

Deloitte.

Centre de
Cyber Intelligence
Centre

Services de sécurité gérés

Aider les entreprises à prévenir, détecter
les cybermenaces, et d'y réagir

Offerts par le Centre
de Cyber Intelligence
de Deloitte





La cybersécurité est plus qu'une question de technologie. Il s'agit d'un enjeu fondamental pour le risque d'affaires. En effet, les cyberattaques, dont le nombre augmente toujours, sont l'une des menaces principales dans le secteur des affaires à l'échelle mondiale.

« Les cyberattaques
représentent 294,15 G\$
du PIB total à risque... »

Rapport Lloyd's Risk Index 2015-2025

Un nouveau type de fournisseur de services de sécurité gérés



À mesure que les cybermenaces évoluent et deviennent plus complexes, de nombreuses entreprises reconnaissent qu'elles ne peuvent pas gérer seules ce problème. Elles se tournent donc vers des fournisseurs de services de sécurité gérés, comme Deloitte, qui deviennent des partenaires pouvant leur offrir une solution rentable pour gérer la surveillance et la détection des cybermenaces, ainsi que l'intervention en cas d'incident.

Puisque nous comprenons que les entreprises veulent des solutions souples, nous offrons une gamme complète de services de cybersécurité enrichis pour aider les clients à adapter leur protection en fonction des risques susceptibles de toucher leur entreprise. Notre objectif est de devenir un prolongement des équipes de sécurité de nos clients, et c'est pourquoi nos services de sécurité gérés sont personnalisés selon leurs besoins.

À titre de fournisseur de services de sécurité gérés, nous offrons plus que des opérations de sécurité et de gestion des informations et des événements de sécurité. Nous sommes le plus important groupe mondial de services de sécurité. Nos services englobent la sécurité des informations, les services-conseils en matière de cybersécurité, la mise en œuvre et l'intégration de solutions, les services gérés, les renseignements pratiques sur les cybermenaces et l'intervention en cas d'incident. Notre réseau mondial d'échange de renseignements sur les cybermenaces et d'analytique fournit aux entreprises la visibilité nécessaire pour mieux protéger leurs données confidentielles et leur infrastructure essentielle, et nos solutions de gestion des incidents permettent une intervention et une reprise des activités rapides. Notre approche est exhaustive : elle vise à aider nos clients à réagir de façon proactive face aux menaces, 24 heures sur 24 et 7 jours sur 7, offrant un niveau de protection encore plus important par l'intermédiaire de centres d'opérations de sécurité à haute disponibilité.

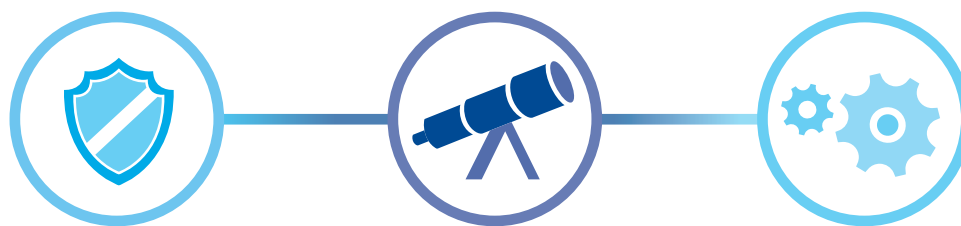
Une approche exhaustive à l'égard de la cyberconfiance

Afin d'offrir des cybersolutions efficaces, nous consultons les entreprises pour définir des plans de résilience en matière de cybersécurité qui les aideront à prévenir les cyberattaques, à les détecter et à réagir rapidement – limitant ainsi les dommages causés. Cette approche les aide à devenir plus que sécurisées.

Pour en arriver à la cyberconfiance, il faut d'abord mettre en place une stratégie et une gouvernance. Notre gamme complète de services de cybersécurité intègre la stratégie et la gouvernance aux capacités de base requises pour aider les entreprises à devenir plus sécurisées, plus vigilantes et plus résilientes. Notre approche couvre tout le cycle de vie des besoins en services-conseils, des exigences de mise en œuvre et des services gérés.

