Centre de Cyber Intelligence Centre

La sécurité de votre entreprise est-elle centralisée?

Minimisez les cyberrisques grâce à une solution de services de sécurité gérés

Deloitte.

Les cybermenaces sont bien réelles…

Depuis quelques années, les cyberattaques sont mieux planifiées et de plus en plus sophistiquées, et les cybercriminels ciblent des organisations, des régions ou des profils de client précis. Pour prévenir de potentiels dommages financiers, opérationnels et liés à la réputation, les organisations ne peuvent plus confiner la cybersécurité au domaine des TI. La haute direction, les conseillers juridiques et les conseils d'administration doivent prendre des mesures proactives pour renforcer leur résilience cybernétique.

Pour évaluer son degré de préparation, votre organisation devrait pouvoir répondre à diverses questions essentielles, telles que :

- Quelle est votre stratégie en matière de cybersécurité?
- Quelles sont les capacités que vous possédez actuellement, et dans quelle mesure êtes-vous certain qu'elles sont efficaces?
- Quels processus devrez-vous suivre si vous êtes victime d'une attaque?

Obtenez les réponses dont vous avez besoin
Le Centre de Cyber Intelligence (CCI) de Deloitte vous aide à gérer les cyberrisques au moyen de services de sécurité adaptés et intégrés qui assurent la sécurité des données et des systèmes cruciaux de votre entreprise 24 heures sur 24, 7 jours sur 7.

Reconnu comme un leader par Kennedy Vanguard et désigné comme le fournisseur offrant l'éventail de compétences le plus complet en matière de cyberespace, Deloitte fournit des services de sécurité à certaines des plus grandes organisations du monde.

… et ne cessent d'augmenter

Portée mondiale; approche adaptée

À l'échelle mondiale, nous pouvons compter sur plus de 900 professionnels possédant la certification CISSP (Certified Information Systems Security Professionals), 1 500 auditeurs possédant la certification CISA (Certified Information Systems Auditors), 150 gestionnaires possédant la certification CISM (Certified Information Security Managers) et 65 professionnels possédant la certification CIPP (Certified International Privacy Professionals). En outre, nos Centres de Cyber Intelligence sont situés dans des endroits stratégiques au Canada et dans le monde.

Que vous recherchiez des services entièrement gérés en matière de cybersécurité ou que vous souhaitiez remplacer ou améliorer vos services actuels, le Centre de Cyber Intelligence peut vous aider.

Nos services de cyberrisques peuvent vous aider à :

Améliorer votre sécurité
En adoptant une approche de prévention des cybercrimes axée sur le risque, vous avez accès à des renseignements opportuns qui vous permettent de mettre en œuvre des interventions contre les menaces et, par conséquent, d'améliorer l'efficacité de vos contrôles de sécurité.

Redoubler de vigilance
Grâce à une approche personnalisée à l'égard des cyberrenseignements qui tient compte de votre environnement, vous pouvez prévoir plus rapidement les incidents liés à la sécurité et les prévenir, renforcer la méthode de gestion des menaces de votre organisation et réduire votre vulnérabilité aux attaques criminelles.

Augmenter votre résilience
Certains cyberincidents peuvent engendrer de graves crises au sein de l'entreprise. En augmentant votre capacité à détecter les menaces et à y réagir, vous réduirez les pertes et reprendrez vos activités normales plus rapidement.

Vous protéger contre les cyberrisques de bout en bout
L'accès à des ressources compétentes, à des processus éprouvés et à des outils efficaces concernant l'ensemble des aspects de la sécurité vous permet de suivre le rythme dans un environnement où les menaces évoluent constamment.

Que pouvons-nous faire pour vous?

Sécurité

Établir un système de sécurité actualisé pour veiller à ce que tous les dispositifs soient corrigés et mis à jour afin d'être prêts à gérer des attaques potentielles.

Vigilance

Établir un examen périodique des logiciels et des technologies qui servent à déceler les vulnérabilités et les bogues.

Résilience

Établir la capacité de gérer les incidents critiques, de reprendre rapidement les activités normales et de réparer les dommages causés à l'organisation.

Invitez-vous les criminels à vous attaquer?

Comme les systèmes de communications mondiaux deviennent de plus en plus complexes et que les possibilités d'accès aux technologies se multiplient, les organisations de toutes tailles et de tous les secteurs sont plus susceptibles d'être victimes d'un nombre croissant de cybermenaces. Pour atténuer l'incidence des atteintes à la sécurité et vous protéger contre les risques opérationnels, financiers et liés à la réputation, vous avez besoin de renseignements personnalisés sur les menaces qui permettent des interventions.

Renseignements sur les cybermenaces

Rapport sur les menaces permettant des interventions
L'analytique prévisionnelle et une modélisation des risques offrent une surveillance constante des systèmes et des menaces externes les plus pertinentes pour votre organisation et votre secteur. Vous pouvez ainsi détecter des menaces sophistiquées et agir avant qu'elles se concrétisent.

Établissement du cyberprofil
Le cyberprofil de votre organisation – l'information disponible sur Internet à propos de votre entreprise, des utilisateurs et des technologies –, vous montrera les outils dont disposent les criminels lorsqu'ils ciblent votre organisation.

Surveillance et cybersurveillance
Une surveillance approfondie des menaces, ainsi qu'une analyse des indicateurs de menaces et du cyberbavardage vous sont présentées dans des rapports personnalisés qui vous tiennent informés et vous permettent d'intervenir efficacement de façon à réduire l'incidence de ces menaces.

Analyse des menaces évoluées
Nos outils d'analytique et d'investigation informatique de la prochaine génération peuvent aider votre organisation à aborder et à répondre aux menaces évoluées qui pourraient causer des dommages irréparables à vos réseaux et à vos systèmes (p. ex., les maliciels, les courriels suspects, les changements non autorisés à des applications et les tentatives d'accès à des données).

