KPMG

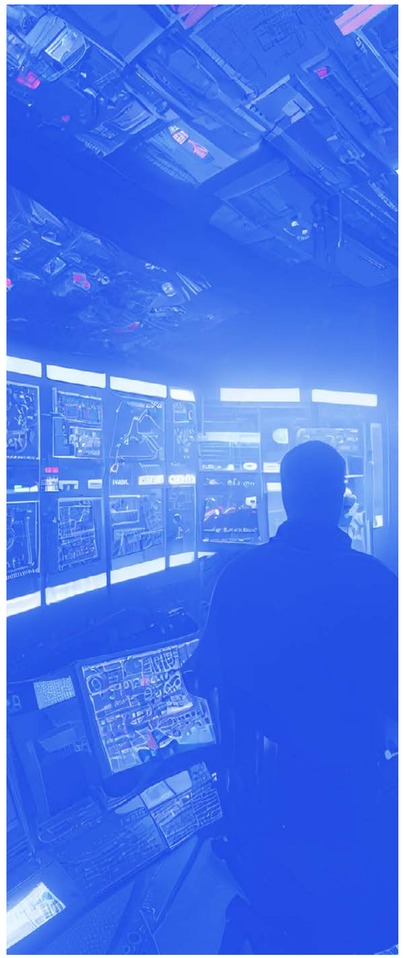
Choisir le fournisseur de service de détection et de réponse gérées qui convient à votre organisation

Table des matières

Introduction

Dans ce monde axé sur la technologie, votre organisation fait face à plus de défis que jamais en matière de protection contre les cyberattaques. La pandémie mondiale, l'explosion du télétravail et la possibilité d'utiliser de multiples appareils pour travailler – personnels et fournis par l'employeur – n'ont fait qu'accroître les risques. Ces facteurs, combinés à l'obligation pour les entreprises de se conformer aux exigences réglementaires mondiales en constante évolution et à une pénurie de talents, compliquent encore plus la situation.

En parallèle, les cybercriminels modernes sont plus créatifs que jamais pour planifier leurs attaques. Les médias abondent en articles concernant des sociétés prestigieuses victimes d'atteintes à la cybersécurité qui compromettent l'information financière, ternissent la réputation, perturbent les transactions en ligne, provoquent des pertes ou interrompent complètement les opérations.



41 % des dirigeants en TI ont signalé une augmentation des incidents liés à la cybersécurité depuis le début de la pandémie[2].

83 % des entreprises disent avoir subi au moins une cyberattaque au cours des 12 derniers mois[3].

Les entreprises sondées ont noté une augmentation de la fréquence des attaques. Parmi les types d'attaques, 44 % ont cité l'hameçonnage, 33 % les escroqueries, 22 % les maliciels et 20 % les rançongiciels[4].

Selon le rapport sur les atteintes à la sécurité des données de l'organisme Identity Theft Resource Center, 1 862 incidents ont eu lieu en 2021, dépassant le nombre 1 108 en 2020 et le précédent record de 1 506 en 2017[1].

Une atteinte réprimée en moins de 200 jours coûte 1 million de dollars de moins qu'une atteinte dont le cycle de vie dépasse les 200 jours[5].

[1]« Data Breach Report », Identity Theft Resource Center, États-Unis, 2021.
[2]Sondage auprès de chefs de l'information, Harvey Nash/KPMG aux États-Unis, 2020.
[3]Rapport de KPMG sur la fraude 2022 – « A Triple Threat Across Americas », KPMG aux États-Unis, 2022.
[4]Ibid.
[5]« Cost of a Data Breach Report », IBM Security, États-Unis, 2020.

Pour se défendre contre les cyberattaques, votre organisation doit continuellement surveiller ses actifs technologiques pour repérer d'éventuelles brèches dans la sécurité, détecter les attaques en temps réel, se défendre efficacement contre ces attaques ou contenir les dommages, et tenter d'anticiper les menaces pour les atténuer avant qu'elles ne se concrétisent.

Le volume des opérations de surveillance quotidienne et le nombre d'outils nécessaires pour garder une longueur d'avance sur les pirates sont élevés et coûteux. En outre, il est de plus en plus difficile pour une organisation de retenir les professionnels qualifiés en cybersécurité, et les équipes en place ont rarement la capacité de surveiller les systèmes de façon continue. Ces équipes doivent de plus tenter d'innover et apporter des améliorations stratégiques qui réduisent les risques liés à la cybersécurité.

