Tendances en matière de cybersécurité au Canada

Concilier la stratégie, la technologie,
l'intelligence artificielle et l'expertise humaine

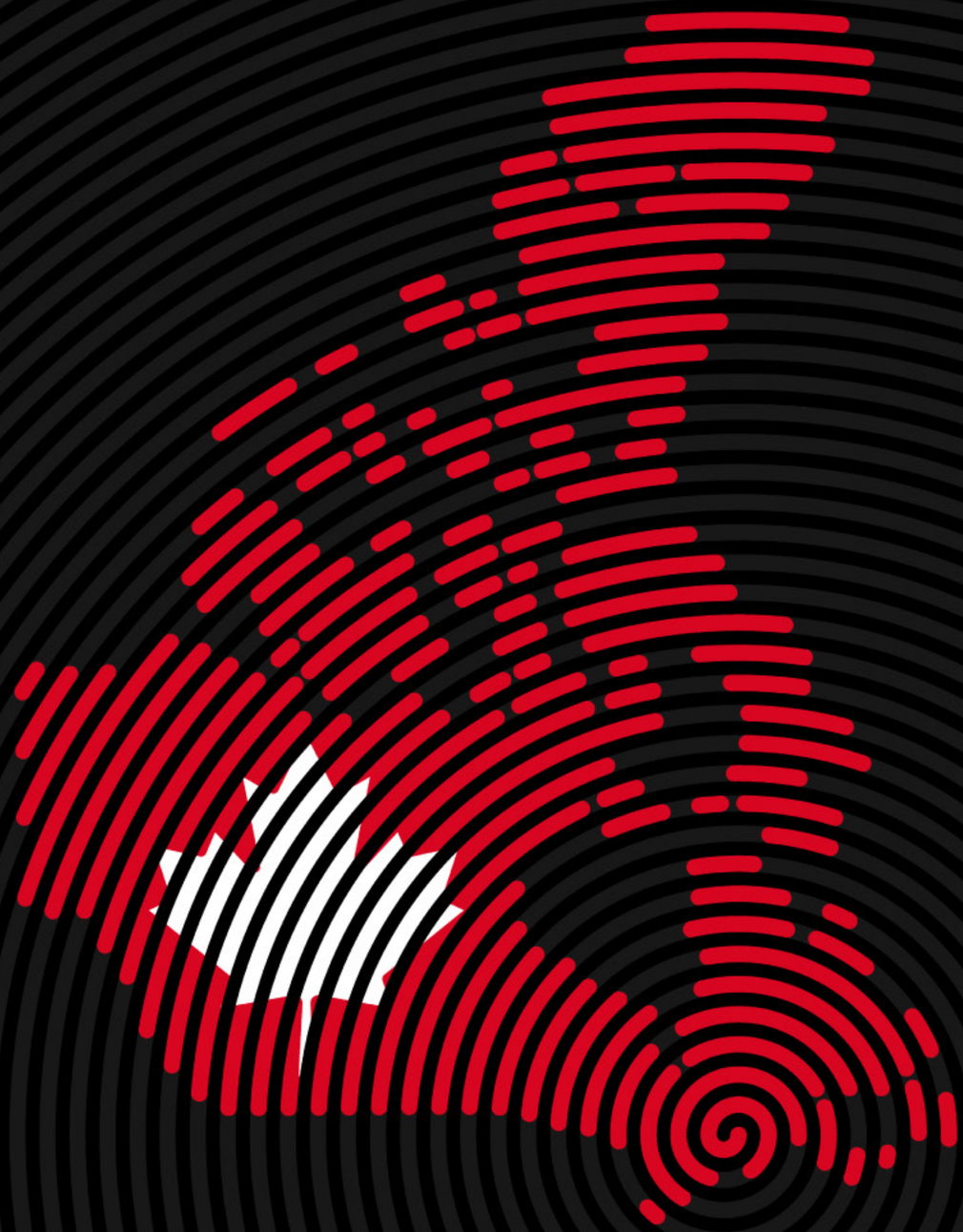


Table des matières

À propos de cette étude 3

- Segmentation de la taille des organisations

Les menaces pour le Canada 4

- La surface d'attaque dynamique
- Cyberattaques, incidents et temps d'indisponibilité
- Nombre moyen de cyberattaques par taille d'organisation
- Taux d'infection par catégorie de cyberincidents
- Taux de succès des cyberattaques
- Temps d'indisponibilité et temps d'indisponibilité par incident

Maturité des programmes de cybersécurité canadiens 11

- Définition des groupes de maturité

Principales constatations 13

- L'adoption de l'IA générative prend du retard
- Les tests de sécurité sont rentables
- Amélioration de la détection et de la réponse aux incidents
- Les défis du modèle à vérification systématique : entre théorie et pratique
- Prévenir les atteintes à la sécurité et accélérer les réponses

Recommandations 38

- Vérification systématique, aucune excuse : transformer la stratégie en action
- Tests d'intrusion : se protéger en continu de manière proactive
- Du chaos à l'ordre : comment les programmes de sécurité matures facilitent l'IA
- L'avantage des services de détection et de réponse gérées (DRG) : une détection plus rapide, une réponse plus intelligente, une sécurité améliorée

Annexe A : Résultats détaillés de l'étude 43

À propos de cette étude

Ces dernières années, le monde des TI a connu des périodes de croissance et de régression qui reflètent sa nature dynamique. Notre étude a analysé spécifiquement la croissance des points terminaux d'utilisateurs (ordinateurs, ordinateurs portatifs, téléphones intelligents et tablettes), des serveurs et des appareils d'Internet des objets (IdO) au fil du temps afin de montrer que la surface d'attaque de TI des organisations est en expansion continue.

Ce rapport présente les résultats de « L'étude Cybersécurité au Canada 2025 » de CDW. Les données contenues dans cette étude ont été obtenues dans le cadre d'une enquête pancanadienne, interprofessionnelle et interprovinciale menée par IDC Canada auprès de 704 professionnels spécialisés dans la sécurité informatique ainsi que dans les risques et la conformité. Tous les participants à l'étude ont fait l'objet d'une sélection pour leur contribution directe à l'amélioration ou à la gestion de la sécurité informatique de leur organisation. Un tri parmi les répondants a permis d'assurer une représentation des organisations d'au moins 15 employés à temps plein, dont au moins 10 % des employés se trouvaient au Canada. L'étude a été menée de novembre à décembre 2024 par IDC Canada pour CDW Canada. L'annexe A présente une description détaillée des statistiques démographiques et firmographiques des participants à l'étude.

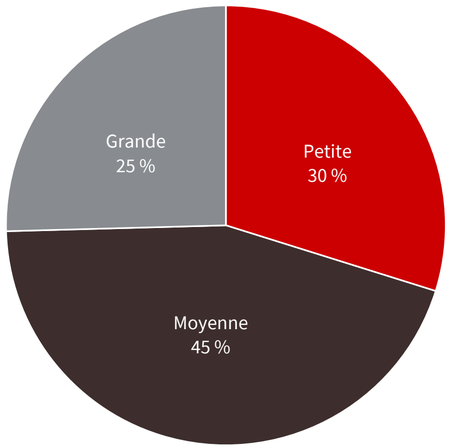


Figure 1 : employés au Canada

Segmentation de la taille des organisations

Aux fins de la présente étude, CDW Canada classifie les organisations ayant répondu comme étant petites, moyennes et grandes. La définition de chaque taille d'organisation est fondée sur le nombre d'employés :

- **Petite :** moins de 100 employés à temps plein situés au Canada
- **Moyenne :** 100 à 999 employés à temps plein situés au Canada
- **Grande :** plus de 1 000 employés à temps plein situés au Canada

Introduction

Les menaces pour le Canada

Cette étude explore l'évolution de la cybersécurité au Canada, en se concentrant sur les tendances, défis et stratégies majeurs que les organisations adoptent pour renforcer leurs défenses. En s'appuyant sur des données d'enquête détaillées, le rapport examine des domaines critiques : la difficulté de mettre en place un modèle à vérification systématique, l'impact des tests de sécurité pour la visibilité, les obstacles à l'adoption de l'IA, l'augmentation des technologies avancées de détection des menaces et les services de détection et de réponse gérées (DRG) comme solution face à la pénurie de main-d'œuvre.

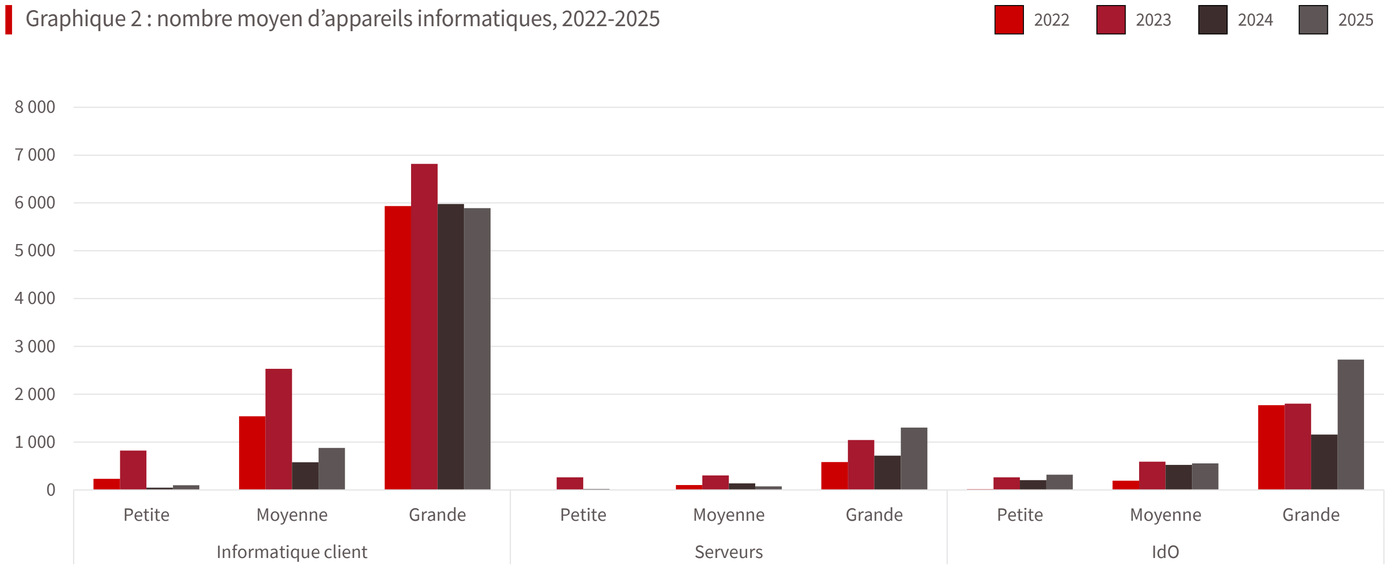
Les résultats mettent en évidence la manière dont les organisations canadiennes gèrent des environnements de sécurité complexes, exploitent les nouvelles technologies et règlent les goulets d'étranglement opérationnels pour atténuer les risques. Les idées et recommandations que nous fournissons visent à donner des pistes concrètes aux professionnels des TI afin qu'ils améliorent la maturité et la résilience de leurs systèmes et qu'ils puissent répondre aux menaces grandissantes.

La surface d’attaque dynamique

Les surfaces d’attaque des organisations canadiennes sont vastes et de plus en plus dynamiques. Elles comprennent les applications de logiciel comme service (SaaS), les interfaces de programmation d’applications (API), les conteneurs, les machines virtuelles (VM), les systèmes de stockage, les appareils de base de données, les appareils réseau, les points terminaux et plus encore. Ces dernières années, le monde des TI a connu des périodes de croissance et de régression qui reflètent sa nature dynamique. Notre étude a analysé spécifiquement la croissance des points terminaux d’utilisateurs (ordinateurs, ordinateurs portatifs, téléphones intelligents et tablettes), des serveurs et des appareils d’Internet des objets (IdO) au fil du temps afin de montrer que la surface d’attaque de TI des organisations est en expansion continue.

Cette évolution a des conséquences, car à mesure que les organisations adoptent de nouvelles technologies et étendent leurs opérations, la taille et la complexité de leurs surfaces d’attaque grandissent. Face à ces défis, les équipes de sécurité doivent s’efforcer de gérer et de protéger ces environnements de façon efficace.

Graphique 2 : nombre moyen d’appareils informatiques, 2022-2025



Informatique client	2022	2023	2024	2025
Petite	231	822	48	99
Moyenne	1 540	2 532	579	880
Grande	5 936	6 817	5 978	5 892

Serveurs	2022	2023	2024	2025
Petite	5	263	20	7
Moyenne	103	302	137	76
Grande	585	1 043	718	1 304

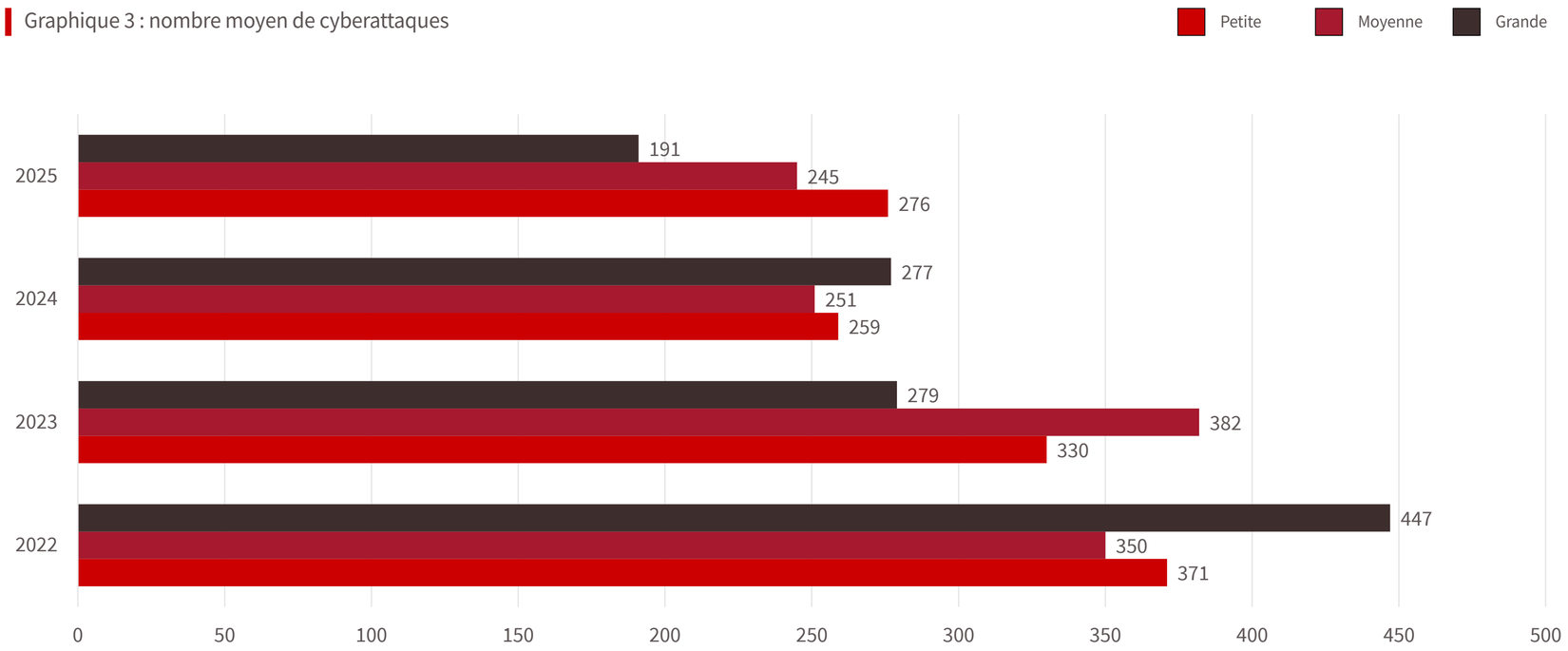
IdO	2022	2023	2024	2025
Petite	17	263	205	319
Moyenne	195	590	523	556
Grande	1 774	1 804	1 159	2 727

Cyberattaques, incidents et temps d’indisponibilité

Pour la deuxième année consécutive, les organisations canadiennes ont signalé une baisse du nombre de cyberattaques en comparaison à l’année précédente. Toutefois, le taux d’infection reste élevé : 86,5 % des répondants en 2024 déclarent avoir subi un incident de sécurité au cours des 12 derniers mois. Si le taux de succès global des attaques a augmenté, c’est que les cyberattaques sont de plus en plus efficaces et difficiles à prévenir.

