Défi simulation de cybermenaces de KPMG au Canada

Les cyberdéfenses de votre organisation vous protégeront-elles? Vous le savez avec certitude?

Les chefs de la direction, les cadres supérieurs et les leaders en cybersécurité et en technologie sont confrontés à des enjeux grandissants liés au maintien de solides postures de cybersécurité, souvent parce que leurs fonctions de sécurité offensives et défensives ne concordent pas. C'est pourquoi les simulations d'adversaire sont si efficaces : elles permettent non seulement de tester les réponses aux intrusions et de signaler les lacunes, elles fournissent également de précieux conseils sur la façon dont les organisations peuvent renforcer leurs cyberdéfenses.

En 2024, KPMG au Canada a lancé son premier Défi simulation de cybermenaces, qui consiste en une simulation gratuite de cyberattaque inspirée d'un exercice de simulation d'adversaire dans un environnement contrôlé, afin d'aider les organisations à évaluer leurs capacités en matière de cybersécurité.

Plus de 150 entreprises de partout au Canada y ont participé, démontrant ainsi l'importance de la cybersécurité pour les chefs d'entreprise d'aujourd'hui et leur vif intérêt à valider leur capacité à détecter les cybermenaces et à y répondre efficacement.

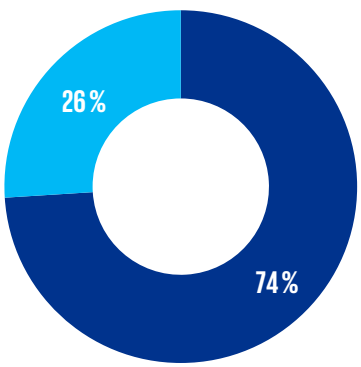
Principale constatation du Défi 2024 : peu d'organisations sont bien préparées

Chaque simulation d'une heure a mis à l'essai de 4 à 7 tactiques réelles fréquemment utilisées dans le cadre de cyberattaques, notamment : système de commande et c ontrôle, recherche, tests d'intrusion, accès aux identifiants, kerberoasting, gestion de la persistance et de l'exécution et test de détection de Rubeus.

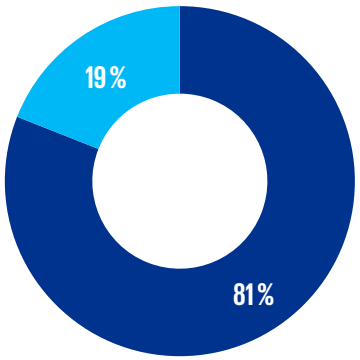
La simulation a mis à l'épreuve les capacités de cybersécurité des organisations en matière de détection et de consignation des attaques et de déclenchement d'aler tes.

Les résultats ont été étonnants.

Détection des attaques



Émission d'alertes



Si les simulations avaient été de véritables intrusions, les attaques seraient probablement passées inaperçues pour la plupart des participants. Les organisations qui ont obtenu de bons résultats lors des simulations disposaient d'une technologie solide pour détecter et consigner les incidents de cybersécurité, ainsi que pour émettre des alertes afin de les traiter le plus efficacement possible.

Certains secteurs ont eu plus de mal que d'autres à détecter les menaces, les services financiers (principalement les petites et moyennes institutions financières), les soins de santé et de bien-être et les aliments et boissons arrivant en tête de liste. Les PME ont également eu tendance à avoir des taux d'échec de détection plus élevés.

Presque tous les participants ont indiqué qu'ils n'avaient pas testé leurs capacités de détection auparavant. Et comme nos recherches indiquent que les fournisseurs de services de sécurité gérés n'effectuent pas souvent d'exercices de simulation d'adversaire dans leur propre environnement, de nombreuses organisations peuvent fonctionner avec des cas d'utilisation de détection inefficaces – et ainsi avoir un faux sentiment de sécurité.

Les exercices de simulation profitent aux entreprises de toutes tailles

On croit à tort que les exercices de simulation d'adversaire sont conçus uniquement pour les grandes organisations. Au contraire, ils sont avantageux pour les entreprises de toutes tailles, surtout lorsque l'étendue et l'approche des exercices correspondent à la maturité, aux ressources et au profil de risque de votre organisation.

Les PME sont de plus en plus vulnérables aux attaques de cybercriminels en raison d'un manque de contrôles rigoureux. Les exercices de simulation d'adversaire aident les PME à détecter les vulnérabilités, à tester les défenses et à améliorer les processus de sécurité de manière rentable. Ils permettent de sensibiliser et de renforcer la culture de sécurité au sein des organisations qui disposent de ressources limitées.

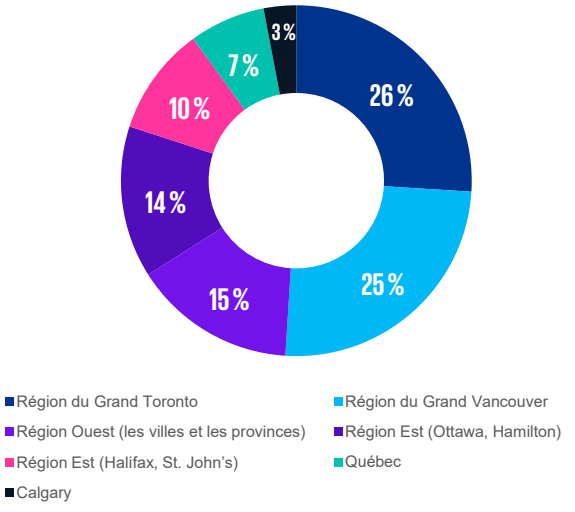
Les entreprises de taille moyenne gèrent des environnements informatiques de plus en plus complexes (p. ex., l'infonuagique, l'Internet des objets, etc.), mais elles peuvent tout de même faire face à des contraintes en matière de ressources. Elles font souvent partie de grandes chaînes d'approvisionnement, ce qui en fait des cibles de choix pour les cyberpirates qui cherchent les infrastructures essentielles ou les associés des entreprises.

