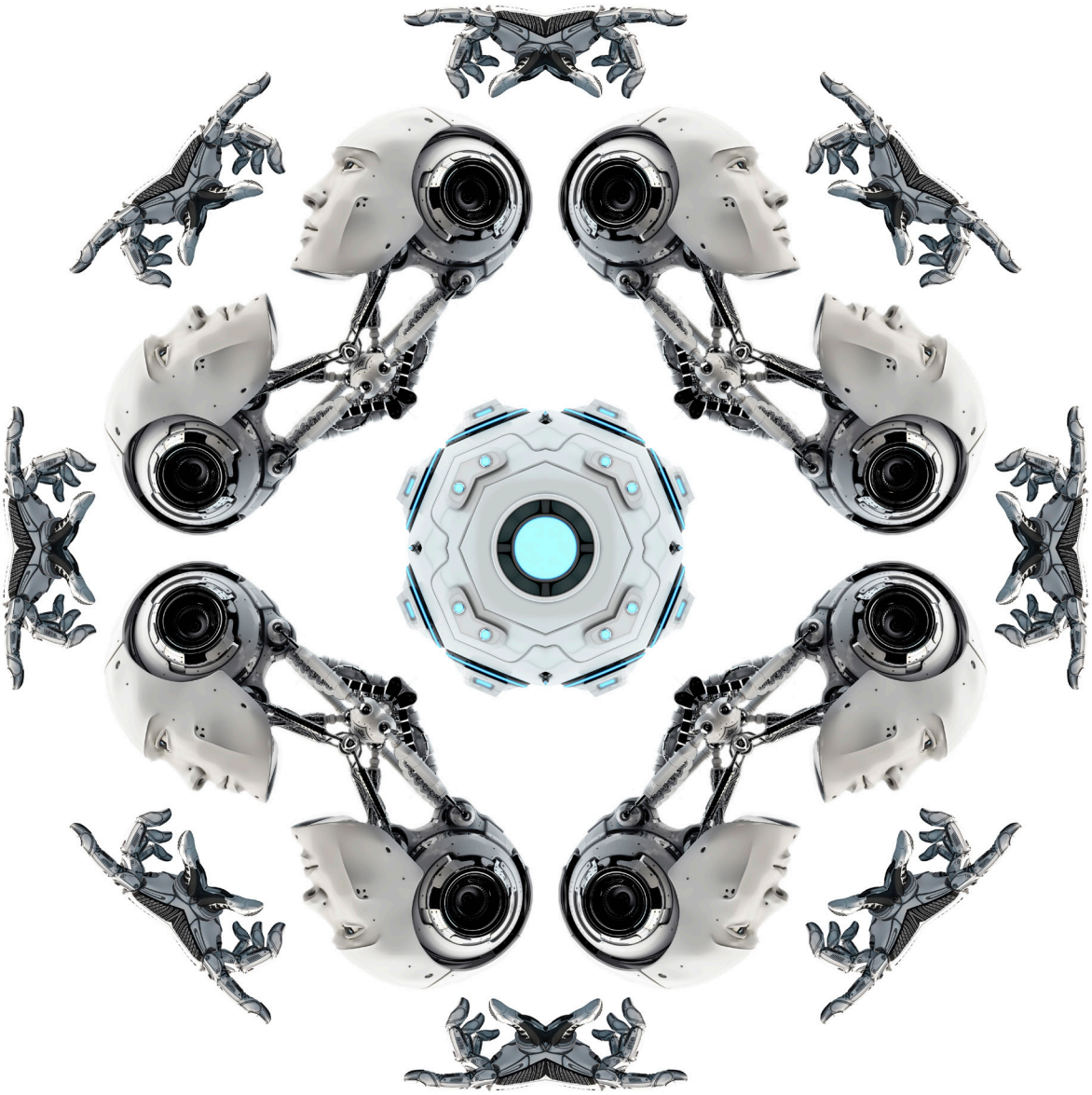
Deloitte.