Nombre moyen de cyberattaques par taille d’organisation

Graphique 3 : nombre moyen de cyberattaques



Cyberattaques : les grandes organisations ont subi moins d’attaques : 447 incidents en 2022 contre 191 en 2025.

Les petites organisations ont subi légèrement plus d’attaques : 259 incidents en 2024 contre 276 en 2025.

Les petites et moyennes organisations ont connu des taux d’attaque relativement semblables par rapport à 2024.

Taux d’infection par catégorie de cyberincidents

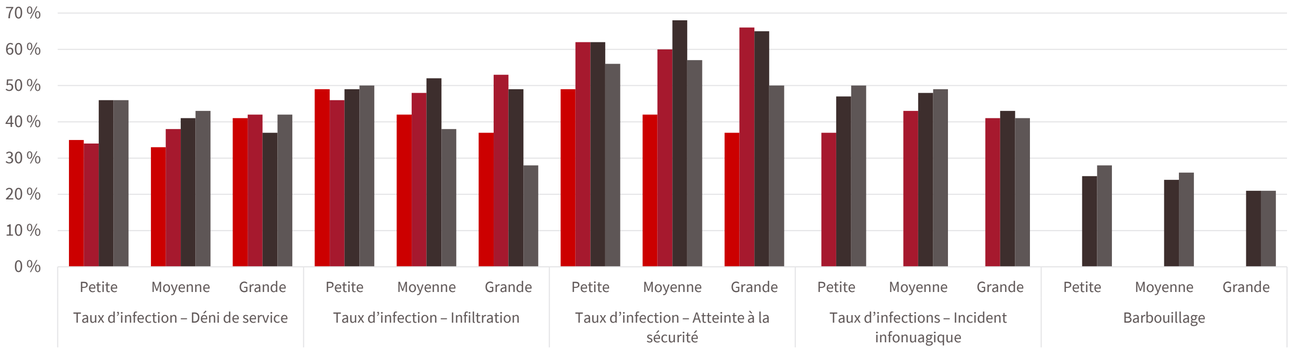
Déni de service (DoS) : le taux d’infection reste stable dans toutes les organisations, même si celles de taille moyenne affichent une légère augmentation : de 41 % en 2024 à 43 % en 2025.

Infiltration : le taux d’infiltration a augmenté dans les petites organisations en atteignant 50 % en 2025, tandis que les grandes organisations ont vu leur taux baisser à 28 % en 2025.

Atteinte à la sécurité : le taux d’atteintes à la sécurité a légèrement diminué dans toutes les organisations, et celles de grande taille ont indiqué une baisse de 65 % à 50 % entre 2024 et 2025.

Taux d’incidents infonuagiques : les taux d’infections infonuagiques affichent une tendance à la hausse dans les petites organisations, en passant de 47 % en 2024 à 50 % en 2025, tandis que les grandes organisations se stabilisent à 41 %.

Incidents de défiguration de site web : les incidents de défiguration de site web ont augmenté dans les petites organisations, en passant de 25 % en 2024 à 28 % en 2025, tandis que ceux des grandes organisations sont restés stables.



Graphique 4 : taux d’infection par catégorie de cyberincidents

2022 2023 2024 2025

Taux d’infection – Déni de service	2022	2023	2024	2025
Petite	35 %	34 %	46 %	46 %
Moyenne	33 %	38 %	41 %	43 %
Grande	41 %	42 %	37 %	42 %

Taux d’infection – Infiltration	2022	2023	2024	2025
Petite	49 %	46 %	49 %	50 %
Moyenne	42 %	48 %	52 %	38 %
Grande	37 %	53 %	49 %	28 %

Taux d’infection – Atteinte à la sécurité	2022	2023	2024	2025
Petite	49 %	62 %	62 %	56 %
Moyenne	42 %	60 %	68 %	57 %
Grande	37 %	66 %	65 %	50 %

Taux d’infections – Incident infonuagique	2023	2024	2025
Petite	37 %	47 %	50 %
Moyenne	43 %	48 %	49 %
Grande	41 %	43 %	41 %

Défiguration de site web	2024	2025
Petite	25 %	28 %
Moyenne	24 %	26 %
Grande	21 %	21 %

Taux de succès des cyberattaques

Alors que le nombre total de cyberattaques et d'infections diminue, le taux de réussite des attaques (incidents causés par des attaques) augmente. Les organisations canadiennes enregistrent 20 à 25 incidents chaque année dans des catégories comme le déni de service, l'infiltration, les atteintes à la sécurité et les incidents infonuagiques.

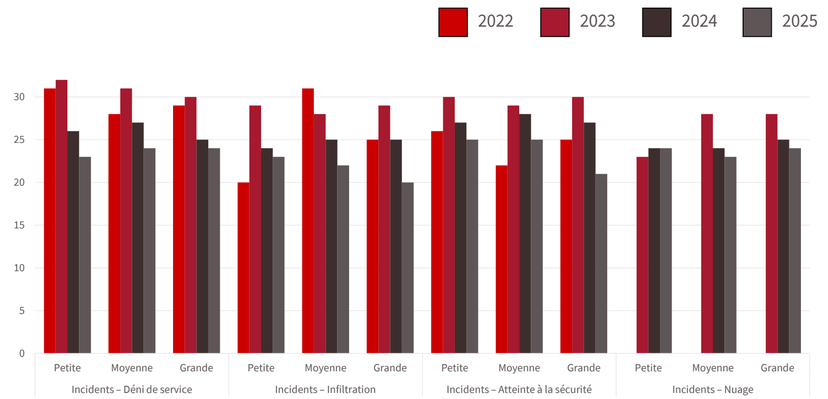
Graphique 5 : nombre d'incidents par catégorie

Incidents – Déni de service	2022	2023	2024	2025
Petite	31	32	26	23
Moyenne	28	31	27	24
Grande	29	30	25	24

Incidents – Atteinte à la sécurité	2022	2023	2024	2025
Petite	26	30	27	25
Moyenne	22	29	28	25
Grande	25	30	27	21

Incidents – Infiltration	2022	2023	2024	2025
Petite	20	29	24	23
Moyenne	31	28	25	22
Grande	25	29	25	20

Incidents – Nuage	2022	2023	2024	2025
Petite	-	23	24	24
Moyenne	-	28	24	23
Grande	-	28	25	24



Incidents de DoS : les organisations de taille moyenne ont observé une légère baisse du nombre d'incidents de DoS, qui sont passés de 27 à 24 entre 2024 et 2025.

Incidents d'infiltration : le nombre d'incidents d'infiltration a diminué dans toutes les organisations, et celles de petite taille ont indiqué une baisse de 24 à 23 entre 2024 et 2025.

Incidents d'atteinte à la sécurité : le nombre d'incidents d'atteinte à la sécurité est resté stable dans les petites organisations (environ 25 en 2025), tandis que celui des grandes organisations a baissé (21 incidents).

Le nombre d'attaques qui diminue combiné au taux d'incidents qui reste stable signifie que les cyberattaques sont devenues plus ciblées et efficaces, en particulier contre les organisations de petite et moyenne taille.

Temps d’indisponibilité et temps d’indisponibilité par incident

Les temps d’indisponibilité causés par les cyberincidents restent importants, mais deviennent de plus en plus courts au fil du temps. En revanche, les temps d’indisponibilité par incident continuent d’augmenter, en particulier ceux qui concernent les atteintes à la sécurité et l’infonuagique, car les problèmes sont de plus en plus compliqués à résoudre et les systèmes de TI sont de moins en moins résilients.

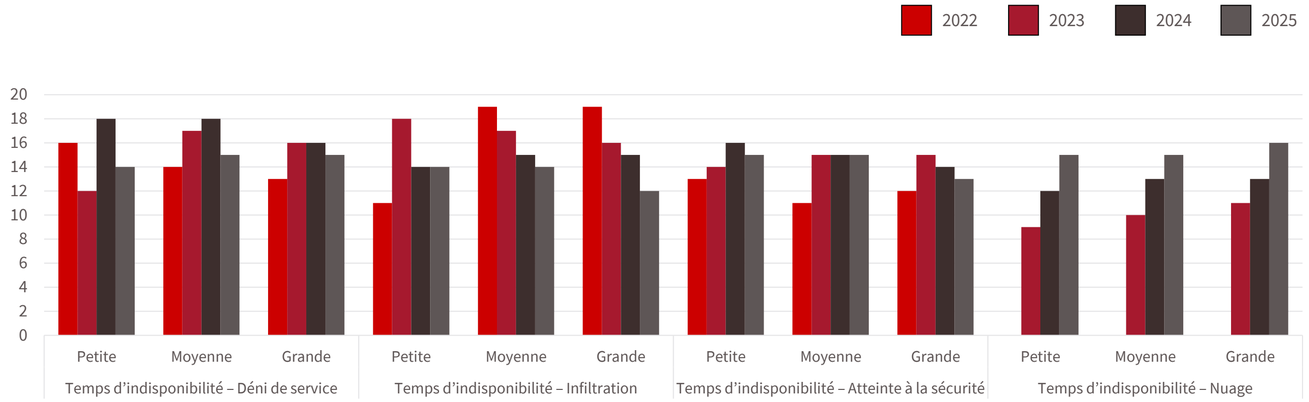
Graphique 6 : temps moyen d’indisponibilité, 2022-2025 (en jours)

Temps d’indisponibilité – Déni de service	2022	2023	2024	2025
Petite	16	12	18	14
Moyenne	14	17	18	15
Grande	13	16	16	15

Temps d’indisponibilité – Infiltration	2022	2023	2024	2025
Petite	11	18	14	14
Moyenne	19	17	15	14
Grande	19	16	15	12

Temps d’indisponibilité – Atteinte à la sécurité	2022	2023	2024	2025
Petite	13	14	16	15
Moyenne	11	15	15	15
Grande	12	15	14	13

Temps d’indisponibilité – Nuage	2022	2023	2024	2025
Petite	_	9	12	15
Moyenne	_	10	13	15
Grande	_	11	13	16



Temps d’indisponibilité liés aux DoS : les petites organisations ont vu leur temps d’indisponibilité lié aux incidents de DoS diminuer et passer d’une moyenne de 18 jours en 2024 à 14 jours en 2025.

Temps d’indisponibilité liés aux infiltrations : il s’est maintenu à un niveau moyen de 14 jours dans les petites et moyennes organisations.

Temps d’indisponibilité liés aux atteintes à la sécurité : le temps d’indisponibilité des petites organisations s’est stabilisé (15 jours en moyenne), tandis que celui des grandes organisations est passé de 14 jours en moyenne en 2024 à 13 jours en 2025.

Temps d’indisponibilité liés aux incidents infonuagiques : le temps d’indisponibilité lié aux incidents infonuagiques est passé de 12 jours en moyenne en 2024 à 15 jours en 2025 dans les petites organisations.

Les temps d’indisponibilité par incidents ont significativement augmenté d’une année à l’autre

Atteinte à la sécurité : en hausse de 10 %. Les petites organisations ont connu une augmentation de 3 %.

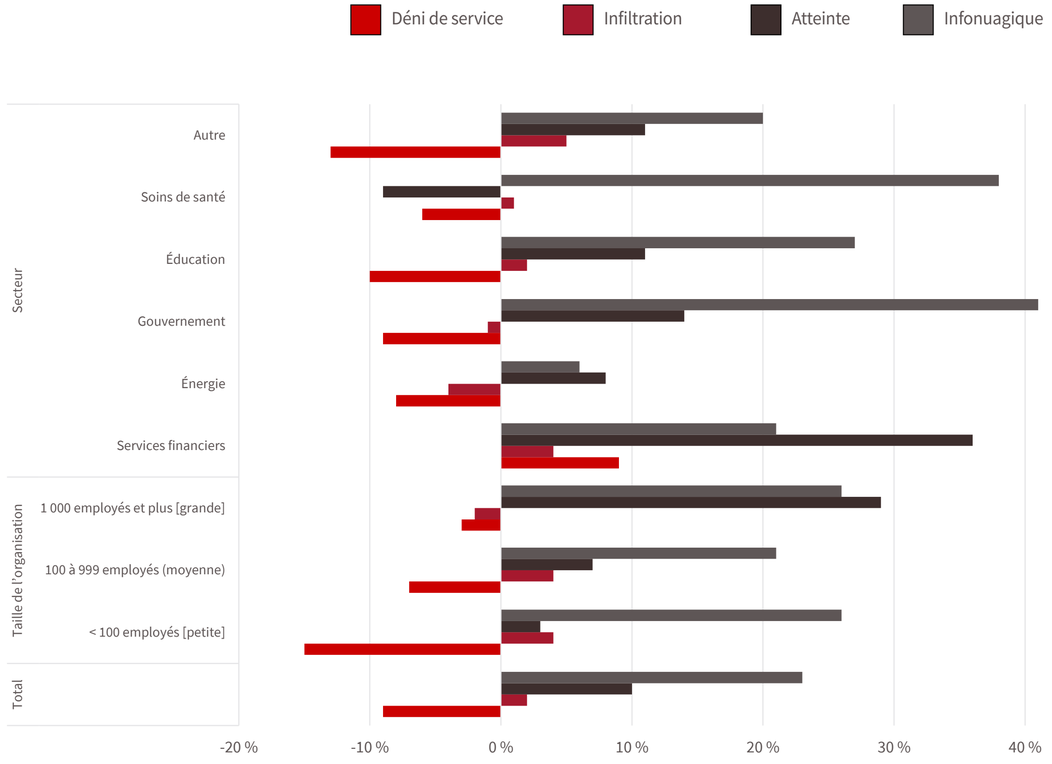
Incidents infonuagiques : en hausse de 23 %. Ils touchent particulièrement les secteurs gouvernementaux (+41 %) et de soins de santé (+38 %).

Graphique 7 : augmentation du temps d’indisponibilité par incident d’une année à l’autre (%)

Temps d’indisponibilité selon la taille de l’industrie	Déni de service	Infiltration	Atteinte	Nuage
Services financiers	9 %	4 %	36 %	21 %
Énergie	-8 %	-4 %	8 %	6 %
Gouvernement	-9 %	-1 %	14 %	41 %
Éducation	-10 %	2 %	11 %	27 %
Soins de santé	-6 %	1 %	-9 %	38 %
Autre	-13 %	5 %	11 %	20 %

Temps d’inactivité selon la taille de l’entreprise	Déni de service	Infiltration	Atteinte	Nuage
Petite	-15 %	4 %	3 %	26 %
Moyenne	-7 %	4 %	7 %	21 %
Grande	-3 %	-2 %	29 %	26 %

Temps d’indisponibilité d’une année à l’autre	Déni de service	Infiltration	Atteinte	Nuage
Total	-9 %	2 %	10 %	23 %



