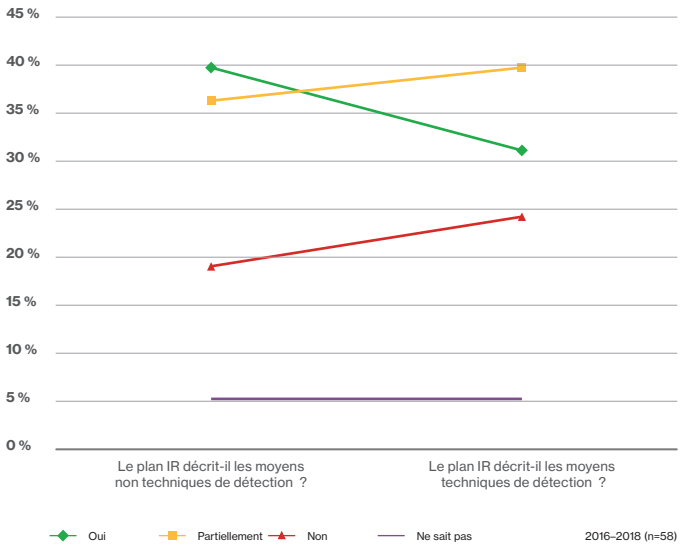
Résultats d'évaluation

Concernant les moyens de détection d'incident (2016–2018), 40 % des plans IR évalués décrivent en intégralité (36 % partiellement) les moyens de détection non techniques, contre seulement 31 % (40 % partiellement) pour les moyens de détection techniques.

Recommandations post-évaluation

Décrivez les moyens techniques et non techniques de détection d'incidents.

Évaluations de plan IR
Phase 2 : moyens de détection



Confinement et éradication

Cette phase évalue les mesures de confinement des menaces de cybersécurité pour limiter le préjudice, ainsi que les mesures d'éradication pour éviter toute récidive ou aggravation.

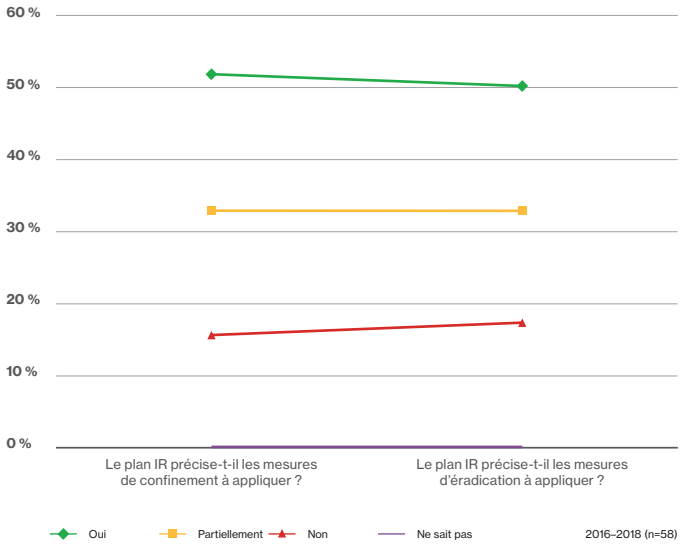
Résultats d'évaluation

Parmi les plans IR évalués entre 2016 et 2018, 52 % détaillent intégralement les mesures de confinement et 50 % les mesures d'éradication. Les mesures de confinement sont partiellement spécifiées dans 33 % des plans, soit exactement le même pourcentage que les mesures d'éradication.

Recommandations post-évaluation

Spécifiez des mesures de confinement et d'éradication.

Évaluations de plan IR
Phase 3 : confinement et éradication



Collecte et analyse

Quand un incident se produit, les indices récoltés permettent d'accélérer les phases de confinement, éradication, remédiation et restauration.

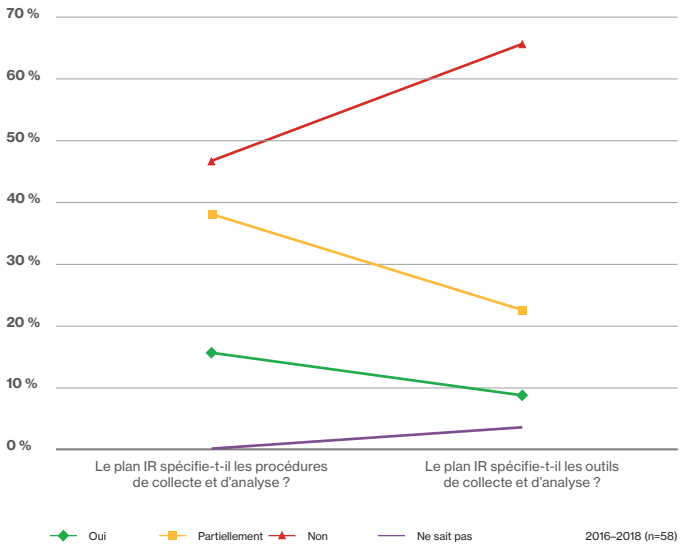
Résultats d'évaluation

En matière de collecte d'indices et d'analyse de données, seuls 16 % des plans IR évalués entre 2016 et 2018 décrivent intégralement les procédures à appliquer, contre 38 % partiellement. Côté pratiques, seuls 9 % spécifient la totalité des outils de collecte et d'analyse, tandis que 22 % ne dresse qu'une nomenclature partielle.