Cybersécurité éclairée

Comment l'IA peut vous aider à gérer les cyberrisques

Cyberrisques

Gérer les cyberrisques grâce à la cybersécurité éclairée

À l'ère numérique, les technologies d'intelligence artificielle commencent à avoir une incidence semblable à celle des usines et des chaînes de montage sur la fabrication à l'aube de l'ère industrielle, améliorant considérablement l'efficacité et rendant possibles de nouveaux produits, services et modèles d'affaires.

Motivées par les pressions internes et externes afin qu'elles fassent évoluer continuellement leurs capacités à atténuer et à minimiser les cyberrisques, les organisations explorent activement les nouvelles technologies et les occasions d'amélioration autant que possible.

L'intelligence artificielle (IA) est un sujet d'actualité dans l'organisation, poussant l'innovation vers de nouveaux sommets dans de nombreux secteurs d'activité. Les progrès réalisés dans les technologies d'IA, les capacités de traitement et la disponibilité des données permettent aux systèmes informatiques d'exécuter des tâches qui exigeaient autrefois une intelligence humaine. Ces tâches incluent l'apprentissage machine, le traitement du langage naturel, la reconnaissance de la parole, la vision artificielle, la compréhension d'image et la robotique.

En cybersécurité, les technologies d'IA peuvent améliorer les renseignements et les prévisions sur les cybermenaces et renforcer la protection contre de telles menaces.

Elles peuvent également accélérer la détection des attaques et les délais de réponse, tout en réduisant le besoin d'experts humains en cybersécurité – qui sont une denrée rare de nos jours[1]. L'IA peut apprendre des analystes de la sécurité et améliorer sa performance au fil du temps, ce qui permet de gagner du temps et de prendre de meilleures décisions. Ces capacités de « cybersécurité éclairée » sont de la plus haute importance alors que les cyberattaques continuent de croître en volume et en complexité.

L'analytique et les données massives sont des moteurs clés pour l'IA, permettant le traitement et l'analyse de grandes quantités de données; l'analyse syntaxique, le filtrage et la visualisation se faisant en temps quasi réel. L'adoption de l'analytique avancée est également un pas essentiel pour devenir une organisation orientée sur l'information.

Le présent rapport décrit comment vous pouvez utiliser les technologies d'IA pour améliorer vos capacités en cybersécurité et gérer les cyberrisques de manière plus efficiente et plus efficace.