Pour pallier ce besoin urgent, de nombreuses organisations font appel à un fournisseur de service de détection et de réponse gérées (DRG). Ce type de service peut vous aider à résoudre des problèmes complexes de cybersécurité. Et si vous collaborez avec le fournisseur approprié, le service de DRG va au-delà de son utilité opérationnelle : il peut ajouter de la valeur et gérer des solutions de sécurité pour qu'elles cadrent avec vos objectifs d'affaires, réduire l'exposition au risque, garder une longueur d'avance sur l'évolution des menaces et élaborer un modèle adapté visant à obtenir les meilleurs résultats possible.

Vous trouverez dans ce guide une liste de critères qui vous aidera à choisir un fournisseur de service de détection et de réponse gérées, et les questions à poser pour trouver celui qui répond le mieux à vos besoins et qui correspond le mieux à votre organisation.

À vous de jouer.

Qu'est-ce qu'un service de détection et de réponse gérées?

Tout d'abord, définissons la notion de détection et réponse gérées (DRG) : il s'agit d'un service qui comprend la surveillance du réseau informatique, des serveurs et des services infonuagiques d'une organisation pour détecter les menaces, déclencher une réponse pour les contenir ou les neutraliser et prévenir d'autres événements semblables. Partie intégrante du centre des opérations de sécurité, le service de DRG exerce ses activités en tout temps et gère des opérations qui sont vitales pour votre organisation.

Guide de sélection d'un fournisseur de service de DRG

Comme il y a de nombreux fournisseurs de service de DRG, il peut être difficile de trouver celui qui répond le mieux à vos besoins, qui comprend votre secteur d'activité et votre entreprise, et qui peut vous aider à atteindre vos objectifs. Voici les principales étapes de la sélection d'un fournisseur de DRG.

1. Comprendre le problème auquel vous faites face

Il y a de nombreuses raisons pour lesquelles vous pourriez envisager d'avoir recours à un fournisseur de service de DRG. Par exemple, il se peut que vous ne disposiez pas d'un portrait complet des menaces auxquelles votre organisation est exposée. Vous pourriez manquer de ressources spécialisées en cyberdétection et en réponse aux alertes. Quoi qu'il en soit, établir une stratégie claire quant à vos besoins est la première étape pour choisir un fournisseur qui vous convient.

2. Définir vos besoins en matière de sécurité à court et à long terme

Cernez les menaces auxquelles vous faites face dans l'immédiat et établissez le niveau de protection dont vous avez besoin. Gardez toujours à l'esprit que ces menaces peuvent évoluer et que d'autres peuvent surgir, de sorte que vous devez choisir un service capable de s'adapter à ces menaces changeantes et à votre stratégie d'affaires.

3. Faire des recherches sur les fournisseurs de DRG

Recherchez des fournisseurs qui ont déjà fourni des services de DRG, qui sont spécialisés dans le type de problèmes que vous éprouvez en matière de sécurité, et qui ont fait leurs preuves. Tenez compte des services supplémentaires qu'ils offrent, que ce soit pendant un incident ou de façon plus générale pour appuyer votre stratégie. Évaluez leur approche en matière de service et la souplesse dont ils disposent pour répondre à vos besoins particuliers, dans l'immédiat et à plus long terme.

4. Présélectionner des fournisseurs et évaluer leurs capacités

Assurez-vous que les fournisseurs présélectionnés disposent des meilleures technologies de sécurité intégrée (SIEM, SOAR, GSTI, veille stratégique), d'un personnel hautement qualifié et accrédité, de processus bien établis et d'expérience dans votre secteur d'activité. Si leurs services nécessitent du matériel ou des logiciels particuliers, peuvent-ils les fournir? Quelles tâches votre équipe devra-t-elle effectuer? Dispose-t-elle des capacités requises?

Vous devrez brosser un tableau de votre organisation pour la présenter. Un bon fournisseur vous posera diverses questions pour vous y aider, mais il doit aussi faire preuve de suffisamment de souplesse pour déterminer les éléments supplémentaires dont vous avez besoin pour atteindre vos objectifs. Il ne se limitera pas à mener une transaction pour vendre ses services.