Gouvernance et stratégie

Cerner les principaux risques, adapter les investissements, élaborer un programme de gestion des cyberrisques contrôlé par la direction et s'adapter à l'évolution des stratégies d'affaires et des menaces. L'objectif final est de soutenir un programme de gestion des cyberrisques contrôlé par la direction, qui établit un équilibre entre les exigences de « sécurité, vigilance et résilience » et la tolérance au risque de l'entreprise.



Sécurité

Adopter une approche mesurée et axée sur les risques pour assurer la défense contre les menaces connues et émergentes.

Vigilance

Acquérir une connaissance de la situation et recueillir des renseignements sur les menaces afin de repérer rapidement les comportements potentiellement dangereux.

Résilience

Pouvoir assurer la reprise des activités après un cyberincident et en minimiser les répercussions sur l'entreprise.

Un prolongement important de votre équipe de cybersécurité

Par l'intermédiaire de nos Centres de Cyber Intelligence, nous utilisons des outils sectoriels et exclusifs de pointe pour offrir une gamme complète de services de sécurité gérés.

La sécurité ne peut pas être tout simplement impartie. À titre de fournisseur de services de sécurité gérés, les services que nous offrons ne se limitent pas aux opérations de sécurité et à la gestion des informations et des événements de sécurité. Et tant que leader reconnu en services-conseils de sécurité, nos années d'expérience nous ont permis de lancer des programmes de sécurité et nous les appliquons à nos activités quotidiennes afin d'apporter constamment des améliorations pour nos clients.

Nous fournissons aussi les ressources, la protection et les talents dont les entreprises ont besoin pour apporter des améliorations et maintenir un programme de cybersécurité solide. Nous aidons les clients à se concentrer sur ce qui compte, en éliminant les fausses alertes, en effectuant un triage efficace avant de lancer une alerte et en établissant la priorité des risques pour assurer l'affectation la plus efficace possible des budgets limités. Surtout, nous agissons en tant que prolongement de l'équipe, travaillant en collaboration avec nos clients pour les aider à renforcer leurs cyberdéfenses. Nos capacités uniques en matière de services de sécurité gérés sont notamment les suivantes :

Gestion des informations et des événements de sécurité

Surveillance en temps réel, corrélation et analyse des événements de sécurité pour l'ensemble des actifs de l'entreprise.

En voici quelques exemples :



Consignation, surveillance et alertes 24 heures sur 24, 7 jours sur 7

Surveillance de sécurité avancée 24 heures sur 24 et 7 jours sur 7 pour détecter rapidement les menaces et les atténuer. La détection rapide permet aux entreprises de bloquer une attaque avant qu'elle touche les services d'affaires.



Solution personnalisée selon le client ou entièrement gérée par Deloitte

Modèle d'opérations entièrement enrichi qui fonctionne avec vos systèmes actuels ou qui est entièrement géré par Deloitte selon les besoins d'affaires. Nous adaptons notre solution à votre entreprise.

Services de sécurité gérés



Gestion des vulnérabilités

Gestion du cycle des vulnérabilités; de l'identification à la gestion du plan de reprise et de rapports.

Services de mise en œuvre

Mise en œuvre et gestion d'outils, de technologies et de processus pour l'élaboration de contrôles axés sur les risques et le soutien des activités.

Gestion des outils de sécurité

Gestion des logiciels antivirus, des outils de sécurité du périmètre et d'autres solutions de prévention et de détection.

Opérations de sécurité sur les lieux

Déploiement de notre personnel chevronné qui collaborera avec vous pour améliorer votre programme actuel de sécurité informatique, ou qui complètera vos besoins en effectif s'il existe des lacunes.