1. Deloitte. *Les différents visages de la cybersécurité : combler les lacunes liées aux cyberrisques*, 2018.

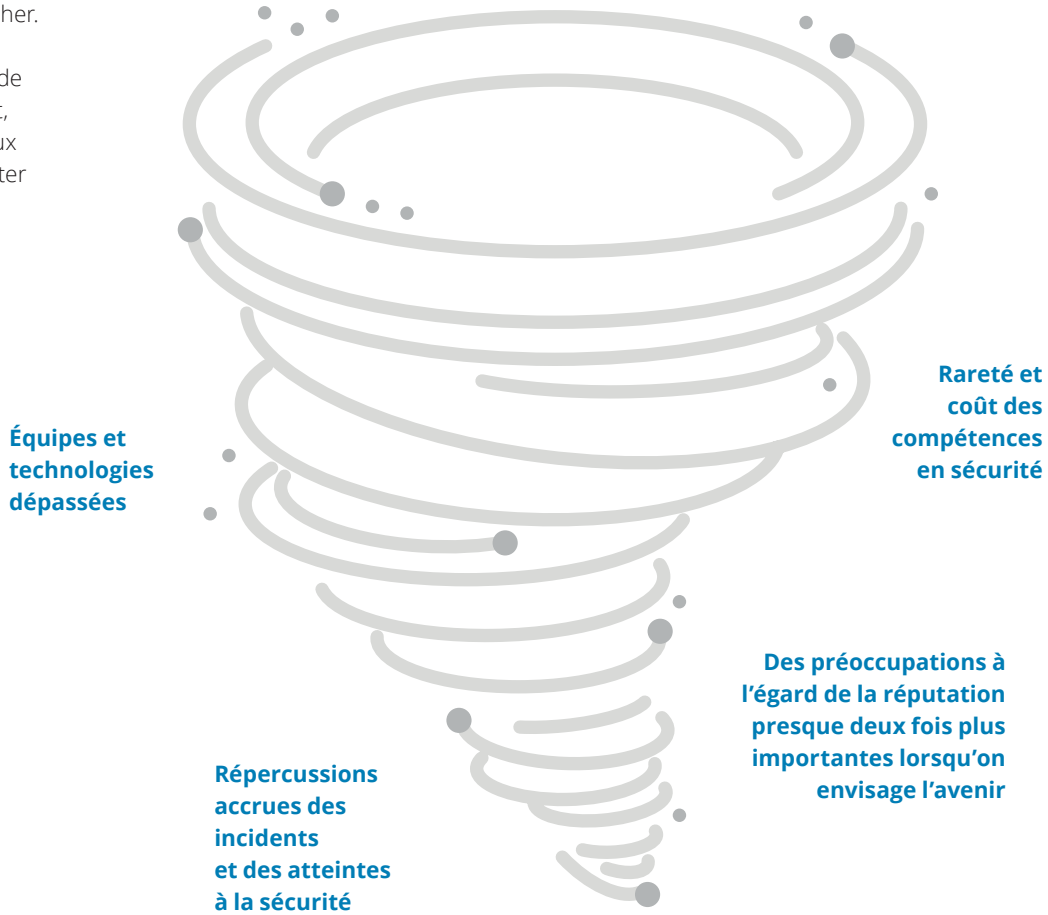
Le bouleversement des cyberrisques

La cybersécurité est l'un des plus grands défis de l'ère numérique. Et il ne cesse de prendre de l'ampleur.

Les cybermenaces connaissent une croissance exponentielle. Les auteurs de menaces internes apprennent à échapper aux systèmes basés sur la signature, et les malfaiteurs utilisent l'IA pour éviter la détection en se tenant au courant des règles de détection les plus courantes.

Les équipes de cybersécurité se sentent dépassées par la taille et la complexité de ce défi grandissant, alors que les experts en cybersécurité dont elles ont besoin pour réussir à contrer les attaques sont de plus en plus coûteux et difficiles à dénicher.

Tous ces éléments réunis sont en train de créer des bouleversements. Cependant, les organisations peuvent faire appel aux technologies émergentes pour surmonter le pire.



Les technologies de cybersécurité éclairée couvrent un large spectre, allant de la simple automatisation fondée sur des règles qui reproduit les comportements humains à l'intelligence artificielle qui reproduit, voire surpasse, l'intelligence et le jugement humains (Figure 1).

Figure 1 : Spectre des technologies de cybersécurité éclairée

Peut imiter les gestes humains	Peut imiter ou augmenter le jugement humain quantitatif	Augmente l'intelligence humaine	Peut imiter l'intelligence humaine
• Utilisée pour des processus fondés sur des règles • Permet : – plus grande vitesse de traitement – accroissement du volume – réduction des erreurs	• Utilisée pour des processus faisant appel au jugement • Capacités : – apprentissage machine – traitement du langage naturel – interprétation des comportements humains	• Utilisée pour la prise de décisions prédictives • Autoadaptation et autogestion dynamiques	• Utilisée pour l'intelligence machine pour l'apprentissage sans supervision, mais également pour la communication et l'interaction de façon transparente avec des équipes d'humains (ou d'associés humains)

L'apprentissage machine utilise des techniques de statistique et des algorithmes qui apprennent à partir des données de manière itérative, et qui créent et améliorent automatiquement des modèles sans nécessiter de programmation supplémentaire. Cette méthode compte de nombreuses applications potentielles en cybersécurité, permettant notamment l'acquisition de cybercapacités automatisées et prédictives grâce auxquelles un agent logiciel intelligent pourrait déceler une attaque active et apporter les modifications nécessaires pour la contrecarrer.

Le traitement du langage naturel (TLN) propose également de nombreuses applications essentielles en cybersécurité, y compris la prévention des fuites de données. À l'aide de points de référence du comportement d'un utilisateur créés par l'analytique comportementale, le TLN pourrait établir un profil pour chaque utilisateur et ensuite surveiller les situations anormales tout en apprenant et en tirant des conclusions des nouvelles tendances comportementales.