Évaluez le niveau de suivi des services proposés par le fournisseur dont vous avez besoin. Quels sont les types de rapports qu'il produit, et à quel point ces renseignements vous sont-ils utiles? Le fournisseur sera-t-il en mesure d'orienter votre stratégie et d'ajouter une valeur réelle qui vous aidera à réduire les risques?

5. Évaluer l'engagement du fournisseur en matière de service continu

L'offre comprend-elle les services d'un gestionnaire de compte, d'un responsable de compte technique et d'un gestionnaire de prestation de services qui s'assureront que : l'entente de service est respectée, les rapports sont produits selon l'échéancier convenu, les services sont améliorés de façon continue, les cas sont transmis à un échelon supérieur en temps opportun et les nouvelles demandes sont prises en charge? Cette équipe est-elle une source de valeur ajoutée pour vos dirigeants en sécurité et en TI? Vous aidera-t-elle à interpréter les rapports et les observations d'une manière qui orientera votre stratégie et votre prise de décision? Peut-elle présenter ses constatations en termes propres aux affaires et exprimer les besoins en matière de DRG de façon à ce que vos décideurs les comprennent, et a-t-elle suffisamment de souplesse pour le faire?

6. Évaluer la réputation et la crédibilité des fournisseurs

Informez-vous sur la réputation de chaque fournisseur en examinant les évaluations de clients et les études de cas. Ont-ils reçu des prix dans leur secteur d'activité? Consultez leurs cotes et leurs accréditations (par exemple, SOC2 ou ISO27001) pour savoir si elles s'harmonisent avec vos cadres de sécurité. Évaluez les profils de compétence des dirigeants et des professionnels qui fournissent les différents services. Ont-ils de l'expérience? S'agit-il vraiment de professionnels en opérations de sécurité ou de cadres mutés qui pourraient se concentrer sur le rendement financier au détriment des intérêts de leurs clients?

7. Examiner la tarification

Recherchez des fournisseurs offrant un modèle de tarification souple et prévisible, fondé sur la croissance et conçu pour s'intégrer à votre infrastructure et à vos paliers de volume de données. L'offre de services comprend-elle le matériel informatique, les logiciels et les licences nécessaires? Certaines tâches précises seront-elles confiées à votre organisation après la mise en œuvre? Le cas échéant, quelles sont les compétences requises à cette fin pour votre équipe? Comparez la tarification proposée par le fournisseur avec les coûts d'une atteinte à la protection des données : perte de propriété intellectuelle, réputation entachée, amende pour infraction aux règles de conformité, paiement de rançon, perturbation des transactions, pertes, etc. Pensez aussi aux capacités remplacées ou compensées par cette offre de services dans votre organisation, et à la façon dont vous pourriez redéployer ces ressources pour des tâches de sécurité ayant une plus grande valeur ajoutée.

La qualité se paie. Il est important d'obtenir une valeur ajoutée, par exemple des rapports présentés de façon experte, une influence auprès des décideurs, des liens avec des personnes-ressources du secteur d'activité et une vaste expertise technique qui va au-delà de la cybersécurité. Si ces éléments comptent pour vous, prenez-les en considération lors de l'évaluation des fournisseurs.

8. Évaluer les modalités du contrat

Examinez la durée et les modalités du contrat de chaque fournisseur pour vous assurer qu'elles : a) sont suffisamment souples pour répondre à vos exigences, b) protègent adéquatement vos intérêts, c) reflètent clairement les livrables des phases de mise en œuvre et de poursuite des activités, d) indiquent comment les services seront évalués, selon quelles normes, et les options de recours s'ils ne conviennent pas (y compris l'entente de niveau de service, l'objectif de niveau de service et les

indicateurs clés de performance qui seront fournis pour les évaluer). Une carte de taux pour les services courants de sécurité ou d'autres services peut accélérer les améliorations apportées aux programmes de votre entreprise en fournissant des options extensibles et en réduisant le temps requis pour les mettre en œuvre.

9. Tenir compte des facteurs de différenciation

Les fournisseurs présentent-ils certains éléments de leur offre de services comme étant des facteurs de différenciation sur le marché? Dans l'affirmative, ces facteurs de différenciation vous interpellent-ils? Appuient-ils votre stratégie?