Maturité des programmes de cybersécurité canadiens

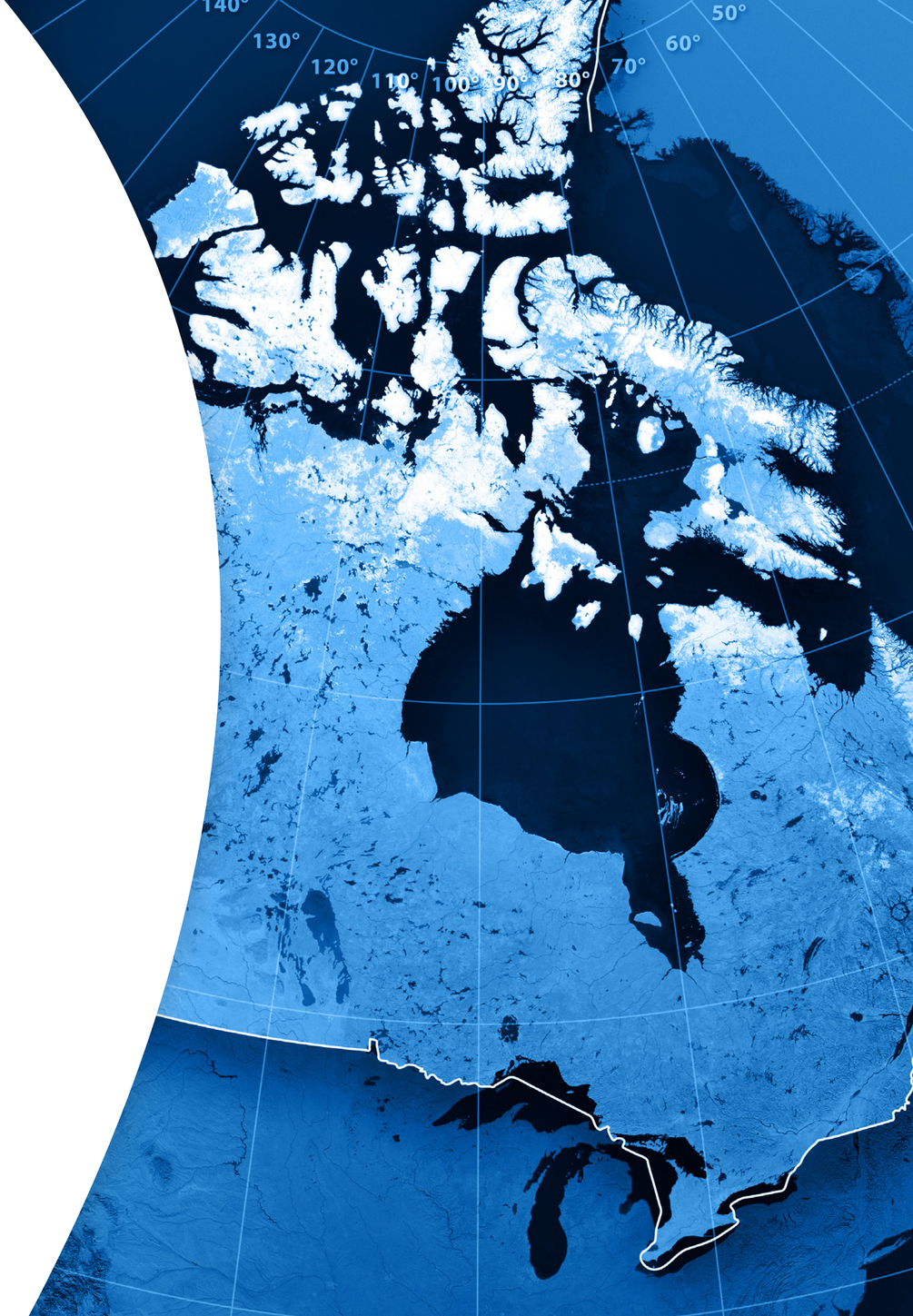
Dans le cadre de « l'Étude Cybersécurité au Canada 2025 » de CDW, les répondants ont dû évaluer la maturité de leur organisation dans dix domaines de cybersécurité essentiels, ainsi que ses capacités globales en matière de cybersécurité. Les groupes suivants sont énumérés des moins matures aux plus matures, afin d'aider les organisations à comparer leur posture de cybersécurité actuelle :

- Gestion des actifs et configuration
- Gouvernance et conformité en matière de sécurité
- Gestion des identités et des accès
- Protection des données et confidentialité
- Gestion des ressources humaines et des menaces internes
- Sécurité du réseau
- Sécurité infonuagique
- Détection et réponse aux incidents
- Continuité et résilience des affaires
- Sécurité des fournisseurs et des tiers

Les résultats ont révélé une forte corrélation entre la maturité par domaine et la maturité globale du programme de cybersécurité d'une organisation.

Ces liens nous ont permis de regrouper les répondants en quatre catégories de maturité différentes : **défense réactive, protection des fondations, résilience opérationnelle et sécurité stratégique.**

Nous utiliserons ces catégories tout au long de l'étude afin de montrer comment le niveau de maturité d'une organisation peut influencer les pratiques et les résultats de cybersécurité.



Définition des groupes de maturité

Nous avons classé les organisations en quatre niveaux de maturité en fonction de leurs processus, de leurs politiques et de leur alignement avec les normes de l'industrie :

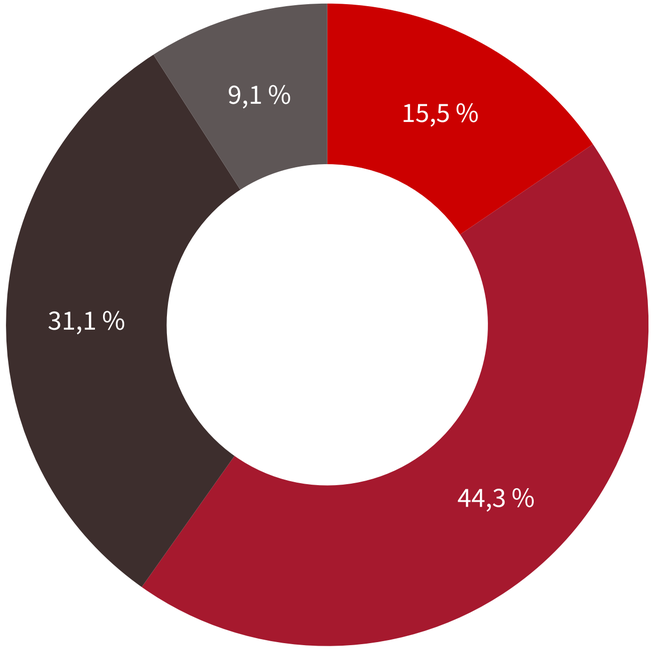
Défense réactive : les organisations de ce groupe ont des processus de cybersécurité limités ou uniquement dédiés à des situations spécifiques. Leur posture de sécurité présente des lacunes importantes, car elle manque de structure, de documentation et de cohérence.

Protection des fondations : ces organisations ont établi des politiques documentées et ont déterminé des rôles pour les processus. Elles ont commencé à s'aligner sur les normes de l'industrie, mais ont des difficultés à assurer la cohérence et l'extensibilité de leurs programmes de sécurité.

Résistance opérationnelle : ces organisations ont des processus bien établis qui sont appliqués et harmonisés avec les normes reconnues de l'industrie. Elles effectuent régulièrement des vérifications de conformité et des examens pour assurer l'efficacité du programme.

Sécurité stratégique : ce groupe représente le plus haut niveau de maturité en cybersécurité. Les processus sont entièrement automatisés, continuellement améliorés et régulièrement vérifiés. Ces organisations privilégient les résultats mesurables et la résilience, tout en adoptant une approche proactive de la cybersécurité.

Cette segmentation basée sur la maturité fournit des renseignements précieux tout au long de l'étude et met en évidence les contrastes entre les organisations qui sont à différents stades de leur parcours de cybersécurité. Elle permet d'identifier les forces et les vulnérabilités, en plus d'aider les organisations à se comparer et à planifier des mesures pour optimiser leur sécurité.



Graphique 8 : pourcentage de répondants par groupe de maturité

Principale constatation 1

L’adoption de l’IA générative prend du retard

Protection des renseignements personnels, pénurie de main-d’œuvre qualifiée et défis techniques : l’IA générative peine à gagner du terrain dans les organisations canadiennes

L’IA générative a le potentiel de révolutionner les industries du monde entier en redéfinissant l’automatisation, les processus de prise de décision et l’innovation. Toutefois, les organisations canadiennes font face à d’importants défis lorsqu’elles souhaitent concrétiser leurs validations de principe. L’étude révèle que les organisations canadiennes ont réalisé en moyenne 17 validations de principe d’IA générative entre 2023 et 2024, mais que seulement 28,2 % d’entre eux ont été concrétisés. Ce faible taux de conversion met en évidence les obstacles qui freinent l’adoption de l’IA générative et empêchent les organisations de profiter pleinement de ses avantages.

Obstacles à l’adoption de l’IA générative

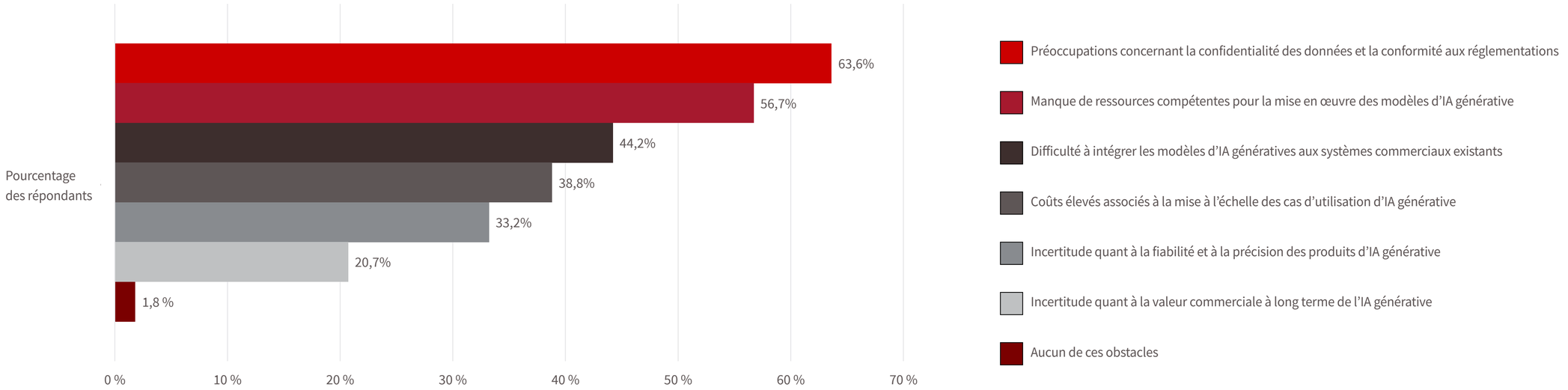
Préoccupations concernant la protection des renseignements personnels et la conformité

La protection des renseignements personnels et la conformité aux réglementations ont été citées comme les principaux obstacles commerciaux empêchant les cas d’utilisation d’IA générative de passer la phase de validations de principe (graphique 9). Les organisations, en particulier dans les industries réglementées, hésitent à exposer des données sensibles pendant les étapes d’entraînement et de mise en œuvre. Ces préoccupations limitent l’intégration de modèle d’IA générative dans les processus opérationnels essentiels.

Pénuries de compétences pour la mise en œuvre de l’IA générative

Le manque de ressources compétentes pour développer, déployer et gérer les modèles d’IA générative reste un obstacle critique (graphique 9). Sans expertise interne, de nombreuses organisations peinent à mettre en œuvre efficacement les projets alimentés par l’IA, qui finissent par ne jamais voir le jour ou par ne pas atteindre les objectifs attendus.

Graphique 9 : obstacles empêchant les cas d’utilisation d’IA générative de concrétiser leurs validations de principe



Défis techniques

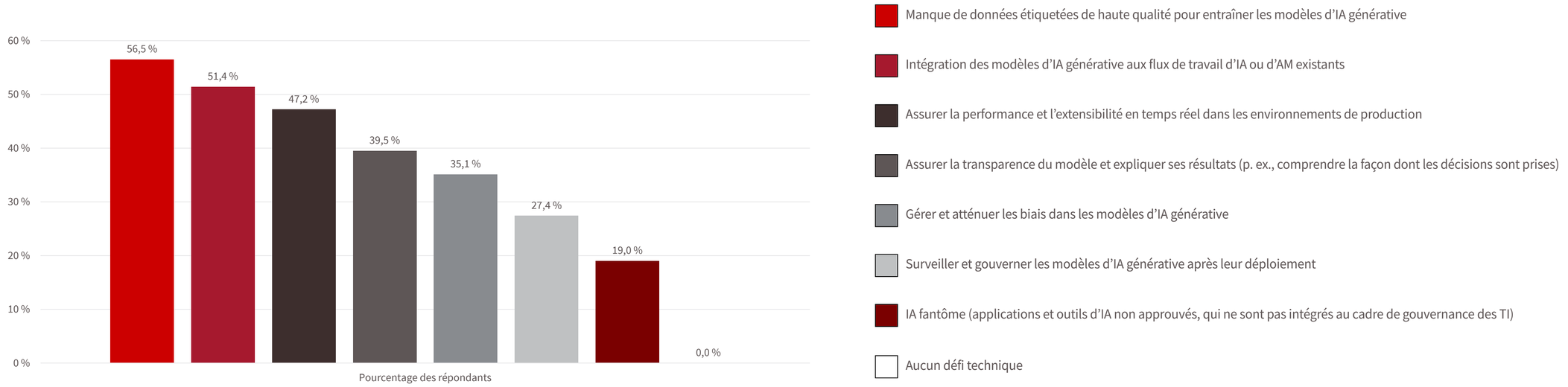
Les répondants ont identifié les défis techniques suivants comme les obstacles majeurs à l'adoption de l'IA générative (graphique 10) :

- **Manque de données étiquetées de haute qualité :** la mauvaise qualité des données compromet la précision et la fiabilité des modèles d'IA générative et les rend moins efficaces dans des scénarios réels.
- **Intégration aux flux de travail d'IA ou d'AM existants :** les environnements de TI complexes et les systèmes hérités complexifient l'intégration des modèles d'IA générative.
- **Performances et mise à l'échelle en temps réel :** de nombreuses organisations ont des difficultés à déployer des modèles d'IA générative à plus grande échelle.

Obstacles supplémentaires

Les organisations ont également mentionné les coûts élevés associés à l'extensibilité des cas d'utilisation d'IA générative et une méfiance quant à la fiabilité et à la précision des produits d'IA générative. Les préoccupations sur des biais et erreurs possibles dissuadent encore les organisations de concrétiser les projets d'IA (graphique 10).

Graphique 10 : défis techniques lors de la mise en œuvre de l'IA générative

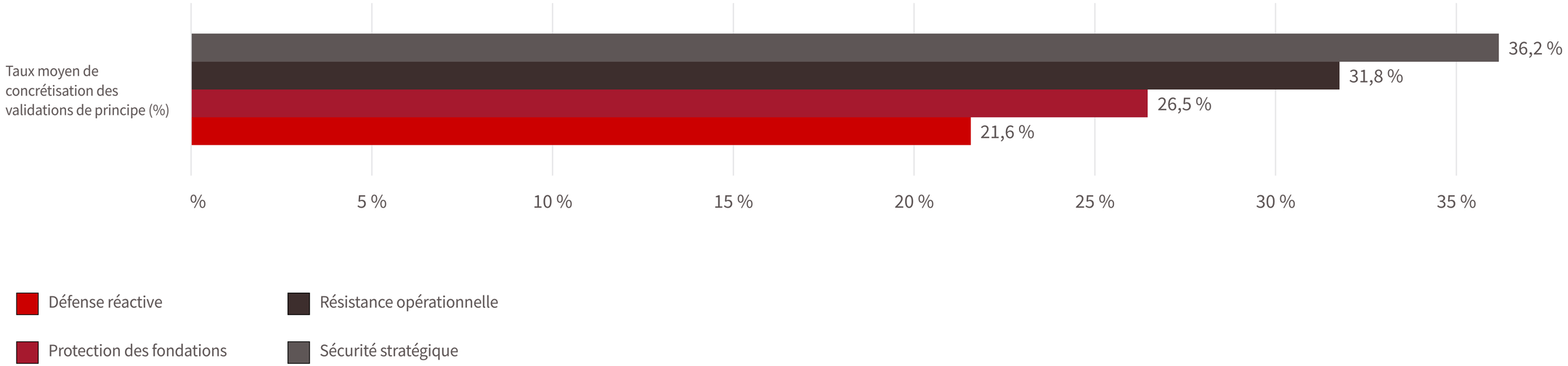


Le rôle de la maturité dans l'adoption de l'IA

Les organisations qui ont des programmes de sécurité matures réussissent davantage à concrétiser leurs cas d'utilisation d'IA générative. Selon l'étude, les organisations de la catégorie de maturité « sécurité stratégique » concrétisent en moyenne 36,17 % de leurs validations de principe, contre 21,56 % seulement pour celles de la catégorie « défense réactive ».

Une maturité accrue permet aux organisations de relever les défis techniques et opérationnels grâce à une meilleure gouvernance des données, à l'intégration de technologies de pointe et à l'allocation des ressources. Les programmes matures favorisent également la confiance accordée aux résultats d'IA, car ils permettent aux organisations d'aligner plus efficacement leurs initiatives d'IA avec des objectifs commerciaux plus larges.