Dans l'univers de la cybersécurité et des cyberrisques, les capacités actuelles les plus matures se situent du côté de l'automatisation des processus robotisés (APR) du spectre des technologies. Toutefois, l'extrémité plus sophistiquée du spectre (automatisation cognitive et intelligence artificielle) évolue rapidement, grâce à cinq principaux facteurs :

1. **Précision croissante des algorithmes prédictifs**
   Les avancées en apprentissage machine améliorent la capacité de déterminer les risques émergents avec plus de précision grâce à la prévision des risques.

2. **Baisse des coûts technologiques**
   À mesure que les capacités d'automatisation et d'informatique s'effectuent plus rapidement et à moindres coûts, la mise en œuvre des modèles de prédiction des risques est de moins en moins coûteuse.

3. **Disponibilité croissante de sources d'information abondantes**
   Jumelée à des progrès en analytique des données non structurées, la disponibilité de précieux ensembles de données externes et internes fait augmenter la puissance et l'incidence de la prévision des risques.

4. **Sophistication croissante des technologies d'IA**
   L'IA a maintenant la capacité d'avancer ses propres hypothèses (comme la prévision des techniques d'attaque) et de proposer ensuite des recommandations pour les vérifier.

5. **Utilisation de la gestion des risques pour accroître la valeur commerciale**
   Le risque fait partie intégrante des activités d'affaires; cependant, l'acquisition de perspectives prévisionnelles pour prendre des décisions plus éclairées est susceptible de conférer un précieux avantage concurrentiel.

Selon le laboratoire en informatique et intelligence artificielle (*Computer Science and Artificial Intelligence Laboratory*) du MIT, dans un avenir prévisible, la cybersécurité sera probablement axée sur une approche hybride, où les humains et les machines uniront leurs efforts pour gérer les cyberrisques de façon plus efficace et plus efficiente.

Avantages de la cybersécurité éclairée

En mettant à profit l'IA et l'analytique avancée pour traiter de grandes quantités de données internes et externes, les technologies de cybersécurité éclairée peuvent générer des perspectives prédictives et concrètes qui vous aideront à prendre de meilleures décisions liées à la cybersécurité et à protéger votre organisation contre les menaces. Elles peuvent aussi vous aider à détecter et à contrer les menaces plus rapidement en surveillant le cyberenvironnement à une vitesse et à un niveau de précision dont seules les machines sont capables. Le plus important, sans doute, est que la cybersécurité éclairée peut vous aider à suivre le rythme des innombrables obstacles provenant d'attaques de plus en plus complexes.

L'approche traditionnelle en niveaux de la cybersécurité ne peut que prévenir et détecter les menaces les moins élaborées. Entre-temps, des cyberattaques modernes sont soigneusement mises au point pour contourner les contrôles de sécurité standards par l'apprentissage des règles de détection. En outre, les contrôles traditionnels peuvent ne pas contrer adéquatement les menaces internes, une forme d'attaque insidieuse lancée par des personnes ayant un accès légitime.

En tirant parti d'un vaste éventail de sources de données, les plates-formes de détection intelligente peuvent apprendre et reconnaître les comportements normaux, établir des bases de référence et détecter les valeurs aberrantes, relever les activités malveillantes semblables à des événements précédemment observés et faire des prédictions au sujet de menaces jamais vues auparavant. Ces objectifs ne peuvent être atteints au moyen des contrôles traditionnels basés sur la signature et sur des règles.

De plus, les technologies de cybersécurité éclairée effectuent des tâches de manière très uniforme et répétée, réduisant ainsi les interventions et les erreurs humaines. Elles offrent l'avantage supplémentaire de faciliter la protection, la gestion et l'audit du cyberenvironnement pour assurer la conformité aux règles gouvernementales et à d'autres exigences externes.