Afin de vous fournir des solutions de sécurité plus approfondies, nous offrons également les services suivants :



Analytique et cybermenaces

La sécurité ne suffit pas toujours. Par l'intermédiaire de notre réseau mondial d'échange de renseignements sur les cybermenaces, nous surveillons proactivement les environnements de nos clients et l'environnement des menaces externes afin de prévenir et de détecter les menaces internes et les cyberattaques ciblées. Nous transformons les mises à jour des renseignements sur les cybermenaces en stratégies d'atténuation réalisables pour aider nos clients à réagir face aux menaces susceptibles de toucher leur entreprise. Notre réseau mondial d'échange de renseignements sur les cybermenaces – et nos puissantes ressources d'analytique – fournissent aux entreprises la visibilité nécessaire pour mieux protéger leurs données confidentielles et leur infrastructure essentielle.

Ces capacités comprennent les suivantes :

- Renseignements sur les cybermenaces et collaboration/échange de renseignements
- Cybersurveillance, y compris l'analyse du Web invisible
- Analyse avancée des menaces
- Rétroingénierie de logiciels malveillants
- Recherche de menaces
- Simulation d'incidents



Intervention en cas d'incident

Malgré tous les efforts déployés de prévention et de détection, il arrive que l'inévitable se produise. Nous fournissons à nos clients des solutions qui les aideront à réagir de façon proactive et à reprendre leurs activités après une cyberattaque. Nos capacités d'intervention en cas d'incident soutiennent les clients dans l'immédiat ainsi qu'à moyen et à long terme après un incident, assurant notamment la gestion de crise, l'enquête technique, la résolution des problèmes de sécurité, l'amélioration du programme de gestion des cyberrisques et la conformité à la réglementation.

Ces capacités comprennent les suivantes :

- Stratégies proactives d'intervention en cas d'incident axées sur l'entreprise
- Évaluation des compromissions
- Simulations d'incident et jeux de guerre
- Gestion des cyberrisques et préparation à l'échelle de l'entreprise



Services-conseils en matière de cyberrisques

En tant que chef de file reconnu dans le domaine des services-conseils en sécurité, Gartner Inc. nous classe annuellement au premier rang à l'échelle mondiale, d'après les revenus, depuis 2012¹. Nous comprenons bien le cadre mondial des cybermenaces et nous savons comment nous y retrouver. Notre expertise s'étend à tous les secteurs, et nos conseillers sont axés à la fois sur les affaires et sur la technologie pour veiller à ce que les budgets limités soient affectés aux aspects prioritaires de la gestion des cyberrisques.

Nous avons adapté ces connaissances dans notre groupe des services-conseils en matière de cyberrisques afin d'offrir à nos clients une approche de gestion du cycle de vie complet à l'égard de la cyberrésilience.

¹ Gartner. Marketshare analysis: *Information security consulting worldwide 2014*. Gartner Inc. 31 mars 2015.

Pourquoi Deloitte?

La cyberconfiance dépend de la confiance envers le fournisseur de services de sécurité gérés

De nos jours, les entreprises ont amplement le choix lorsqu'elles recherchent un fournisseur. Alors, pourquoi choisir Deloitte?



Notre équipe est la vôtre

En agissant comme un puissant prolongement de votre équipe, nous répondons à toute la gamme de vos besoins : définition des exigences, intégration, stabilité des opérations, le tout afin d'assurer le maintien du savoir-faire interne en matière de technologie, de processus et de gestion des risques. Possédant une vaste expertise sectorielle, nos conseillers sont axés à la fois sur les affaires et sur la technologie pour veiller à ce que les budgets limités soient affectés aux besoins prioritaires.



Nous sommes un leader de la technologie

Nous offrons aux entreprises bien plus que des services-conseils traditionnels pour relever les défis. Grâce à nos capacités technologiques évoluées, nous sommes régulièrement reconnus comme un chef de file du secteur dans le domaine des services-conseils en cybersécurité. En fait, Gartner Inc. nous classe annuellement au premier rang à l'échelle mondiale, d'après les revenus, depuis 2012.



Nos solutions sont personnalisées, exhaustives et stratégiques

Nos services de sécurité gérés comprennent une gamme complète de solutions personnalisées selon les besoins de l'entreprise, et ils se fondent sur notre vaste expérience de tous les secteurs et de toutes les facettes des affaires.