Graphique 11 : taux de concrétisation moyen des validations de principe par groupe de maturité (%)

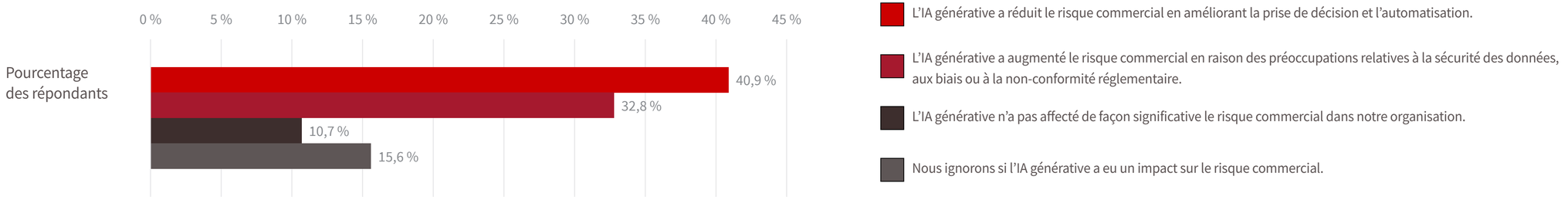


Impact sur les organisations canadiennes

En tardant à adopter l'IA générative, les organisations canadiennes ont des difficultés à exploiter pleinement ses capacités de prise de décision, d'automatisation et d'innovation. Si 41 % des répondants ont déclaré que l'IA générative avait réduit les risques commerciaux en améliorant la prise de décision et l'efficacité opérationnelle, 33 % ont exprimé des inquiétudes quant à l'augmentation des risques liés à la sécurité des données, aux biais et à la non-conformité réglementaire (graphique 12).

Ces obstacles, combinés à des défis techniques tels que la mauvaise qualité des données et les difficultés d'intégration, empêchent les organisations de mettre à l'échelle les solutions d'IA générative et d'obtenir des avantages concurrentiels.

Graphique 12 : impact de l'IA générative sur le risque commercial



Conclusion

Les organisations doivent tirer parti de la lente adoption de l'IA générative. En améliorant les cadres de gouvernance des données, en renforçant les capacités d'IA à l'interne et en se concentrant sur des solutions évolutives et fiables, les organisations peuvent non seulement accélérer la mise en œuvre de leurs validations de principe, mais aussi surmonter des obstacles comme la gouvernance des données, la gestion des identités et des accès, l'intégration de la sécurité et la pénurie de compétences. Ces efforts nécessaires renforcent la sécurité globale et les fondations des TI. Ces obstacles mettent en évidence une dette technique et de sécurité persistante, qui doit être maîtrisée non seulement pour l'IA, mais aussi pour la résilience à long terme des organisations.

En relevant ces défis fondamentaux, les organisations peuvent concrétiser leurs validations de principe en toute confiance, en s'assurant que le déploiement de l'IA est responsable, sécurisé et adapté à leurs besoins. Le travail effectué aujourd'hui pour aligner les objectifs de sécurité, de conformité et de commerce permettra aux organisations d'exploiter tout le potentiel de l'IA en réduisant les risques au minimum. Ce retard est peut-être une étape nécessaire vers une adoption durable de l'IA et une posture de sécurité plus saine.

Principale constatation 2

Les tests de sécurité sont rentables

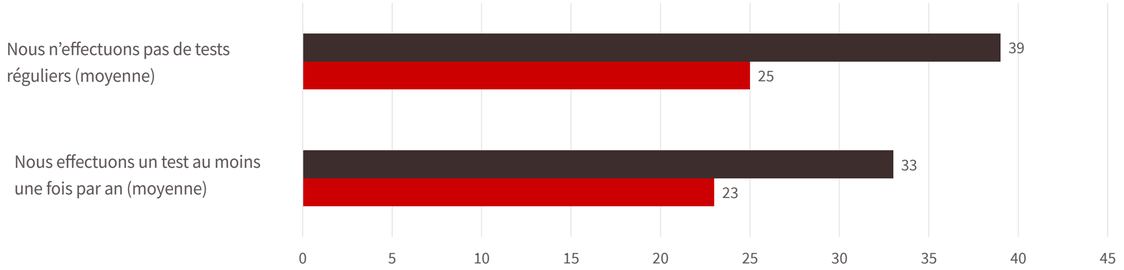
Les tests annuels réduisent les risques d'atteinte à la sécurité et aident les organisations canadiennes à réduire les incidents graves

Les tests de sécurité se sont avérés être l'un des outils les plus efficaces pour réduire le risque de cyberinfractions et prévenir les incidents de sécurité importants. Les organisations qui effectuent des tests de sécurité (test d'intrusion/simulation d'attaque) au moins une fois par an sont mieux équipées pour identifier les vulnérabilités avant qu'elles puissent être exploitées. L'enquête révèle que les organisations qui effectuent des tests de sécurité annuels signalent moins d'incidents d'infiltration (23 incidents en moyenne) et moins d'atteintes à la sécurité (33 incidents en moyenne) que celles qui n'effectuent pas de tests réguliers, qui signalent 25 et 39 incidents, respectivement. Ces chiffres démontrent l'impact des tests de sécurité sur l'atténuation des risques et l'anticipation des incidents.

Graphique 13 : fréquence des tests de sécurité et nombre moyen d'infiltrations et de failles dans la sécurité des données subies par les organisations canadiennes

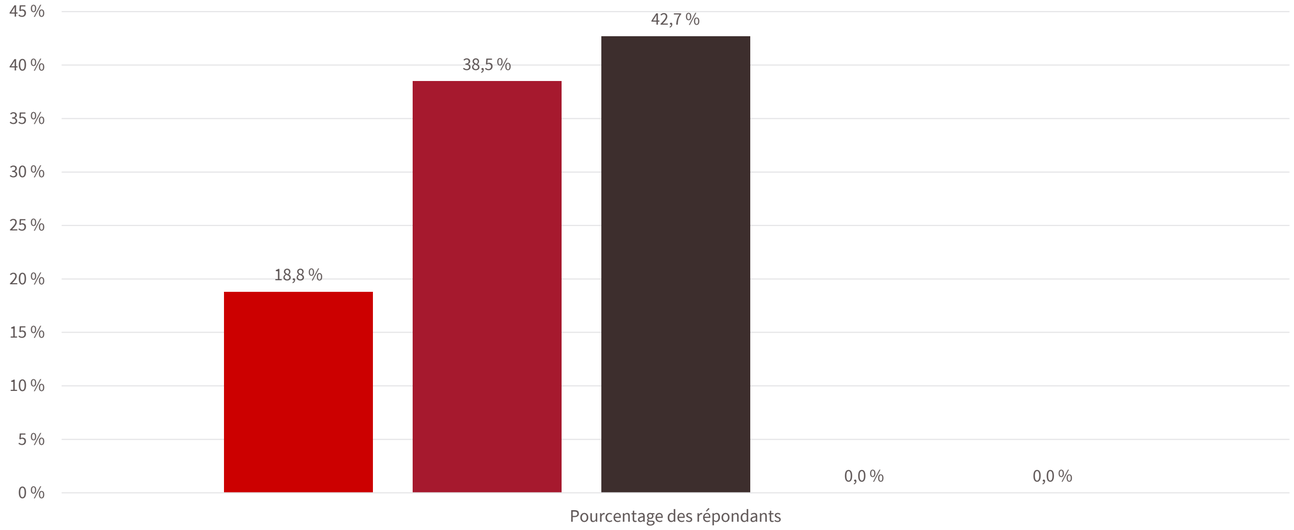
Infiltration (les auteurs des attaques ont pu accéder au réseau, à l'infrastructure ou aux données de l'organisation, mais aucune donnée n'a été exfiltrée)

Atteinte à la sécurité (des données ont été exfiltrées)



L'efficacité des tests d'intrusion

Les tests d'intrusion sont la pierre angulaire des programmes de sécurité efficaces. Selon l'étude, 61 % des répondants ont indiqué que les tests d'intrusion avaient permis de découvrir des vulnérabilités qui auraient pu prévenir des incidents antérieurs, tandis que 81 % ont ciblé et évité des futures atteintes à la sécurité. Il est important de noter qu'aucune personne interrogée n'a jugé les tests d'intrusion inefficaces, ce qui souligne le rôle essentiel qu'ils jouent dans la découverte des lacunes de sécurité et le renforcement des défenses.



Graphique 14 : efficacité des tests d'intrusion dans la découverte de vulnérabilités qui préviennent les incidents graves

Oui, incidents passés seulement

Oui, incidents futurs seulement

Oui, incidents passés et futurs

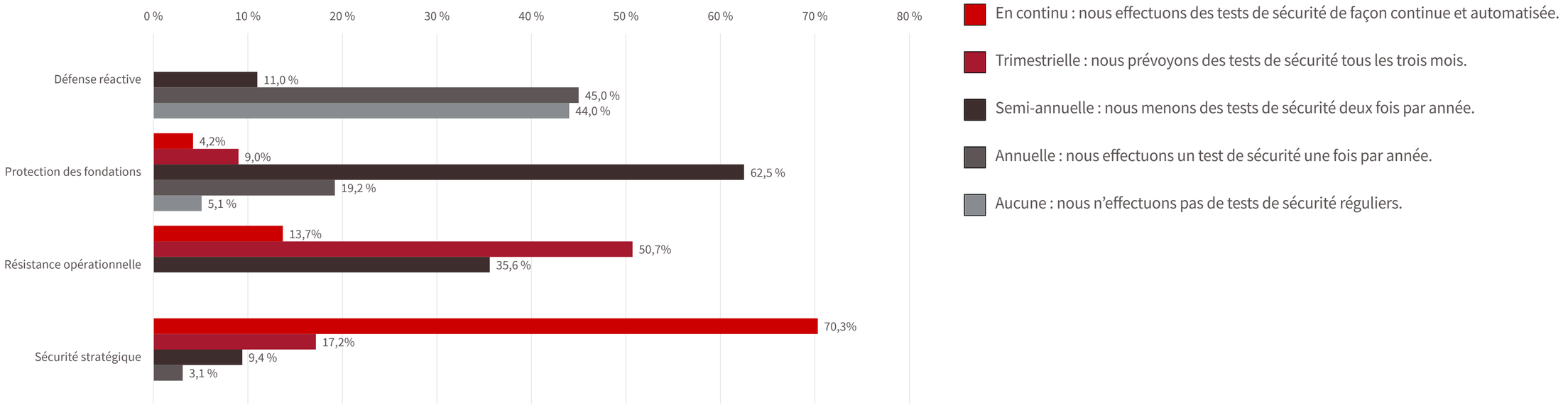
Non

Ne sait pas

Tests continus : la solution pour assurer la maturité des programmes de sécurité

Les tests de sécurité et la validation en continu sont essentiels pour assurer la maturité des programmes. Les données montrent que 70,3 % des organisations dans la catégorie « sécurité stratégique » effectuent des tests automatisés continus, contre 13,7 % dans le groupe « résistance opérationnelle » et 4,2 % dans le groupe « protection des fondations » (graphique 15). Les organisations qui effectuent des tests en continu peuvent détecter et traiter les vulnérabilités de manière proactive et en temps réel, ce qui leur permet de s'adapter à des environnements de menaces modernes et dynamiques. Les organisations qui intègrent ces tests dans les pratiques agiles et les pratiques de développement et exploitation, et qui tirent parti de l'automatisation, sont moins dépendantes des processus manuels, améliorent leur efficacité et traitent les risques plus tôt dans le cycle de vie du logiciel. Cette approche est essentielle pour assurer la résilience dans le paysage de la cybersécurité en constante évolution.

Graphique 15 : fréquence des tests de sécurité par groupe de maturité

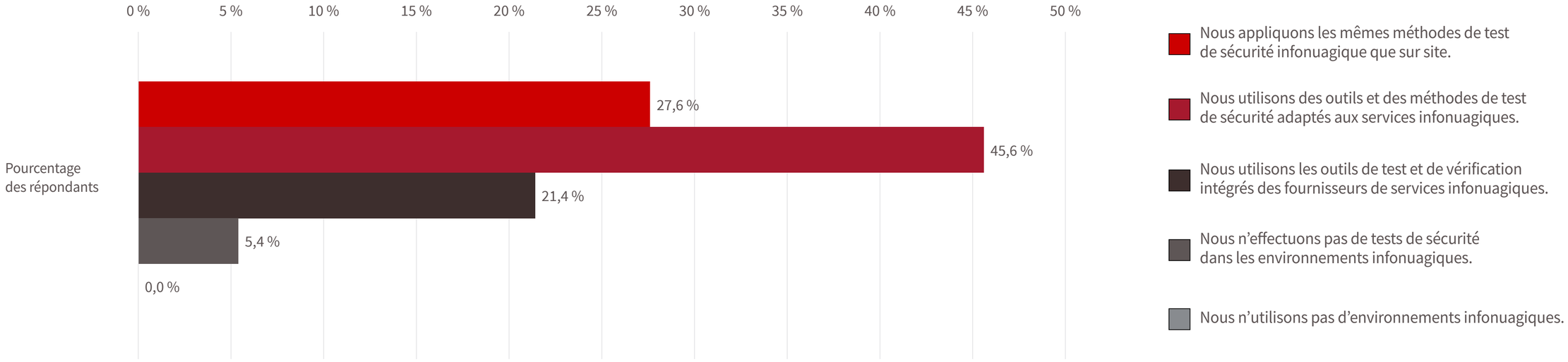


Tests de sécurité de l’infonuagique : un domaine à la traîne

Même si presque 100 % des organisations canadiennes sont passés à l’infonuagique, beaucoup d’entre elles tardent à faire évoluer leurs tests de sécurité pour les environnements infonuagiques. Seulement 45,6 % des répondants ont indiqué qu’ils utilisent des outils et des méthodologies de test de sécurité adaptés à leur environnement. En revanche, 27,6 % continuent d’appliquer les mêmes méthodes de test que celles utilisées pour les systèmes sur site, tandis que 21,4 % s’appuient uniquement sur les outils de test de sécurité intégrés des fournisseurs de services infonuagiques (graphique 16). Cette absence de tests exhaustifs propres à l’infonuagique augmente le risque dans les infrastructures de TI hybrides et infonuagiques natives.

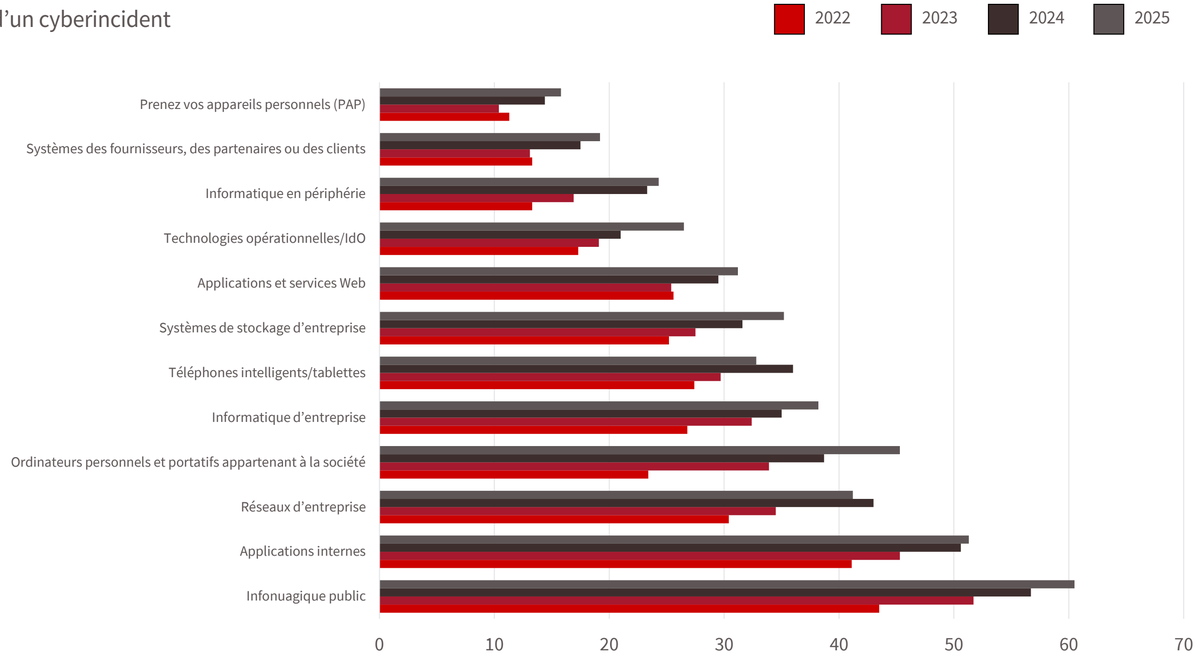
En outre, l’étude révèle que les environnements infonuagiques publics sont les composants de TI les plus affectés par les cyberincidents : 60,5 % des répondants ont déclaré avoir été affectés en 2025. Ce chiffre est en augmentation constante par rapport à 2022 (43,5 %), ce qui confirme le besoin urgent d’adopter des pratiques plus robustes en matière de tests de sécurité infonuagiques.