10. Demander une démonstration

Demandez une démonstration du service de DRG pour voir comment il fonctionne et si ses caractéristiques clés répondent à vos besoins. Le service s'intégrera-t-il aisément à vos systèmes (par exemple, intégration interentreprises de votre système de signalement des incidents), à vos cas d'utilisation personnalisés, à vos guides, à vos rapports et à votre tableau de bord? Le service peut-il être personnalisé? Vos données seront-elles hébergées au Canada? Êtes-vous à l'aise avec l'équilibre entre expertise humaine et automatisation que le fournisseur propose?

Questions à poser aux fournisseurs de service de DRG pour faciliter vos recherches

1. Expérience, expertise, recommandations

- Quelles sont les capacités de votre centre opérationnel de la sécurité des systèmes d'information (SOC) et où se trouve-t-il?
- Quelles sont les pratiques d'embauche et de formation du personnel affecté à la cybersécurité?
- Quel est le parcours de formation et de perfectionnement de vos analystes? Quel est le taux de roulement?
- Fournirez-vous une équipe d'experts qui se consacre à notre organisation?
- Pouvez-vous fournir de 4 à 6 recommandations de clients?

2. Conformité et normes de référence du secteur

- Êtes-vous en conformité avec les normes SOC2 ou ISO 27001?
- Avez-vous adopté des cadres, comme le NIST et le MITRE ATT&CK?

3. Modèle de tarification

- Comment appliquez-vous vos prix?
- Demandez-vous un paiement mensuel, trimestriel ou annuel?

4. Hébergement des données

- De quelles données avez-vous besoin pour nous fournir votre service?
- Où allez-vous héberger nos données? D'où y accéderez-vous?
- Nos données seront-elles hébergées au Canada?
- Comment allez-vous recueillir, stocker, traiter et analyser nos données?

5. Technologies

- Pouvez-vous utiliser nos technologies de sécurité actuelles ou devons-nous en mettre en place de nouvelles?
- Quelle pile technologique offrez-vous pour la prestation de service de DRG de bout en bout, et pourquoi l'avez-vous choisie?
- Vos technologies sont-elles infonuagiques ou devons-nous mettre en œuvre des solutions sur place?
- Quelles sont les technologies de sécurité auxquelles votre service peut s'intégrer?
- En quoi votre stratégie en matière de service de DRG diffère-t-elle pour ce qui est de la technologie sur place, de l'infrastructure infonuagique et des applications infonuagiques?

6. Personnalisation

- Votre offre de services peut-elle être adaptée pour notre organisation?
- Pouvez-vous donner des exemples de façons dont vous avez adapté vos services à l'environnement d'un client?
- Fournissez-vous des rapports et des tableaux de bord personnalisés?
- Votre modèle de prestation de services comprend-il des cas d'utilisation personnalisés et des carnets tactiques?

7. Intégration

- Comment se déroule votre processus d'intégration?
- Combien de temps faut-il, en moyenne, pour qu'un client soit pleinement intégré?
- Quelle activité ou quelle tâche marque la fin de l'intégration?

8. Entente de niveau de service et gestion des incidents

- Quel est votre plan type d'intervention en cas d'incident? Pouvez-vous présenter votre entente de niveau de service?
- Comment détectez-vous les menaces, et comment les contrez-vous?
- De quelles façons contenez-vous les attaques? Comment y répondez-vous?
- À quelle fréquence effectuez-vous une recherche proactive de menaces?
- Quel est le temps moyen de détection et le temps moyen d'intervention pour un incident de sécurité d'importance critique?
- Comment interagirez-vous avec nous lors d'un incident de sécurité?
- Quel est le processus si vous ne détectez pas une menace?
- Quel est votre processus d'amélioration continue?
- Comment avez-vous amélioré votre service à la suite de résolution d'incidents de sécurité chez vos clients?

9. Rapports et tableau de bord

- Quels types de rapports fournissez-vous, et à quelle fréquence?
- Comment pouvons-nous nous assurer que votre centre opérationnel de la sécurité des systèmes d'information prend les bonnes décisions pour notre organisation?
- Comment savons-nous si le service fonctionne et qu'il assure la sécurité de notre organisation?
- Fournissez-vous des rapports de conformité à la réglementation?
- Disposez-vous d'un portail client où nous pouvons consulter nos données et voir les alertes?