Nous offrons la portée de services qui correspond à vos besoins

Notre groupe des services de sécurité gérés est le plus important² au monde, et nos services englobent les services-conseils en matière de cybersécurité, la mise en œuvre de solutions, l'intégration, les services de sécurité gérés, les renseignements sur les cybermenaces, ainsi que l'analytique et l'intervention en cas d'incident. Nous ouvrons chaque année de nouveaux Centres de Cyber Intelligence pour pouvoir servir le marché mondial et aider les clients 24 heures sur 24 et 7 jours sur 7, tous les jours de l'année. Au Canada, nous comptons des Centres de Cyber Intelligence à Montréal, Toronto et Calgary, qui sont au service des clients du pays. Ces centres ont le niveau de sécurité Protégé B du gouvernement fédéral du Canada, ils exercent leurs activités selon le cadre de la norme ISO 27001, et leur personnel qualifié détient la cote de sécurité « secret » du gouvernement du Canada.

² The Forrester Wave™: Information Security Consulting Services, Q1 2016 | The 13 global providers that matter most and how they stack up, 29 janvier, 2016



Nous connaissons l'environnement des cybermenaces et nous nous adaptons au changement

Nous transformons les renseignements sur les cybermenaces en contenu utile dont nos clients peuvent se servir pour détecter et prévenir proactivement les incidents liés à la sécurité. De plus, nos solutions d'intervention en cas d'incident permettent de réagir et de reprendre les activités rapidement après une cyberattaque.



Nous sommes motivés par la nécessité d'une amélioration constante

Votre entreprise évolue au fil du temps, les cybermenaces aussi. En offrant des cybercapacités essentielles à votre entreprise, nos professionnels continuent à mettre continuellement en pratique les leçons apprises afin d'améliorer les opérations et rester à l'avant-garde.



Les détails et les normes ont une grande importance pour nous

Nous effectuons une analyse des capacités existantes de votre entreprise, de ses talents et de sa complexité pour vous aider à déterminer le modèle d'opérations de sécurité qui convient le mieux à votre entreprise. Nous comprenons que les budgets sont limités et nous aidons nos clients à établir les priorités de leurs investissements.



La communication dans les deux sens constitue pour nous une priorité

Nous ne croyons pas à l'approche « pas de nouvelles, bonnes nouvelles » en matière de gestion des cyberrisques. Nous insistons sur l'importance d'avoir régulièrement des entretiens hebdomadaires ou mensuels avec nos clients afin de discuter des menaces et de l'état global de leurs mesures de sécurité. Tout aussi important, nous comprenons la nécessité de maintenir une communication ouverte de façon à répondre aux questions en tout temps, pas seulement lorsqu'elles deviennent urgentes.

Le genre d'aide dont votre entreprise a besoin



Le cybercrime fait des ravages à toute heure du jour et de la nuit et pour le contrer, il faut pouvoir compter sur un partenaire qui saura protéger votre entreprise 24 heures sur 24, 7 jours sur 7. Les exigences d'aujourd'hui nécessitent un fournisseur de services de sécurité gérés qui peut non seulement alléger le fardeau des cyberattaques sophistiquées pour votre entreprise, mais également agir comme un puissant prolongement de votre équipe.

Pour en apprendre davantage sur la façon dont nous pouvons collaborer avec vous pour aider votre entreprise à devenir plus cyberconfiante, communiquez avec nous dès aujourd'hui.



Personnes-ressources

Rocco Galletto

Associé
Leader national,
Services de sécurité
gérés

rgalletto@deloitte.ca

Justin Fong

Associé
Service des risques
d'entreprise,
Ouest du Canada

jfong@deloitte.ca

Amir Belkhelladi

Associé
Service des risques
d'entreprise,
Est du Canada

abelkhelladi@deloitte.ca

Nick Galletto

Associé
Leader des Amériques,
Services liés aux
cyberrisques

ngalletto@deloitte.ca





www.deloitte.ca/cyber

Deloitte, l'un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de la certification, de la fiscalité, de la consultation et des conseils financiers. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.