Graphique 16 : méthode de test de sécurité infonuagique



Graphique 17 : pourcentage de répondants ayant signalé un impact sur des composants de TI à la suite d'un cyberincident

	2022	2023	2024	2025
Infonuagique public	43,5	51,7	56,7	60,5
Applications internes	41,1	45,3	50,6	51,3
Réseaux d'entreprise	30,4	34,5	43	41,2
Ordinateurs personnels et portatifs appartenant à la société	23,4	33,9	38,7	45,3
Informatique d'entreprise	26,8	32,4	35	38,2
Téléphones intelligents/tablettes	27,4	29,7	36	32,8
Systèmes de stockage d'entreprise	25,2	27,5	31,6	35,2
Applications et services Web	25,6	25,4	29,5	31,2
Technologies opérationnelles/IdO	17,3	19,1	21	26,5
Informatique en périphérie	13,3	16,9	23,3	24,3
Systèmes des fournisseurs, des partenaires ou des clients	13,3	13,1	17,5	19,2
Prenez vos appareils personnels (PAP)	11,3	10,4	14,4	15,8



Conclusion

Les tests de sécurité réguliers présentent des avantages évidents pour les organisations canadiennes : ils réduisent directement les risques d'atteinte à la sécurité et améliorent la prévention des incidents. Les organisations qui effectuent des tests annuels ou continus sont mieux préparées à identifier et à traiter les vulnérabilités, ce qui renforce leur position globale en matière de sécurité. Mais le faible nombre de tests adaptés à l'infonuagique entraîne des vulnérabilités dans les environnements hybrides en pleine expansion. Pour faire face efficacement aux menaces dynamiques d'aujourd'hui, les organisations doivent effectuer des tests de sécurité automatisés et continus, adaptés à leurs infrastructures de TI uniques, en particulier dans les environnements infonuagiques. Ces changements sont essentiels pour atténuer les risques et assurer la résilience dans le paysage de la cybersécurité en constante évolution.

Principale constatation 3

Amélioration de la détection et de la réponse aux incidents

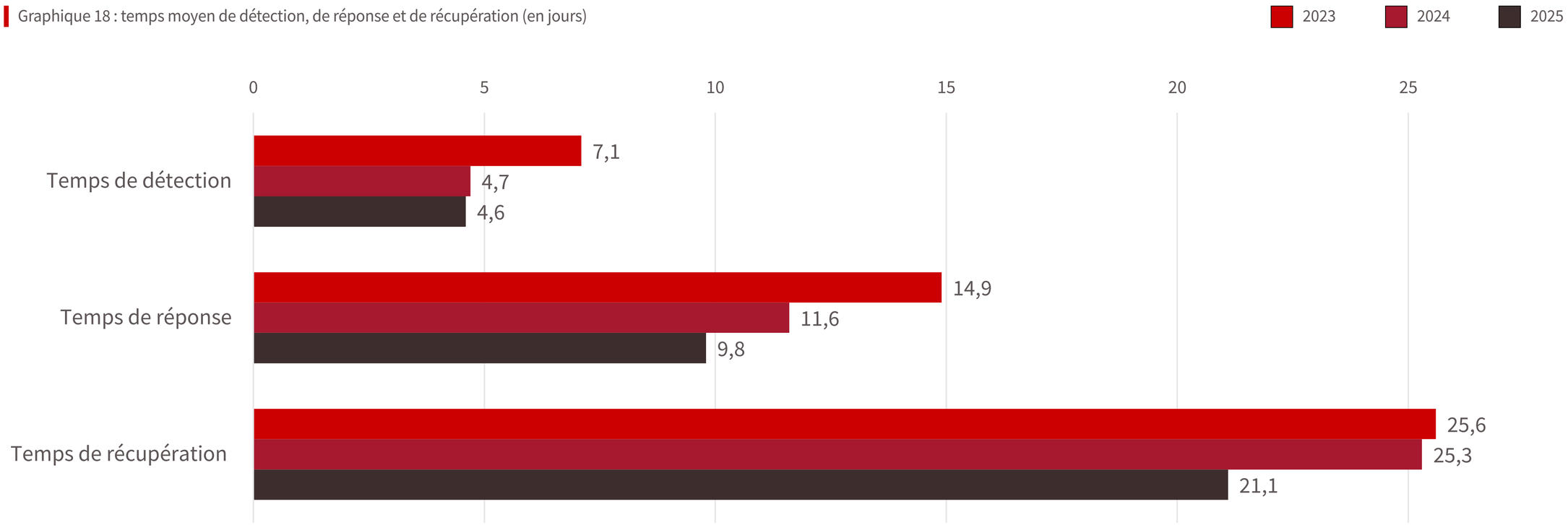
Les équipes de sécurité canadiennes améliorent les délais de réponse en adoptant des technologies avancées de détection des menaces

Le succès d'un programme de cybersécurité dépend de l'efficacité des systèmes à détecter des menaces, puis à y répondre et à se rétablir. L'étude révèle que les organisations canadiennes réalisent des progrès constants dans ces trois domaines, car elles adoptent de plus en plus de technologies avancées de détection des menaces. Les organisations constatent une réduction significative du temps nécessaire de détection, de réponse et de récupération en cas d'incidents.

Le délai moyen de détection des cyberattaques s'est amélioré pour passer de 7,1 jours en 2023 à 4,6 jours en 2025, tandis que les délais de réponse ont considérablement diminué, de 14,9 jours en 2023 à 9,8 jours en 2025. De même, les temps de récupération se sont améliorés, de 25,6 jours en 2023 à 21,1 jours en 2025.

Ces tendances reflètent une efficacité croissante dans la gestion des cybermenaces, qui permet aux organisations d'atténuer les attaques plus rapidement et de minimiser les perturbations dans les opérations. Cependant, la tendance est inversée pour les petites organisations, qui ont vu leurs délais de détection augmenter de 4 jours à 6,8 jours entre 2024 et 2025. Leurs délais de réponse et de récupération sont également plus longs que les moyennes et grandes organisations.

Graphique 18 : temps moyen de détection, de réponse et de récupération (en jours)

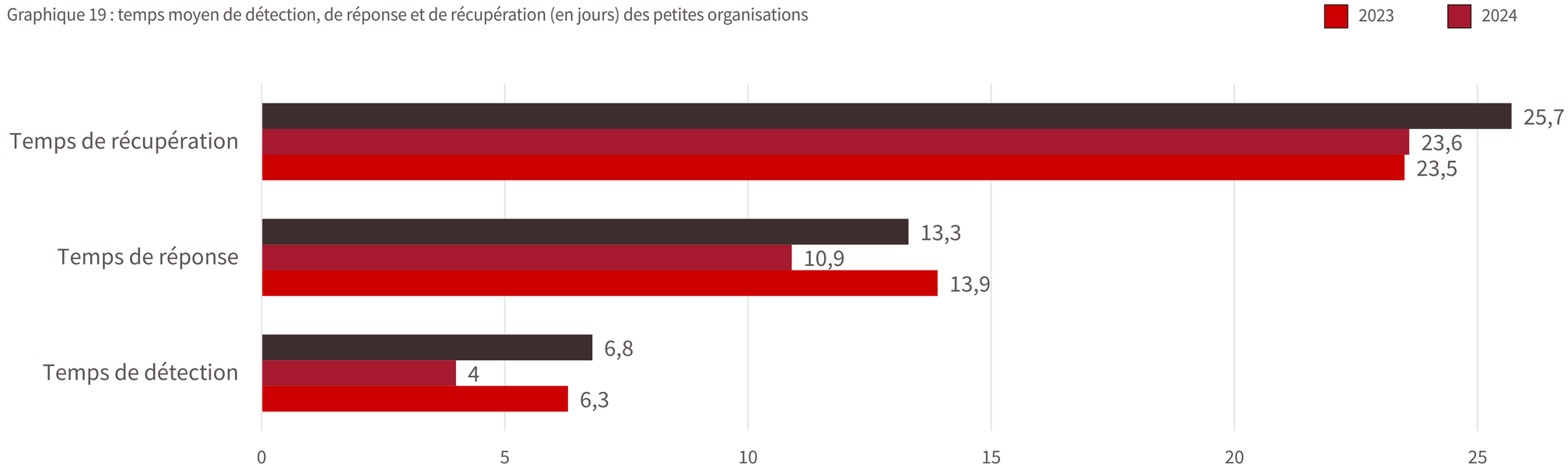


Les défis pour les petites organisations

Alors que les grandes entreprises s'améliorent, les petites organisations (moins de 100 employés) peinent à réduire les temps de détection et de réponse. Plusieurs facteurs contribuent à cette disparité, notamment :

- **Capacités limitées de réponse aux incidents :** les petites organisations ne disposent souvent pas de centre des opérations de sécurité (COS) ou d'équipes de sécurité dédiées. Elles s'appuient sur leur personnel de TI, dont l'expertise en cybersécurité est limitée, ce qui retarde la détection et la réponse en cas de menace.
- **Contraintes budgétaires et autres priorités :** les petites entreprises doivent faire le choix d'investir dans la cybersécurité ou dans d'autres technologies informatiques, ce qui limite l'accès aux outils de sécurité avancés, au personnel et aux solutions de réponse automatisée aux menaces.
- **Absence de sensibilisation et de formation sur la cybersécurité :** sans programme structuré de sensibilisation à la sécurité, les employés sont plus exposés à l'hameçonnage et au piratage psychologique, ce qui augmente le risque de menaces non détectées.

Graphique 19 : temps moyen de détection, de réponse et de récupération (en jours) des petites organisations



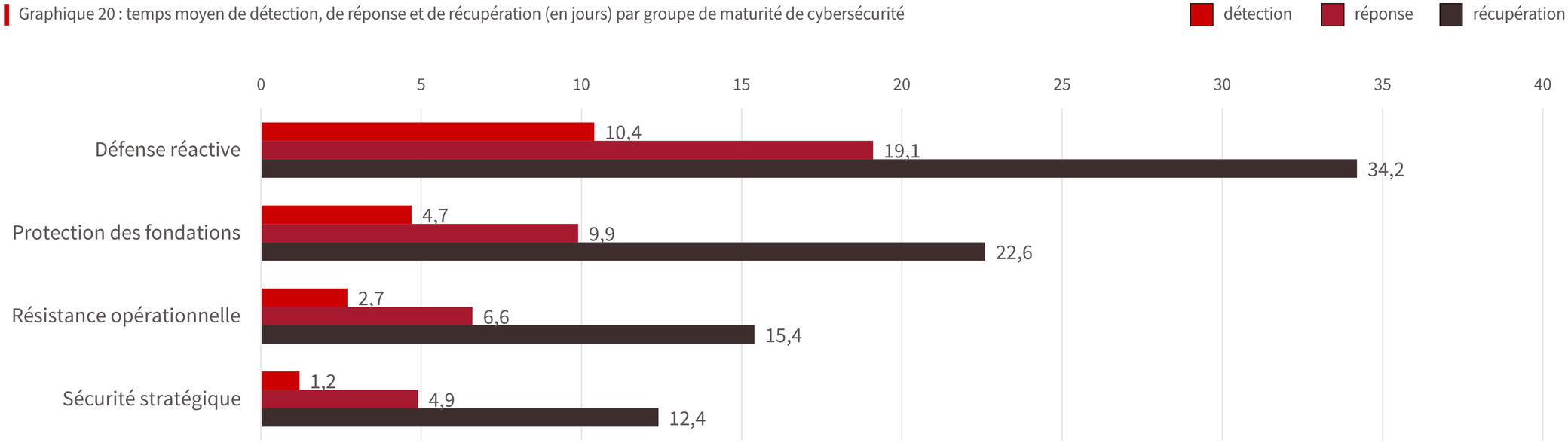
La maturité en cybersécurité fait la différence

La maturité du programme de sécurité d'une organisation a un impact direct sur sa capacité à détecter les cyberincidents, à y répondre et à se rétablir. Mais l'étude montre que les organisations dans la catégorie « sécurité stratégique » (le groupe le plus mature) détectent les cybermenaces près de 10 fois plus rapidement que celles dans la catégorie « défense réactive » (le groupe le moins mature) d'une moyenne de 1,2 jour contre 10,4 jours. La même tendance s'applique aux temps de réponse et de récupération.

Les éléments suivants contribuent à la maturité d'un programme de sécurité :

- Processus d'intervention bien définis qui permettent une atténuation rapide;
- Détection proactive des menaces au moyen de stratégies de défense multicouche;
- Automatisation et analyse évoluées, qui permettent aux équipes de répondre aux menaces en temps réel.

Graphique 20 : temps moyen de détection, de réponse et de récupération (en jours) par groupe de maturité de cybersécurité



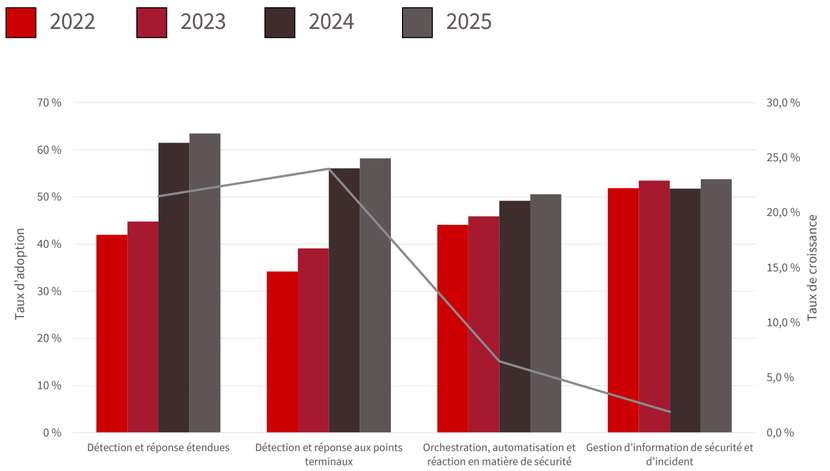
Les technologies de détection et réponse aux points terminaux et de détection et réponse étendues ont le vent en poupe

L'adoption de nouvelles technologies de détection et réponse aux points terminaux et de détection et réponse étendues dépasse les solutions de sécurité traditionnelles comme la gestion d'information de sécurité et d'incident et l'orchestration, automatisation et réponse aux incidents de sécurité.

Tendances clés d'adoption :

- L'adoption d'outils de détection et réponse étendues a augmenté de 42,0 % en 2022 à 63,5 % en 2025 : une croissance de 21,5 % en quatre ans. La hausse la plus marquée a eu lieu entre 2023 et 2024, avec une augmentation de 44,8 % à 61,5 %.
- L'adoption de nouvelles technologies de détection et réponse aux points terminaux est passée de 34,2 % en 2022 à 58,2 % en 2025, soit une augmentation de 24 %. Les organisations semblent donc se concentrer sur la détection et la réponse des points terminaux.
- La gestion d'information de sécurité et d'incident est restée relativement stable et n'a augmenté que de 1,9 % entre 2022 (51,9 %) et 2025 (53,8 %). Sa courbe d'adoption est plus lente que pour la détection et réponse aux points terminaux et la détection et réponse étendues.

Graphique 21 : taux d'adoption des technologies clés de détection et de réponse



Technologies	2022	2023	2024	2025	Croissance (2022-2025)
Détection et réponse étendues	42,0 %	44,8 %	61,5 %	63,5 %	21,5 %
Détection et réponse aux points terminaux	34,2 %	39,1 %	56,1 %	58,2 %	24,0 %
Orchestration, automatisation et réaction en matière de sécurité	44,1 %	45,9 %	49,2 %	50,6 %	6,5 %
Gestion d'information de sécurité et d'incident	51,9 %	53,5 %	51,8 %	53,8 %	1,9 %

Conclusion

L'amélioration continue des temps de détection, de réponse et de récupération des organisations canadiennes témoigne de leur capacités à gérer les cybermenaces de plus en plus efficacement. L'adoption de la détection et réponse étendues et de la détection et réponse aux points terminaux y a joué un rôle essentiel. Elle permet aux organisations de détecter les menaces et d'y répondre plus rapidement qu'auparavant. Toutefois, l'écart croissant entre les grandes et les petites organisations révèle une inégalité dans leurs capacités à faire face aux cybermenaces. Pour combler ce fossé, les petites organisations doivent investir dans les technologies de sécurité modernes et améliorer leur réponse en cas d'incident. En assurant la maturité de la cybersécurité et en tirant parti de l'automatisation, les organisations canadiennes peuvent atténuer davantage les menaces, réduire les temps d'indisponibilité et améliorer la cyberrésilience dans son ensemble.