Conclusion

Pour choisir le fournisseur de DRG qui convient à votre organisation, il faut tenir compte de votre stratégie et de vos besoins opérationnels clés, puis effectuer des recherches, évaluer l'expérience, les capacités, la qualité du service et les prix de chaque fournisseur. Soyez prêt à poser beaucoup de questions pour déterminer si le fournisseur correspond aux besoins de votre organisation et à vos objectifs en matière de cybersécurité. Assurez-vous de consulter les recommandations, d'obtenir une démonstration du service offert et tentez de concevoir ce que sera votre relation avec le fournisseur à l'avenir.

Un mot sur le service de détection et de réponse gérées de KPMG

La plupart des entreprises sont vulnérables aux cyberattaques, et le seront davantage si elles n'agissent pas rapidement. La prévention est la clé. Le service de détection et de réponse gérées de KPMG fait partie des solutions pour les organisations qui souhaitent accroître leur cyberrésilience dans le contexte hostile d'aujourd'hui.

De nombreux fournisseurs de services de cybersécurité se concentrent principalement sur la gestion de la prévention. Or, KPMG a choisi d'élargir sa portée afin que sa réponse aux incidents soit plus exhaustive. Ainsi, les cybermenaces sont contrées avant qu'elles ne puissent avoir une incidence sur votre entreprise.

Nous pouvons vous aider à raccourcir les délais d'intervention et à réduire les coûts et l'incidence d'une attaque. Voici comment :

01 Intégration transparente avec vos équipes et vos outils de sécurité afin de maximiser le rendement de votre investissement dans vos technologies existantes.

02 Gestion partielle ou totale des activités courantes de surveillance de votre organisation en fonction de vos besoins, ce qui permet à vos équipes internes de se concentrer sur vos activités de base.

03 Repérage automatique des attaques pour les neutraliser rapidement, ce qui limite l'ampleur des mesures correctives et la nécessité de mener d'importantes activités pour les combattre.

04 Présentation améliorée et personnalisée de l'information qui s'insère dans votre stratégie de sécurité.

05 Modèle de prestation de service axé sur la collaboration qui met à la disposition de votre organisation des experts techniques compétents. Nos professionnels en cybersécurité présentent leurs observations en contexte, les expliquent à toutes les parties prenantes et formulent des recommandations quant aux moyens efficaces de faire face aux menaces, ce qui est un élément essentiel d'une gestion efficace de la cybersécurité.

Faites ce que vous faites le mieux, nous nous occupons du reste! Laissez-nous prendre en charge les tâches complexes, fastidieuses et répétitives qui sous-tendent un service de détection et de réponse gérées.

Notre service de DRG est unique dans le secteur, car il offre une portée mondiale et l'accès à un bassin d'experts techniques qui ont votre succès à cœur.

Bénéficiez des avantages de notre approche analytique et prédictive :

votre organisation sera mieux préparée à une attaque potentielle et le risque de perturbations majeures sera réduit grâce à nos processus fiables et résilients.

Améliorez l'exactitude de vos prévisions financières dans un contexte inflationniste :

en concluant un contrat pluriannuel avec nous, vous serez en mesure d'établir des prévisions financières plus précises à l'égard des opérations de sécurité de votre organisation.

Profitez d'une création de valeur rapide :

dans un contexte de changement constant, nous sommes reconnus pour la rapidité avec laquelle nous aidons nos clients à répondre aux perturbations. Notre service de DRG tire parti de nos décennies d'expérience en matière de composants préconfigurés, d'accélérateurs et de feuilles de route de mise en œuvre éprouvés sur le marché et adaptés à vos besoins. Ainsi, nous vous aidons à atteindre rapidement vos objectifs en matière de cybersécurité.

Communiquez avec nous

Cliquez ici pour en savoir plus sur notre service de détection et de réponse gérées et pour obtenir les coordonnées de nos associés.

Robert Moerman
Associé et leader, Cyberdéfense et services gérés de sécurité
KPMG au Canada
416-777-8308
rmoerman@kpmg.ca

Guillaume Clément
Associé, Services-conseils en cybersécurité et président, KPMG Egyde Conseils
KPMG au Canada
418-653-5335
guillaumeclement@kpmg.ca

Hartaj Nijjar
Associé et leader national, Cybersécurité
KPMG au Canada
416-228-7007
hnijjar@kpmg.ca

kpmg.com/ca/fr