Les grandes entreprises sont des cibles de grande valeur en ce qui concerne les menaces persistantes avancées, les rançongiciels et les attaques qui visent l'État. Avec des écosystèmes informatiques complexes et des équipes distribuées, les exercices de simulation d'adversaire assurent la collaboration et la coordination entre leurs équipes offensives et défensives. Ils aident à valider les outils et les stratégies de sécurité, à peaufiner les processus d'intervention en cas d'incident et à s'aligner sur les exigences de conformité.

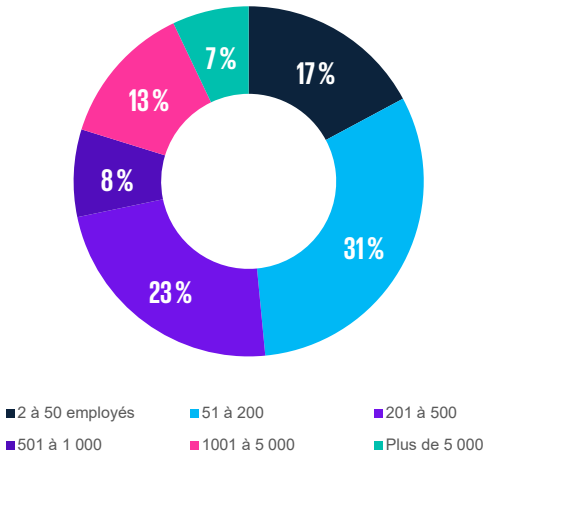
Lorsque les temps d'arrêt ou les intrusions ont des conséquences catastrophiques, y compris des atteintes à la sécurité, des pertes financières et des pertes de réputation, voire des pertes de vie, les exercices de simulation d'adversaire peuvent jouer un rôle clé dans les opérations de cybersécurité de votre organisation, peu importe la taille ou le secteur d'activité.

Défi simulation de cybermenaces de KPMG : les résultats

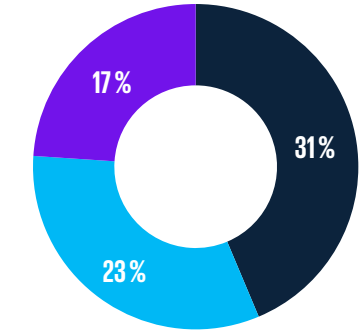
Participants par province en 2024



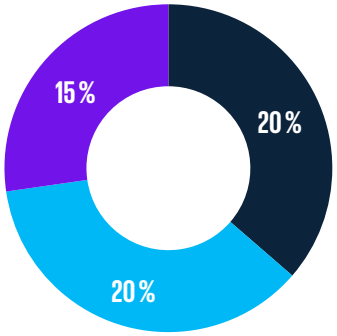
Participants selon la taille de l'entreprise en 2024

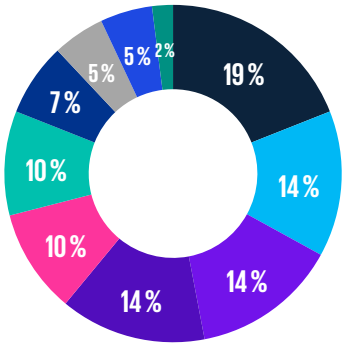


Les trois principaux participants selon la taille de l'entreprise en 2024



Les trois principaux participants par secteur en 2024





Participants par poste en 2024

- Soutien des technologies de l'information
- Administrateurs et haute direction
- Haute direction
- Gestion financière
- Leaders en technologies de l'information
- Administration et conseiller juridique
- Gestion opérationnelle
- Leaders en cybersécurité
- Innovation et développement technologique
- Direction des ventes et du marketing

Vos mesures de cybersécurité vous protégeront-elles? Inscrivez-vous dès maintenant au Défi simulation de cybermenaces 2025 de KPMG au Canada pour découvrir la réponse.

Quelles sont les exigences pour participer au Défi 2025?

Vous aurez besoin d'un ordinateur Windows joint à un domaine qui autorise l'accès Internet sortant, de préférence un ordinateur virtuel qui peut être supprimé par la suite pour vous aider à assurer un nettoyage complet. Vos logiciels de sécurité doivent y être installés et les droits d'administrateur local ne sont pas requis. Il n'y a aucuns frais d'inscription.

Que sera le déroulement du Défi 2025?

1. Après avoir procédé à votre inscription en ligne, vous recevrez un courriel de présentation et un premier appel de notre équipe.
2. Nous vous expliquerons la simulation, répondrons à vos questions, confirmerons la date et les personnes devant être présentes pour l'exercice d'attaque.
3. Nous vous enverrons un fichier Zip qui nous permettra d'exécuter notre maliciel et des commandes précises dans votre environnement. Nous effectuerons la simulation et prendrons note de nos observations. Une fois la simulation terminée, vous pourrez supprimer le maliciel.
4. Par la suite, nous vous fournirons un rapport de nos constatations et organiserons un appel pour en discuter.