Recommandations post-évaluation

Spécifiez les outils et procédures de collecte d'indices et d'analyse de données.

Évaluations de plan IR
Phase 4 : collecte et analyse



Remédiation et restauration

Cette phase vise deux objectifs : 1) éliminer les vulnérabilités exposées pendant l'incident pour éviter toute récidive, et 2) organiser le retour à la normale.

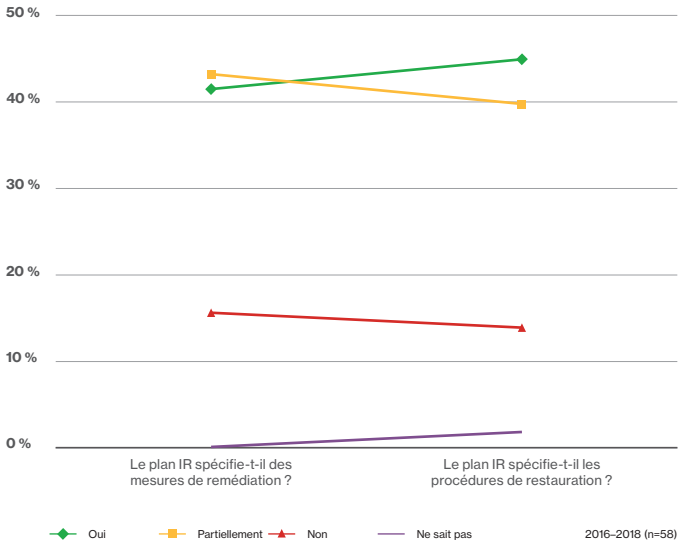
Résultats d'évaluation

Parmi les plans IR évalués entre 2016 et 2018, seuls 41 % spécifient la totalité des mesures de remédiation, contre 43 % partiellement. Concernant les mesures de restauration, ce rapport s'établit à 45 % contre 40 %.

Recommandations post-évaluation

Précisez les mesures de remédiation et de restauration.

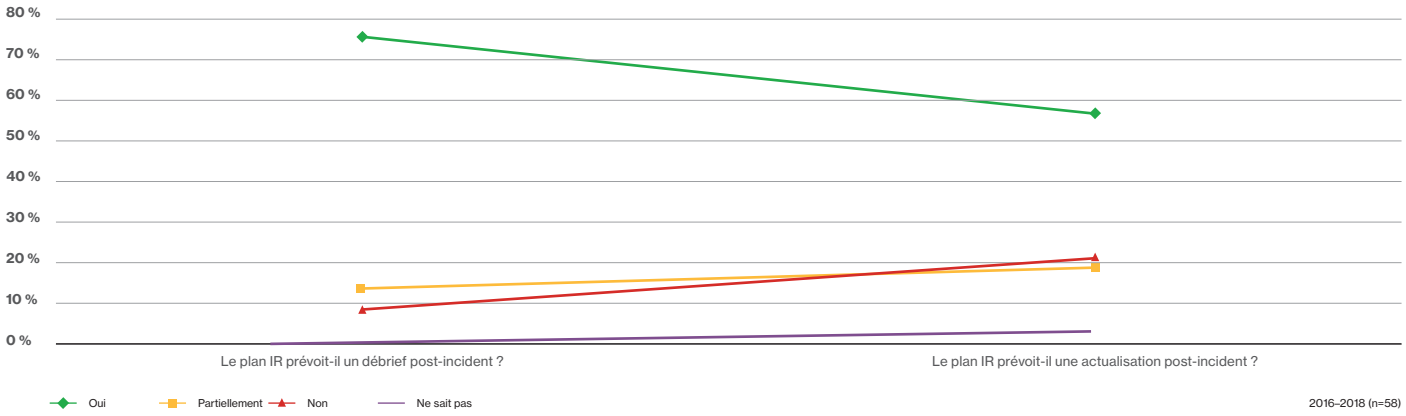
Évaluations de plan IR
Phase 5 : remédiation et restauration



Évaluation et ajustement

La phase finale du processus consiste à dresser un bilan des activités IR de façon à identifier les faiblesses et défauts systémiques, l'objectif étant d'améliorer les contrôles et les pratiques de cybersécurité.