Principale constatation 4

Les défis du modèle à vérification systématique : entre théorie et pratique

Les organisations canadiennes ont des difficultés à tirer parti des stratégies et des évaluations pour progresser

Le modèle à vérification systématique est devenu la pierre angulaire des stratégies modernes de cybersécurité. Son principe : « ne jamais faire confiance, toujours vérifier ». Son adoption a pris de l'ampleur au sein des organisations canadiennes, mais la mise en œuvre de cette politique reste un défi de taille. Selon les résultats de l'enquête, de nombreuses organisations ont du mal à transformer les modèles à vérification systématique de haut niveau et les évaluations de maturité en mesures concrètes permettant de réaliser des progrès tangibles. Ce décalage crée des lacunes critiques dans l'architecture de sécurité et va à l'encontre des principes mêmes du modèle à vérification systématique.

La mise en œuvre du modèle à vérification systématique présente des défis

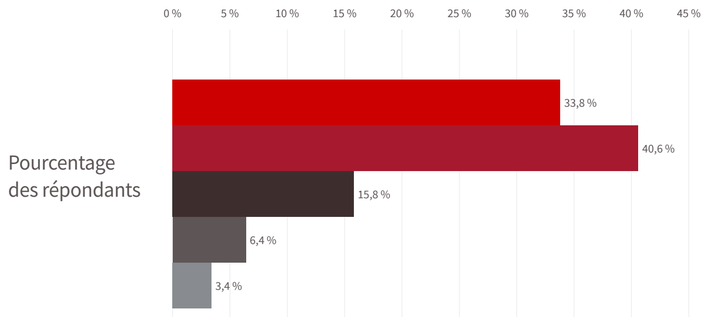
Difficultés à mettre en place des stratégies

Une grande partie des organisations éprouvent des difficultés à combler le fossé entre la stratégie et la mise en œuvre. Les évaluations ne permettent pas de définir des initiatives politiques, techniques ou procédurières claires. En conséquence, les équipes de sécurité ne savent pas comment exécuter le modèle à vérification systématique. Le décalage entre les équipes stratégiques et les équipes opérationnelles est souvent causé par des contraintes de ressources, d'autres priorités et un manque de compréhension commune des risques commerciaux. Ces défis peuvent ralentir la mise en œuvre des initiatives de sécurité et empêcher de lutter efficacement contre les vulnérabilités.

Transformer les idées en concepts tangibles

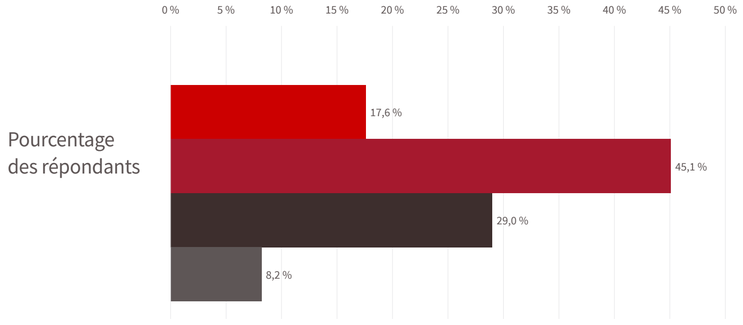
D'après les résultats de l'étude, 63 % des organisations canadiennes ont du mal à transformer les modèles à vérification systématique de haut niveau en exigences techniques réalisables (graphique 22). En outre, même si 37 % des organisations évaluent la maturité de leur modèle à vérification systématique, elles jugent les rapports qui en résultent peu pratiques ou trop abstraits pour agir, tandis que 45 % déclarent que certaines parties des rapports sont utiles, mais nécessitent des efforts supplémentaires pour être pleinement transformées en exigences techniques (graphique 23). Ce décalage crée des lacunes critiques dans l'architecture de sécurité et va à l'encontre des principes mêmes du modèle à vérification systématique.

Graphique 22 : mise en œuvre du modèle à vérification systématique



- Extrêmement efficace : nous avons une feuille de route claire et documentée de la stratégie à la mise en œuvre.
- Très efficace : nous avons des lignes directrices générales, mais la traduction technique n'est pas uniforme d'un département à l'autre.
- Peu efficace : nous avons du mal à adapter les objectifs stratégiques aux exigences techniques spécifiques.
- Pas efficace : il y a un décalage important entre la stratégie et l'exécution.
- Nous n'avons pas adopté de modèle à vérification systématique

Graphique 23 : mise en œuvre après évaluation de la maturité de la cybersécurité



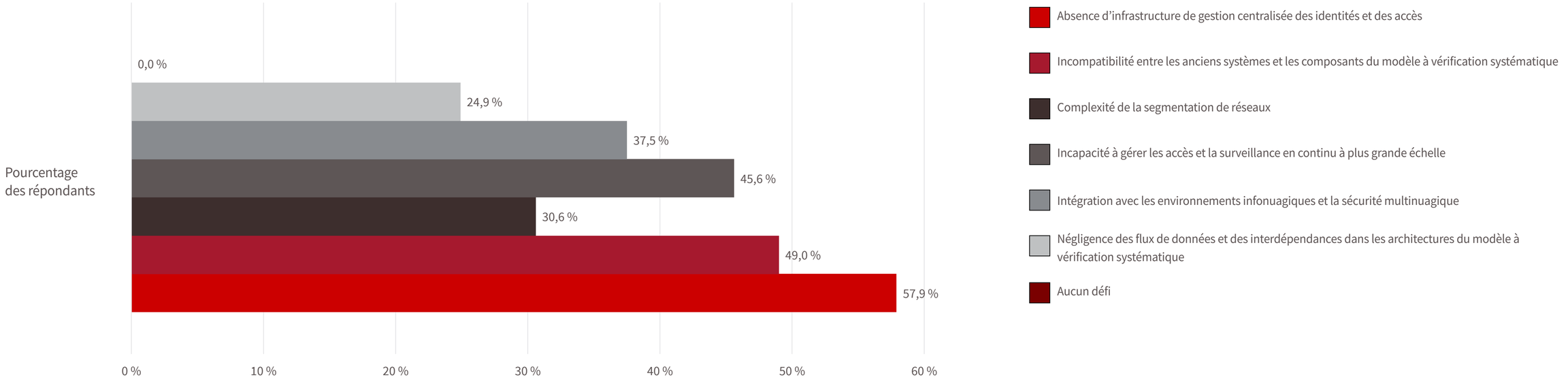
- Très efficace : le rapport indique directement les mesures à prendre pour l'équipe des TI.
- Modérément efficace : nous pouvons utiliser certaines parties du rapport, mais des discussions internes sont nécessaires.
- Peu efficace : le rapport fournit des conseils détaillés, mais nous avons du mal à mettre en œuvre des recommandations particulières.
- Pas efficace : le rapport est souvent mis de côté, car il manque d'applications pratiques pour nos équipes techniques.

Modèle à vérification systématique : les défis architecturaux

Les obstacles architecturaux représentent un autre frein majeur à la mise en œuvre du modèle à vérification systématique (graphique 24). Les principaux défis comprennent :

- Gestion des identités et des accès (IAM) : pour 58 % des répondants, les systèmes inadaptés de gestion des identités et des accès sont une préoccupation majeure, car ils empêchent d'appliquer efficacement les principes du modèle à vérification systématique.
- Intégration avec les systèmes existants : les environnements de TI hybrides compliquent l'intégration des solutions modernes du modèle à vérification systématique : 49 % des organisations considèrent qu'il s'agit d'un obstacle important.
- Problème de mise à l'échelle : l'extension des principes du modèle à vérification systématique à divers systèmes et zones géographiques pose des problèmes à 46 % des organisations, ce qui complique encore leurs efforts de mise en œuvre.

Graphique 24 : défis architecturaux lors de la mise en œuvre du modèle à vérification systématique



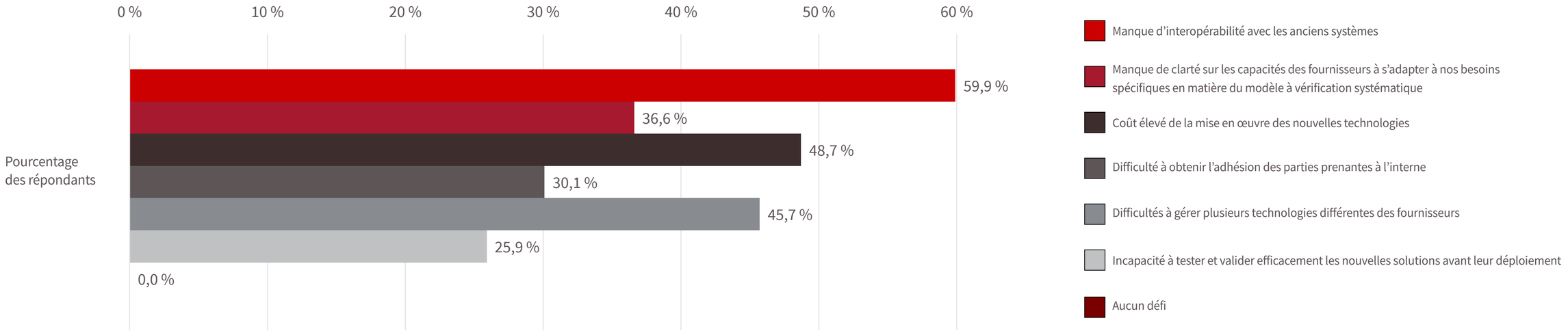
Nouvel appareil, mêmes problèmes : l'adoption de nouvelles technologies

Les organisations sont confrontées à d'autres obstacles dans la mise en œuvre de la structure technique du modèle à vérification systématique. L'étude met en évidence plusieurs préoccupations majeures (graphique 25) :

- Manque d'interopérabilité avec les anciens systèmes
- Coûts élevés associés aux nouvelles solutions
- Difficultés à gérer plusieurs technologies de différents fournisseurs

Ces défis compliquent l'intégration des principes du modèle à vérification systématique dans les environnements de TI existants, ce qui ralentit les progrès et accroît la pression opérationnelle.

Graphique 25 : défis liés à l'adoption de nouvelles technologies dans le cadre du modèle à vérification systématique

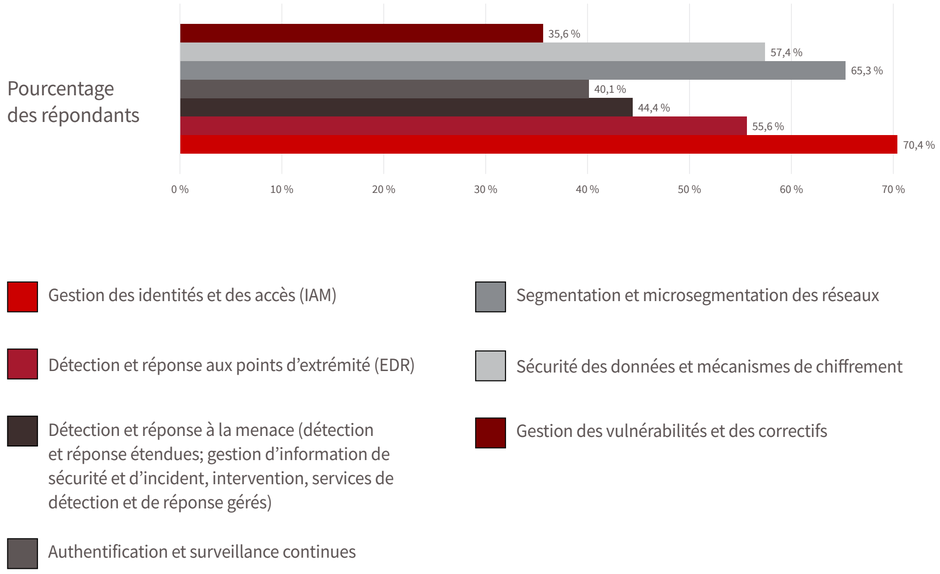


Cybersécurité : adopter une stratégie personnalisée pour progresser

Le modèle à vérification systématique doit être adapté aux besoins spécifiques d'une organisation et prendre en compte sa structure organisationnelle, son environnement de TI et ses exigences en matière de conformité. Pour réaliser des progrès significatifs, les organisations doivent personnaliser leurs initiatives du modèle à vérification systématique afin de les aligner sur leurs objectifs et profils de risque. Les principaux aspects qui doivent être personnalisés comprennent (graphique 26) :

- **Gestion des identités et des accès (IAM) :** les organisations ont besoin de politiques d'accès granulaires et de mécanismes d'authentification adaptés à leurs environnements.
- **Segmentation et microsegmentation des réseaux :** les organisations ont des difficultés à mettre en œuvre la microsegmentation sans interrompre les flux de travail existants.
- **Chiffrement et sécurité des données :** les différents environnements de données entre les organisations exigent des flux de travail personnalisés pour protéger les renseignements sensibles.
- **Gestion des correctifs :** des solutions sur mesure permettent de garantir des mises à jour en temps réel et une gestion proactive des vulnérabilités.

Graphique 26 : composants du modèle à vérification systématique qui nécessitent le plus de personnalisation



Ces domaines mettent en évidence le besoin de trouver des solutions ciblées qui s'adaptent à chaque organisation tout en respectant les principes de vérification systématique.

Conclusion

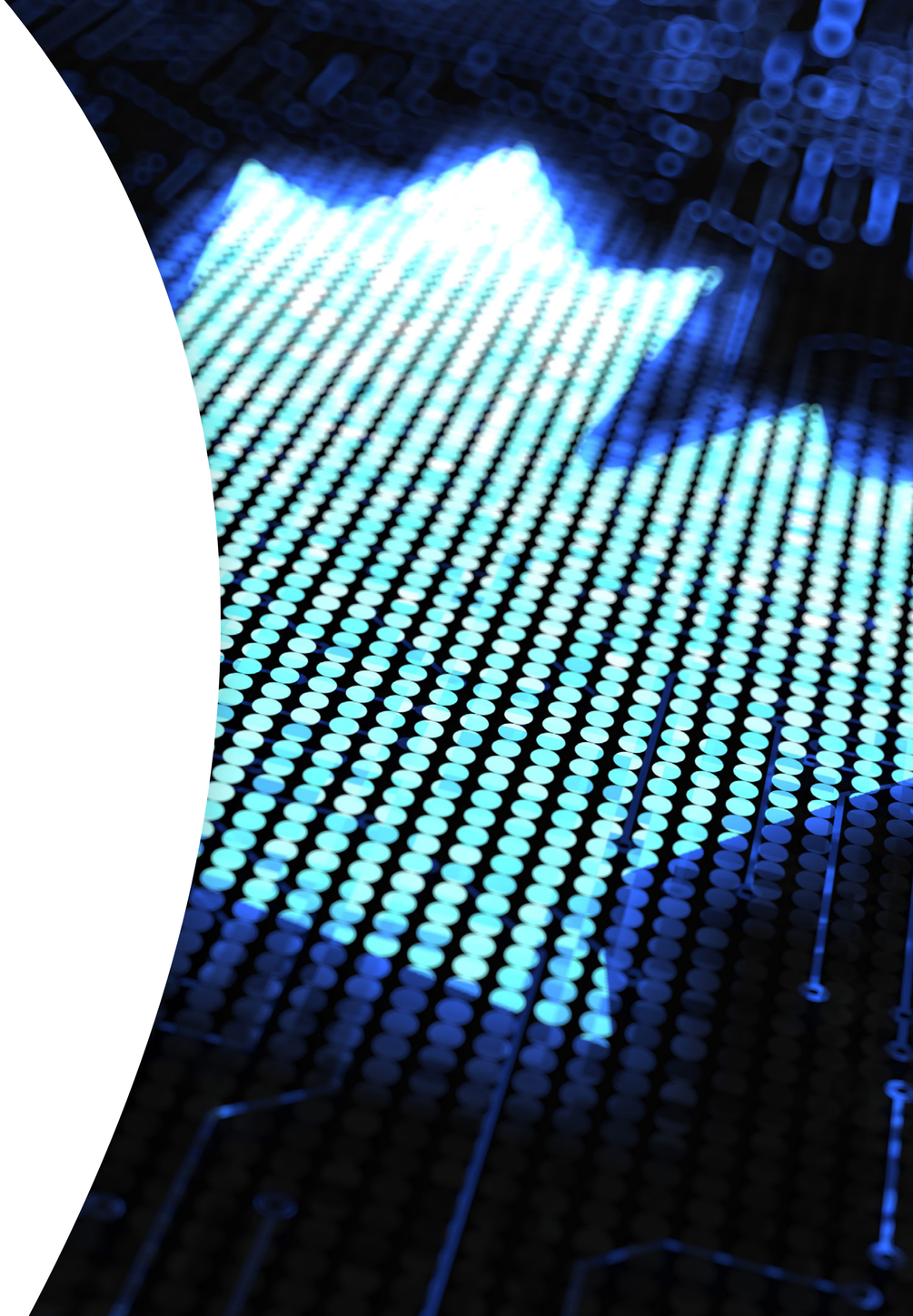
Les organisations ne sont pas obligées d'adopter des principes du modèle à vérification systématique, mais celles qui le font améliorent leur sécurité. Nous constatons également que celles qui peinent à la mettre en œuvre deviennent vulnérables aux cybermenaces et aux inefficacités opérationnelles. Les lacunes dans des domaines comme la gestion des identités, la segmentation du réseau et la gestion des correctifs augmentent les risques de sécurité, tandis que les difficultés à adopter de nouvelles technologies et à gérer la complexité des fournisseurs ralentissent les progrès. Le paysage technologique fragmenté et le manque de conseils pratiques amplifient ces problèmes. Il est donc essentiel de collaborer avec les fournisseurs et trouver des solutions sur mesure. Il faut combler ces lacunes pour que les organisations améliorent leur position en matière de cybersécurité et profitent pleinement des avantages du modèle à vérification systématique.