Finalement, les technologies de cybersécurité éclairée peuvent vous aider à tirer le maximum de vos rares talents en cybersécurité. Elles permettent à vos équipes de réaliser le travail avec moins de ressources, tout d'abord en accomplissant la plus grande partie des tâches routinières et exigeantes en main-d'œuvre afin de permettre aux experts humains de se concentrer sur les activités plus utiles et stratégiques et ensuite, en offrant aux cyberspécialistes les outils nécessaires pour fournir un rendement élevé sans nécessiter des années d'expérience et de formation.

Principaux avantages des technologies de cybersécurité éclairée :

- Elles complètent les applications et les contrôles de sécurité existants par la détection de menaces progressives, émergentes et inconnues.
- Elles permettent aux entreprises de détecter des menaces persistantes avancées et de définir les indicateurs d'infraction pouvant ne pas être décelés par les mesures de sécurité existantes.
- Elles améliorent le processus de recherche de menaces par la collecte, la corrélation et l'analyse d'un vaste éventail de données sur la sécurité.
- Elles établissent des schémas de menaces en puisant dans les renseignements sur les cybermenaces, les renseignements sur la vulnérabilité, les journaux d'événements des appareils et les données contextuelles, d'où sont tirées des perspectives de sécurité proactives et prévisionnelles.

Aller au-devant des risques grâce à la prévision des risques

Traditionnellement, la gestion des cyberrisques a été une activité en mode réactif, axée sur les risques et les pertes déjà survenus. Mais grâce à l'adoption croissante de l'analytique avancée et des technologies d'IA, la gestion devient de plus en plus prospective et prévisionnelle.

La prévision des risques utilise l'analytique et les technologies d'IA pour vous informer à l'avance des risques émergents, accroître la sensibilisation aux menaces externes, et permettre à l'organisation de mieux comprendre son exposition aux risques et les pertes qu'elle pourrait subir.

Désormais, les activités de surveillance se déroulent tout au long du cycle de vie de gestion des risques et sont divisées en trois catégories :

Activités réactives

Consigner les pertes et isoler les incidents évités de justesse. Élaborer de l'information de base pour quantifier l'incidence des pertes liées aux événements. Signaler l'état des risques actuels et des mesures correctives.

Activités prédictives

Rassembler et intégrer de l'information interne et externe pour permettre la diffusion d'alertes en temps quasi réel. Décrire les tendances et les risques émergents. Utiliser les résultats issus des approches réactives et intégrées pour générer des perspectives prédictives en matière de risques grâce à l'analytique avancée.

Activités intégrées

Mesurer objectivement le rendement par rapport aux risques en facilitant l'élaboration d'indicateurs de risque clés, d'indicateurs de rendement clés et des seuils connexes. Favoriser une description précise de l'exposition aux risques en dressant un portrait complet de l'ensemble de l'organisation.