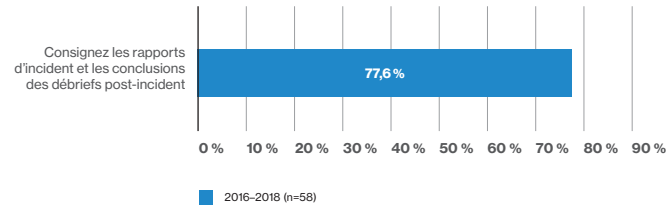
Évaluations de plan IR
Phase 6 : leçons à tirer



Résultats d'évaluation

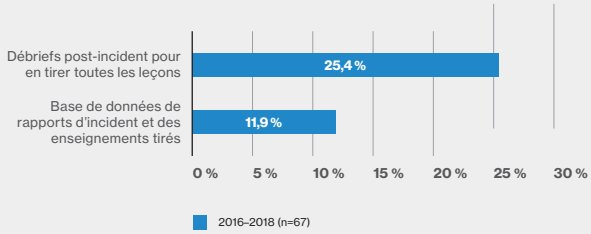
Parmi les plans IR évalués entre 2016 et 2018, 76 % font une description exhaustive (14 % partielle) des débriefs à tenir pour tirer les leçons des incidents. Côté mise à jour, 60 % prescrivent explicitement une actualisation du plan IR post-débrief (19 % partiellement).

Recommandations post-évaluation



Dans cette phase, les recommandations post-évaluation portent à 78 % sur la consignation des conclusions des débriefs post-incident.

Recommandations de simulation



Côté simulations d'incident entre 2016 et 2018, la tenue de débriefs post-incident arrive en tête des recommandations avec 25 %, devant la consignation des rapports d'incident et des enseignements tirés (12 %).

À retenir

Nous vous invitons à lire l'intégralité du rapport VIPR 2019, véritable mine d'informations, d'analyses et de conseils pour élaborer votre plan IR. En attendant, voici un récapitulatif des 20 grandes leçons à retenir pour mettre en place un plan de réponse à incident fiable et efficace.

Phase	À retenir
1 : Planification et préparation	1. Créez un plan IR logique et efficace 2. Rédigez des guides d'intervention par type d'incident 3. Effectuez régulièrement des bilans, tests et actualisations de votre plan IR 4. Stipulez les standards et bonnes pratiques internes et externes de cybersécurité et réponse à incident 5. Définissez les rôles et responsabilités des acteurs IR internes 6. Réunissez régulièrement les acteurs IR internes pour faire le point sur l'état actuel de la menace 7. Formez et développez les compétences des intervenants de première ligne 8. Réévaluez régulièrement les prestataires de cybersécurité externes et les procédures de contact
2 : Détection et validation	9. Définissez ce qui constitue un événement de cybersécurité (idem pour les incidents) 10. Classifiez les incidents par type et par degré de gravité 11. Décrivez les moyens de détection d'incidents techniques et non techniques 12. Précisez les mécanismes de suivi des incidents et des événements 13. Spécifiez les procédures d'escalade et de notification
3 : Confinement	14. Formulez des mesures de confinement et d'éradication
4 : Collecte et analyse	15. Spécifiez les outils et procédures de collecte d'indices et d'analyse de données 16. Détaillez les procédures de traitement et d'envoi des indices
5 : Remédiation et restauration	17. Précisez les mesures de remédiation et de restauration
6 : Évaluation et ajustement	18. Organisez des débriefs post-incidents (et incorporez les enseignements tirés au plan IR) 19. Établissez une politique de rétention des données et des documents 20. Effectuez un suivi des métriques de réponse à incident

Ressources consacrées à la cybersécurité et aux compromissions de données

https://enterprise.verizon.com/resources/

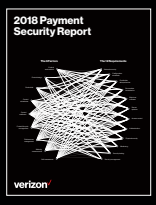
Rapport 2019 de préparation et de réponse à incident Compromissions de données : comment ne pas tomber dans la spirale infernale !

Rapport d'enquête 2019 sur les compromissions de données

Rapport 2019 sur les menaces internes : La sécurité pour tous les utilisateurs, même à distance

Mobile Security Index 2019 : Il est temps de s'attaquer à la sécurité mobile.

Data Breach Digest 2018 (18 scénarios)



Rapport 2018 sur la sécurité des paiements

Sécurité du cloud – Le guide du RSSI 2019 : principes à connaître et questions à poser avant d'acheter

Évaluation d'une plateforme de sécurité d'entreprise : les 5 critères à prendre en compte

Téléchargez le rapport Verizon de préparation et de réponse à incident

enterprise.verizon.com/resources/reports/vipr/

verizon