Principale constatation 5

Prévenir les atteintes à la sécurité et accélérer les réponses

Les organisations canadiennes se tournent vers les fournisseurs pour améliorer la détection des menaces et les réponses

Les services de détection et de réponse gérés (DRG) sont devenus la pierre angulaire des stratégies de cybersécurité des organisations canadiennes. Face à l'évolution des cybermenaces et à la pression croissante exercée sur les équipes de sécurité internes, les entreprises recherchent des solutions gérées et proactives pour améliorer leurs capacités de détection, de réponse et de récupération. L'étude révèle que 41 % des organisations canadiennes ont déjà adopté les services de DRG, tandis que 37 % prévoient de le faire prochainement. Ils représentent donc une valeur ajoutée aux programmes de sécurité.



Facteurs clés de l’adoption des services de DRG

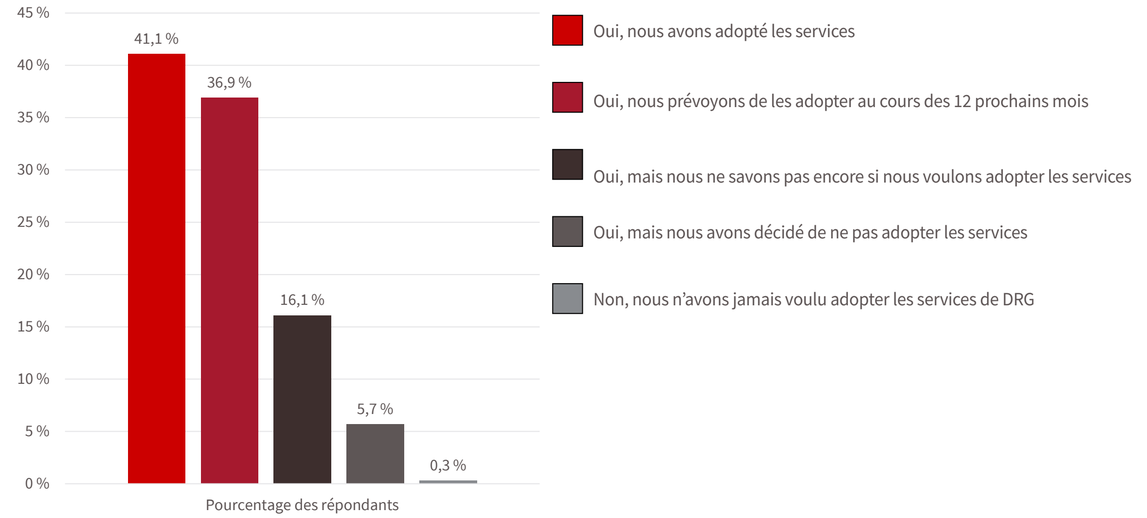
Les organisations se tournent de plus en plus vers les services de DRG pour renforcer leur sécurité. Voici les trois principales raisons pour lesquelles ces services sont adoptés :

- Prévenir et atténuer les atteintes à la sécurité
- Améliorer le temps de réponse aux incidents
- Améliorer la visibilité des menaces et les rapports

En plus de ces facteurs clés, d’autres éléments poussent les organisations à adopter des services de DRG :

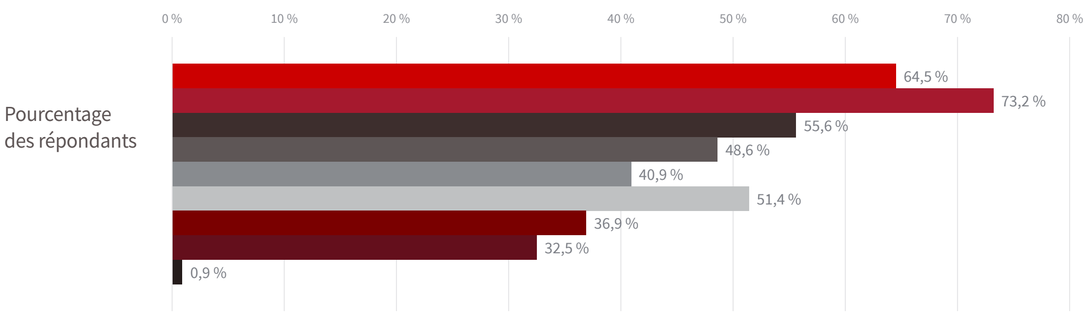
- Assurer la conformité et l’harmonisation de la réglementation
- Réduire la charge de travail opérationnelle des équipes internes
- Améliorer la sécurité en continu

Graphique 27 : taux d’adoption des services de DRG par les organisations canadiennes



Il est intéressant de noter que les économies de coûts ne figurent pas parmi les cinq principales raisons. Les organisations canadiennes privilégient ainsi les résultats et la résilience en matière de sécurité plutôt que la réduction des coûts lorsqu’elles évaluent les services de détection et réponse gérés. Il s’agit d’une approche axée sur la valeur, qui met l’accent sur une sécurité plus efficace plutôt que sur des économies financières à court terme.

Graphique 28 : raisons pour lesquelles les services de DRG ont été adoptés



Le rôle de la technologie et de la surveillance humaine

Tirer parti de l'IA générative pour répondre à la pénurie de compétences

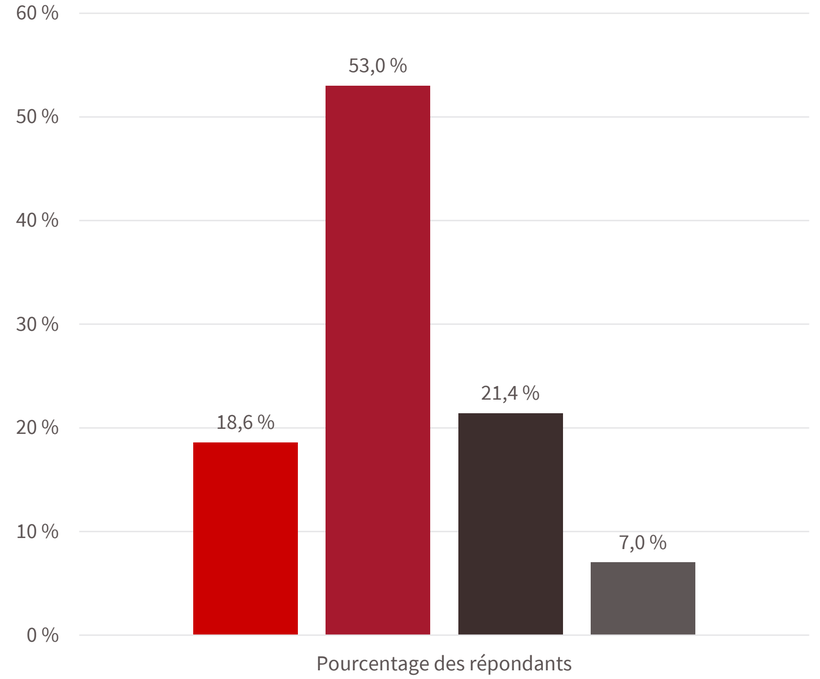
De plus en plus, les fournisseurs de services de détection et réponse gérés intègrent l'automatisation alimentée par l'IA générative afin de réduire leur dépendance vis-à-vis des équipes de sécurité internes. Cette solution permet de répondre à la pénurie actuelle de main-d'œuvre en cybersécurité. Les outils alimentés par l'IA permettent :

- de détecter des menaces et d'y répondre plus rapidement grâce à l'automatisation des processus clés;
- de prendre des mesures correctives plus efficaces grâce à l'analyse prédictive et à la gestion des incidents fondée sur l'IA;
- de réduire la charge de travail manuelle des analystes de la sécurité pour leur permettre de se concentrer sur les menaces à priorité élevée.

La surveillance humaine reste essentielle

Malgré les avancées en matière de détection des menaces alimentée par l'IA, l'expertise humaine reste essentielle dans les opérations de cybersécurité. L'étude révèle que 53 % des répondants estiment que même si l'IA générative a stimulé l'automatisation, la supervision humaine reste nécessaire pour la majorité des tâches. Les professionnels de la sécurité fournissent :

- une analyse contextuelle des menaces que l'IA ne peut pas entièrement interpréter;
- une validation des alertes pilotées par l'IA pour réduire les faux positifs;
- une prise de décision stratégique pour répondre aux incidents et gérer les risques.



Graphique 29 : amélioration de l'hyper-automatisation et réduction de la dépendance à la main-d'œuvre humaine grâce à l'IA générative

Totale : nous avons considérablement réduit l'intervention humaine pour les tâches de sécurité de routine

Partielle : l'automatisation a augmenté, mais la surveillance humaine reste nécessaire pour la plupart des tâches

Légère

Aucune

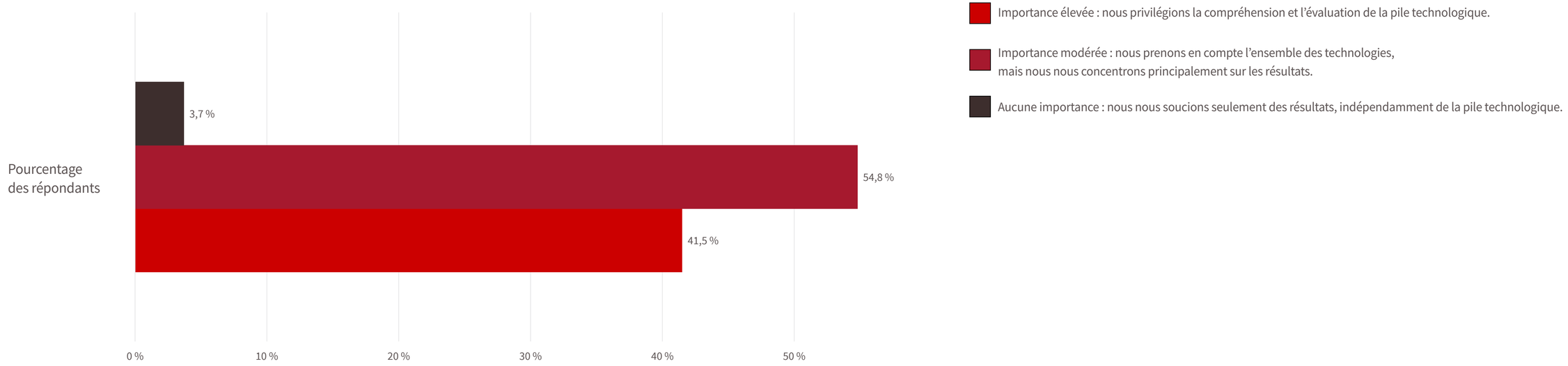
Privilégier les résultats aux piles technologiques

Alors que les fournisseurs de détection et réponse gérés s'appuient sur diverses technologies comme la gestion d'information de sécurité et d'incident, la détection et réponse aux points terminaux et la détection et réponse étendues, les organisations privilégient les résultats des services plutôt que les piles technologiques spécifiques. Près de 55 % des répondants déclarent que si la pile technologique est examinée, elle n'est pas le principal facteur de décision. Les facteurs les plus importants sont les suivants :

- Réduction des risques
- Rapidité de détection et réponse en cas de menace
- Amélioration globale de la sécurité

Seulement 41,5 % des répondants considèrent la pile technologique comme un facteur clé dans le choix d'un fournisseur de services de détection et réponse gérés. La qualité du service est donc de plus en plus privilégiée par rapport aux outils spécifiques.

Graphique 30 : importance de la pile de technologies dans le choix du fournisseur de DRG



Mesurer l’efficacité des services de DRG

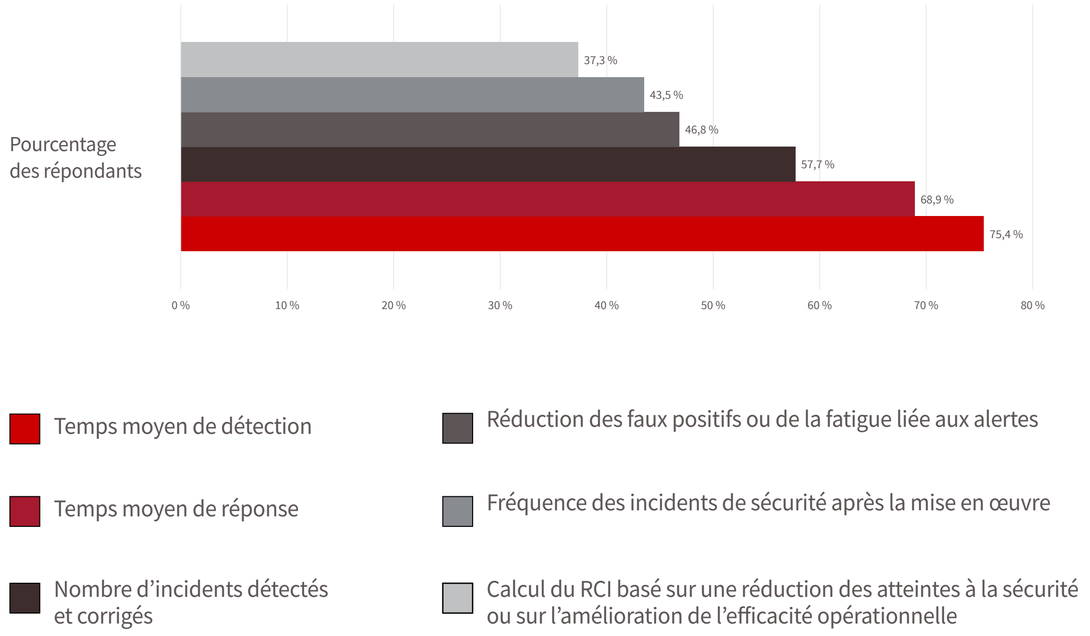
Les organisations utilisent plusieurs indicateurs de performance clés pour évaluer l’efficacité d’un service de détection et réponse gérés. Les trois principales mesures comprennent :

- le temps moyen de détection : mesure la rapidité avec laquelle les menaces sont identifiées;
- le temps moyen de réponse : mesure la rapidité avec laquelle un incident est maîtrisé et résolu;
- le nombre d’incidents détectés et corrigés : évalue l’impact des services de détection et réponse gérés sur la prévention des menaces.

Les autres mesures secondaires utilisées par les organisations comprennent :

- la réduction de la fatigue liée aux alertes, car les services de DRG aident les équipes de sécurité à gérer un nombre important d’alertes de sécurité;
- la fréquence des incidents avant et après l’adoption des services de DRG, qui permet de constater des améliorations.