Protéger et détecter

Les approches traditionnelles en matière de cybercrime sont tout simplement inefficaces quand il s'agit des cybermenaces perfectionnées et en évolution. Grâce à la prochaine génération de contrôles de sécurité pour la détection et la prévention, vous pouvez vous préparer aux nouvelles menaces en fonction de l'exposition de votre organisation à des menaces précises.

Atténuation des cybermenaces

Cyber COS
Le cyber COS de Deloitte (Centre des opérations de sécurité) établit un centre au sein de votre organisation, qui gère vos activités de préparation, de détection, d'intervention et d'atténuation. Les capacités de base comprennent les suivantes :

- **Surveillance de sécurité avancée 24 heures sur 24 et 7 jours sur 7** pour une détection précoce des menaces;
- **Analytique de la sécurité avancée**, comme l'analytique prévisionnelle et la modélisation adaptative des risques;
- **Gestion des menaces évoluées de Deloitte**, où les nouvelles données améliorent continuellement la connaissance des menaces et leur atténuation.

Analyse avancée de la vulnérabilité de la cybersécurité
Les cybercriminels cherchent constamment à repérer de nouvelles vulnérabilités et faiblesses (exposition par l'intermédiaire d'applications Web, mauvaise configuration, lacunes dans la formation, etc.) qui se soldent par des données non protégées. Il faut donc évaluer et vérifier votre exposition et votre vulnérabilité, repérer les menaces pertinentes et améliorer votre sécurité à l'aide d'une combinaison de services et d'une application de pointe en matière de diagnostic des attaques, ainsi que de tests de pénétration du réseau.

Prévention de la perte de données et des menaces internes
Notre Centre de Cyber Intelligence peut aider à repérer les menaces aux actifs de données essentiels, les menaces internes et l'activité d'utilisateurs imbriquée.

La technologie axée sur les menaces évoluées combinée à notre expertise de classe mondiale en transformation de la sécurité organisationnelle, fournit à votre organisation une solution complète permettant de gérer les risques posés par les cybermenaces internes.

Une attaque est inévitable – mais perdre la bataille ne devrait pas l'être

Dans le monde d'aujourd'hui où les menaces évoluent rapidement, l'objectif est de savoir quand une attaque se produira, et non si elle se produira. La préparation est essentielle. Lorsque vous êtes victime d'un incident de sécurité, vous devez pouvoir réagir rapidement, mobiliser les bonnes personnes, isoler l'incident et réparer tout dommage avec le moins de perturbations possible. Vous assimilez ensuite ces connaissances, apprenez de vos erreurs et en ressortez encore plus fort.

Interventions liées aux cyberincidents

Cybersimulations
À l'aide de techniques interactives, cette solution plonge les participants dans une simulation de cyberattaque pour aider leur organisation à évaluer ses interventions actuelles et son degré de préparation réel pour réagir efficacement aux cyberattaques.

Intervention liée aux menaces évoluées et reprise des activités
Nous offrons un accès aux compétences, à l'expérience et aux connaissances dont votre organisation a besoin pour gérer efficacement les interventions en cas de crise, réduire la sévérité des atteintes à la sécurité et réduire les délais d'intervention et de reprise des activités.

Analyse judiciaire de la sécurité et analyse des causes fondamentales
Après le processus d'intervention et de reprise des activités, vous voudrez évaluer ce qui s'est passé, découvrir comment c'est arrivé et vous assurer que la situation ne se reproduira plus. L'analyse des causes fondamentales peut inclure non seulement les incidents, mais également les défaillances des contrôles conçus pour *empêcher* les incidents; elle inclut en outre les procédures d'atténuation.

Nous disposons des ressources, des processus, des outils et de la technologie nécessaires pour surveiller et évaluer *en tout temps* les menaces propres à votre organisation.

Transformez votre fonction de cybersécurité

Le Centre de Cyber Intelligence de Deloitte peut aider votre organisation à contrer les attaques lorsqu'elles se produisent, à réduire le temps et les coûts de reprise des activités, et à contrer les menaces futures.

Nous fournissons des ressources, des processus, des outils et des technologies pour surveiller et évaluer les menaces propres à votre organisation 24 heures sur 24, 7 jours sur 7, pour que vous puissiez atténuer rapidement et efficacement les risques et renforcer votre résilience cybernétique. Nos professionnels peuvent également contextualiser les menaces pertinentes pour déterminer les risques qui guettent votre entreprise, vos clients et les parties prenantes.

Pour discuter des stratégies qui vous permettront d'améliorer votre cyberrésilience, communiquez avec les personnes suivantes :

National

Mark Fernandes
Leader de la cybersécurité
416-601-6473
markfernandes@deloitte.ca

Nick Galletto
Leader du groupe services liés aux cyberrisques
416-601-6734
ngalletto@deloitte.ca

Regional

Amir Belkhelladi
Associé
Service des risques d'entreprise
514-393-7035
abelkhelladi@deloitte.ca

Adam Crawford
Directeur principal
Service des risques d'entreprise
416-601-6082
adcrawford@deloitte.ca

Justin Fong
Associé
Service des risques d'entreprise
403-503-1464
jfong@deloitte.ca

Rocco Galletto
Directeur de service
Service des risques d'entreprise
416-643-8718
rgalletto@deloitte.ca

Dina Kamal
Associée
Service des risques d'entreprise
416-775-7414
dkamal@deloitte.ca

Albert Yap
Associé
Service des risques d'entreprise
604-640-3279
ayap@deloitte.ca

www.deloitte.ca/cyber

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 13-3727T