Graphique 31 : mesures utilisées par les organisations canadiennes pour évaluer l’efficacité du service de DRG



Conclusion

L’adoption croissante des services de détection et réponse gérés reflète un changement stratégique chez les organisations canadiennes, qui souhaitent renforcer leurs capacités de sécurité et faire face aux contraintes de ressources. Les organisations canadiennes espèrent qu’en intégrant l’IA générative, les services de détection et réponse gérés amélioreront la vitesse de détection et de réponse en cas de menace pour atténuer les risques de manière plus efficace. Toutefois, la supervision humaine reste cruciale pour garantir l’exactitude, le contexte et la fiabilité des alertes, en particulier lors du traitement d’incidents de sécurité complexes. L’évolution vers des évaluations axées sur les résultats plutôt que sur les piles technologiques démontre que les organisations privilégient la qualité des services et les améliorations mesurables aux spécifications techniques. Cette combinaison de technologies avancées, de mesures stratégiques et d’opérations de sécurité menées par des experts font des services de détection et réponse gérés un outil essentiel pour assurer la maturité des programmes de cybersécurité au Canada.

Étude sur la sécurité au Canada

Recommandations

Vérification systématique, aucune excuse : transformer la stratégie en action

Le modèle à vérification systématique est devenu une stratégie fondamentale de la cybersécurité, mais de nombreuses organisations peinent à la mettre en œuvre de manière efficace. Même en évaluant la maturité du modèle à vérification systématique, les organisations trouvent souvent les résultats trop abstraits pour savoir comment la mettre en œuvre, et les équipes de sécurité n'ont pas de feuille de route claire. Les contraintes liées aux systèmes existants et le manque d'expertise pratique ralentissent encore les progrès, et le modèle à vérification systématique devient une ambition plutôt qu'un projet réalisable. Pour combler le fossé entre la stratégie et l'exécution, les organisations ont besoin d'une approche structurée et systématique qui transforme les principes du modèle à vérification systématique en améliorations mesurables.

Conseils essentiels :

- **Créer un modèle de l'état final :** établissez un cadre de vérification systématique clair avec des contrôles de sécurité adaptés aux priorités de l'entreprise et une gestion des risques adaptée aux besoins opérationnels. Il servira de base à la mise en œuvre.
- **Établir des feuilles de route claires :** convertissez les stratégies de vérification systématique en plans d'action étape par étape, en attribuant des responsabilités et des objectifs clairs aux équipes de sécurité pour qu'elles atteignent l'état final prévu.
- **Classer les données et les applications :** fournissez un aperçu des données en montrant la façon dont elles sont présentées aux utilisateurs (au moyen d'applications). Cette méthode permet de créer une stratégie claire de contrôle d'accès à base de rôles (RBAC) pour la fourniture d'informations ponctuelle et pour la mise en place d'un processus de validation de vérification systématique.
- **Vérifier la compatibilité des systèmes :** identifiez les limites des systèmes existants qui entravent la mise en œuvre de la vérification systématique et créez un contrôle compensatoire ou une feuille de route d'intégration avec les solutions prises en charge par les fournisseurs.
- **Tirer parti des solutions IAM :** déployez des contrôles adaptatifs de gestion des identités et des accès (IAM) qui permettent des restrictions d'accès granulaires et contextuelles alignées sur les principes de vérification systématique, y compris le RBAC.
- **Développer les compétences des équipes de sécurité :** proposez une formation pratique aux équipes de sécurité sur les mécanismes d'application du modèle à vérification systématique, y compris la microsegmentation, l'authentification continue et le contrôle d'accès basé sur des politiques concernant les données, les applications, le réseau, les appareils et les piliers de l'identité dans l'organisation.

L'approche du modèle à vérification systématique doit aller au-delà d'un cadre théorique : il doit également être un modèle de sécurité pratique qui nécessite une exécution structurée et une adaptation continue. Les organisations qui se concentrent sur la mise en œuvre, la formation et la préparation de l'infrastructure adopteront une approche de la sécurité axée sur le modèle à vérification systématique.

Tests d’intrusion : se protéger en continu de manière proactive

Les tests de sécurité annuels ont prouvé leur efficacité dans la réduction des risques d’intrusion, mais les organisations réalisent aujourd’hui que ces vérifications ponctuelles ne suffisent plus. Face à l’évolution des cybermenaces, une validation continue est nécessaire pour détecter les vulnérabilités et y remédier en temps réel. Les environnements infonuagiques, en particulier, possèdent des architectures dynamiques et partagées, qui nécessitent des méthodologies de test spécifiques. En automatisant les tests d’intrusion, en les intégrant dans les pipelines de développement et en exploitant des outils de test de sécurité infonuagiques, les organisations pourront transformer leurs évaluations réactives en protection proactive.

Conseils essentiels

- Automatiser les processus d’essai : mettez en œuvre des cadres de tests de sécurité continus qui intègrent des analyses automatisées des vulnérabilités, des équipes rouges et des simulations d’attaques dans les opérations de sécurité de routine.
- Valider les contrôles de cybersécurité et la détection : allez au-delà des tests d’intrusion traditionnels et adoptez des approches de test de sécurité infonuagiques natives qui prennent en compte les fonctions sans serveur, le stockage d’objets et de secrets, la sécurité des API et les charges de travail conteneurisées.
- Intégrer les tests au développement : intégrez les tests de sécurité aux pipelines d’intégration et de livraison continues, en veillant à ce que chaque déploiement de logiciels fasse l’objet d’une évaluation automatisée des vulnérabilités avant la production.
- Valider les contrôles grâce à des exercices avec l’équipe violette : effectuez des missions collaboratives avec l’équipe violette pour tester et valider activement les outils de détection, les contrôles de sécurité et les plans d’intervention en cas d’incident. Ce processus garantit que votre technologie est correctement configurée, que votre personnel peut utiliser efficacement les solutions de sécurité et que vos opérations de sécurité sont prêtes à répondre efficacement aux incidents réels.
- Collaborer avec les fournisseurs de sécurité : travaillez avec des entreprises de sécurité spécialisées ou des fournisseurs de détection et réponse gérés qui proposent des tests d’intrusion à la demande, une équipe rouge et une gestion de la surface d’attaque adaptée à l’évolution des menaces.

Les tests de sécurité doivent faire partie d’un processus continu et automatisé qui évolue en même temps que les cybermenaces. En intégrant ces tests dans les opérations informatiques quotidiennes, les organisations peuvent anticiper les attaques et renforcer leurs défenses en temps réel.

Du chaos à l'ordre : comment les programmes de sécurité matures facilitent l'IA

Les initiatives d'IA générative commencent généralement au stade de validation de principe, ce qui permet aux organisations de relever les défis en matière de sécurité, d'intégration et d'exploitation de manière proactive. Plutôt que de considérer cette phase comme un obstacle, les organisations devraient en tirer parti pour résoudre des problèmes fondamentaux comme la dette de sécurité, la complexité de l'intégration et la pénurie de compétences. Pour relever ces défis, il est nécessaire d'accélérer l'adoption de la technologie d'IA générative, mais aussi de renforcer considérablement la posture de cybersécurité et la résilience organisationnelle.

Conseils essentiels

- Résoudre rapidement la dette de sécurité : privilégiez les pratiques de sécurité fondamentales, y compris la visibilité des actifs, la gestion des vulnérabilités et une solide gouvernance des données, pour vous assurer que les initiatives d'IA reposent sur une infrastructure sûre et fiable. Si la dette de sécurité est maîtrisée de manière proactive, vous pourrez réduire les risques dans l'ensemble de l'organisation, et pas seulement dans les projets d'IA.
- Adopter des stratégies qui protègent les renseignements personnels : appliquez des méthodes d'apprentissage fédérées, de confidentialité différentielle ou de chiffrement pendant l'entraînement de l'IA afin de protéger les données sensibles. Ces approches réduisent les risques d'exposition des données et renforcent la protection de la vie privée dans tous les processus fondés sur les données.
- Investir dans des programmes de formation complets : élaborez des programmes structurés d'amélioration des compétences sur l'IA et la cybersécurité pour les équipes, en mettant l'accent sur la gouvernance des modèles d'IA, le traitement sécurisé des données, le déploiement éthique de l'IA et la détection des menaces. Cet ensemble de compétences plus large est bénéfique à la sécurité organisationnelle au-delà des initiatives d'IA.
- Simplifier l'intégration du flux de travail : établissez un partenariat étroit avec les fournisseurs d'IA et de cybersécurité afin d'intégrer les nouveaux outils de manière transparente dans les flux de travail existants, en minimisant les perturbations et en augmentant l'efficacité opérationnelle dans l'ensemble de l'organisation.
- Privilégier la qualité des données : mettez en place des mesures strictes de gouvernance des données afin de garantir l'exactitude, l'intégrité et l'atténuation des biais dans les données d'entraînement. Les données de haute qualité améliorent la prise de décision, réduisent les incidents de sécurité et améliorent la fiabilité de l'IA.

Pour passer avec succès la phase de validation de principe de l'IA générative et atteindre celle du déploiement à grande échelle, il est important de résoudre les problèmes plus généraux de sécurité et d'intégration de l'organisation. En privilégiant la sécurité des fondations et l'excellence opérationnelle, les organisations pourront non seulement libérer le potentiel de l'IA, mais aussi améliorer durablement leurs capacités globales en matière de cybersécurité et de gestion des risques.

L’avantage des services de DRG : une détection plus rapide, une réponse plus intelligente, une sécurité améliorée

Les services de détection et de réponse gérées (DRG) deviennent un investissement essentiel dans la sécurité des organisations canadiennes, car ils permettent d’améliorer la détection des menaces, la réponse aux incidents et l’automatisation de la sécurité. L’adoption des services de DRG ne dépend pas de la technologie, mais des résultats : les organisations privilégient la réduction des risques, l’atténuation plus rapide des menaces et l’amélioration des indicateurs clés de sécurité plutôt que des outils spécifiques utilisés par les fournisseurs de services de DRG. En outre, l’intégration de l’IA générative aux services de DRG a considérablement amélioré leur efficacité, mais la supervision humaine reste essentielle pour garantir la précision et la prise de décision en contexte dans les opérations de cybersécurité.

Conseils essentiels

- Privilégier les IRC : choisissez les fournisseurs de DRG en fonction de leur capacité à améliorer le temps moyen de détection, le temps moyen de réponse et la réduction globale des incidents, plutôt que sur la base de technologies spécifiques.
- Miser sur les technologies de pointe : choisissez des fournisseurs de DRG qui intègrent l’IA générative, l’apprentissage automatique et l’analyse automatisée des menaces pour accélérer la détection et la réponse aux menaces, tout en assurant une supervision humaine pour les prises de décision complexes.
- Se conformer aux exigences : assurez-vous que les services de DRG comprennent des caractéristiques intégrées de conformité réglementaire, des capacités d’établissement de rapports de vérification et une gouvernance complète de la sécurité afin de répondre aux exigences industrielles et légales.
- Intégrer la réponse aux incidents : choisissez des fournisseurs de DRG qui offrent des capacités intégrées de réponse aux incidents ou qui travaillent en étroite collaboration avec des spécialistes en réponse aux incidents. Ils permettent de répondre rapidement et de manière coordonnée aux incidents de sécurité critiques, de réduire les temps d’indisponibilité et d’améliorer le temps de récupération.
- Examiner et optimiser les performances régulièrement : évaluez en permanence les performances des fournisseurs de DRG, procédez à des examens trimestriels de la sécurité et affinez les stratégies de détection et de réponse grâce aux renseignements en temps réel sur les menaces.

Les services de DRG allègent la charge de travail des équipes de cybersécurité, comblent les lacunes de compétences, automatisent la réponse aux menaces et améliorent les opérations de sécurité. En choisissant des solutions de DRG fondées sur les résultats de sécurité, l’alignement réglementaire et les efficacités basées sur l’IA, les organisations peuvent améliorer considérablement leur capacité à détecter et à atténuer les menaces à l’échelle.

Annexe A : Résultats détaillés de l'étude

Statistiques démographiques : Un échantillonnage de 8 748 professionnels canadiens spécialisés dans la sécurité informatique et dans les risques et la conformité a été sélectionné pour recevoir une invitation à participer à cette étude. Tous les participants à l'étude ont fait l'objet d'une sélection pour leur contribution directe à l'amélioration ou à la gestion de la sécurité informatique de leur organisation. Le tableau suivant présente les résultats, y compris la suppression de certains participants sur la base des contrôles de sélection et de fiabilité. L'échantillon final était composé de 704 répondants, soit un taux de réponse de 8 %. Voici les données firmographiques et démographiques de l'étude :

Laquelle des catégories de secteur suivantes représente le mieux l'activité principale de votre organisation?

	%
Services commerciaux/professionnels (p. ex., avocat, comptable, ingénieur, architecte, etc.)	2,6
Services personnels/pour consommateur (p. ex., voyages, beauté, entraînement personnel, nettoyage à sec, etc.)	1,8
Construction	3,1
Hôtellerie	2,8
Informatique	5,4
Sans but lucratif	0,0
Fabrication	5,8
Société d'État ou autre organisme financé par l'État	0,3
Enseignement (maternelle à 12e année)	5,8
Enseignement collégial/universitaire	9,7
Services financiers	8,7

	%
Gouvernement	14,2
Soins de santé	14,3
Secteur primaire (p. ex., agriculture, mines, foresterie, etc.)	1,1
Pétrole et gaz ou services liés à l'exploitation	4,0
Secteur du détail	6,0
Communications (p. ex., câble et services de télécommunications, etc.)	2,0
Médias (p. ex., radio/télédiffusion)	2,0
Impression, édition, etc.	1,0
Transports et entreposage	3,1
Services publics	3,4
Vente en gros et distribution	2,8

Le siège social de votre organisation est-il situé au Canada, et dans ce cas, dans laquelle des régions suivantes se trouve-t-il?

	%
Pas de siège social au Canada	4,0
Ouest et Centre du Canada (C.-B. Alb., Sask., Man.)	15,9
Ontario	30,3
Québec	25,1
Canada atlantique (N.-B., N.-É., T.-N.-L., Î.-P.-É.)	16,8
Nord (Yukon/Territoires du Nord-Ouest/Nunavut)	8,0

Dans votre organisation, jouez-vous un rôle ou intervenez-vous dans les fonctions suivantes?

	%
La direction de la fonction informatique	38,2
L'amélioration/la gestion de la sécurité informatique	100,0
L'établissement des priorités des TI	43,5
La gestion des budgets des TI	41,3

Lequel des énoncés suivants décrit le mieux le service où vous travaillez?

	%
Direction générale niveau C sauf TI	9,8
Gestion de secteur d'activité sauf TI	4,0
Cadre supérieur des TI, y compris le directeur des systèmes d'information/directeur des techniques informatiques/chef de sécurité d'entreprise/chef de la sécurité de l'information, etc.	7,2
Finance/Comptabilité	5,0
TI/Systèmes d'information/Systèmes d'information de gestion/Centre de traitement des données/Sécurité informatique	63,1
Juridique/conformité/risque	10,9

Notre mission est d’utiliser la technologie de façon à permettre aux gens de réaliser de grandes choses.

CDW Canada Corp. est un chef de file parmi les fournisseurs de services et de solutions technologiques pour les entreprises, le gouvernement, le milieu de l’enseignement et celui des soins de santé. Créé en 2003, CDW Canada est le conseiller de confiance du Canada en matière de cybersécurité, d’infrastructure hybride et de transformation numérique. Les experts de CDW Canada conçoivent, orchestrent et gèrent des services et des solutions sur mesure. Leur mission est d’utiliser la technologie de façon à permettre aux gens de réaliser de grandes choses. Grâce à son approche axée sur les services, CDW Canada simplifie les technologies complexes pour permettre à ses clients de se concentrer sur leurs activités et de prospérer dans un environnement en évolution rapide. CDW Canada est une filiale détenue par CDW Corporation (NASDAQ : CDW), une entreprise figurant au classement Fortune 500.

Pour plus d’informations sur CDW, visitez CDW.ca

International Data Corporation (IDC) est le premier fournisseur mondial de renseignements commerciaux, de données et d’événements sur le marché de la technologie de l’information, des télécommunications et des technologies grand public. Avec plus de 1300 analystes dans le monde, IDC offre une expertise mondiale, régionale et locale sur la technologie et les possibilités de l’industrie dans plus de 110 pays. L’analyse et la vision d’IDC aident les professionnels de l’informatique, les dirigeants d’entreprise et la communauté des investisseurs à prendre des décisions technologiques fondées sur des faits et à atteindre leurs principaux objectifs commerciaux.

Référence du document IDC nº US53206325