Comment appliquer la prévision des risques au sein de votre organisation

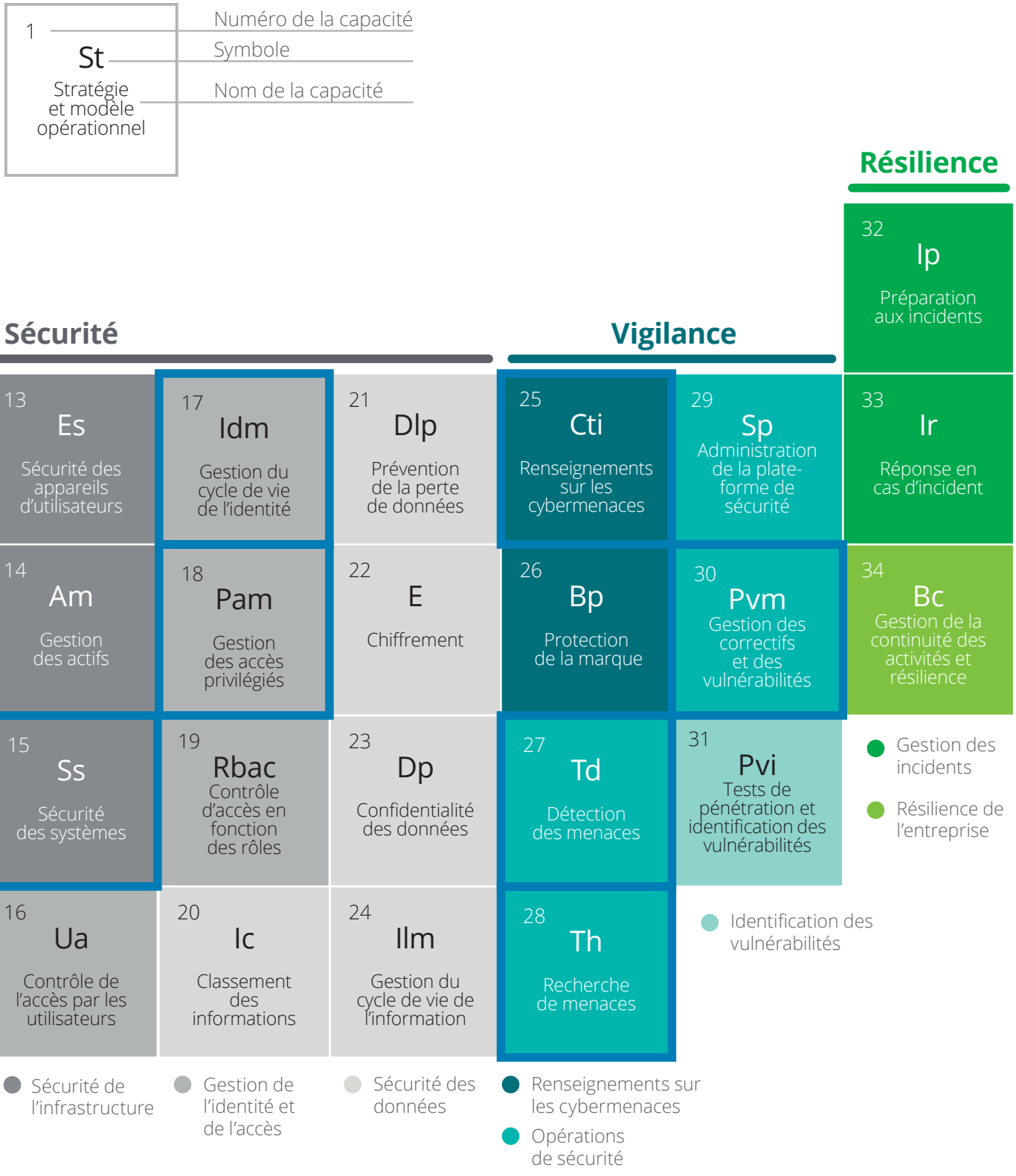
Ce type de gestion des risques est susceptible d'aider votre organisation dans quatre domaines importants de la cybersécurité :

- **Prise de décisions liées aux risques.** Analyser de grands volumes de données contextuelles et de points de décision pour déterminer les choix logiques, afin d'aider les dirigeants à prendre des décisions stratégiques et financières qui correspondent à la tolérance au risque de l'organisation (p. ex., analyser les anciennes données d'investissement et les nouvelles financières en temps réel pour prendre des décisions d'investissement, évaluer de façon rationnelle les risques liés aux actifs).
- **Détection des risques.** Déterminer ou prévoir les risques que les humains et les systèmes fondés sur des règles ont de la difficulté à repérer, comme les nouvelles catégories de risques, les signaux diffus ou les sources potentielles de futurs risques (p. ex., utiliser des données provenant de tribunes publiques, comme les médias sociaux et les blogues, où les clients et les critiques, entre autres, se rassemblent pour aborder et évaluer la réputation d'une organisation et les risques connexes).
- **Surveillance et détection des menaces.** Effectuer un suivi des activités et des entités pour établir les comportements normaux, et détecter les sources d'anomalies qui pourraient entraîner des risques potentiels (p. ex., la détection de fraude et de blanchiment d'argent; la détection des menaces internes, notamment les cyberrisques et les risques liés à la conformité venant de l'intérieur; les renseignements sur les cybermenaces en temps réel).
- **Automatisation des processus de gestion des risques.** Automatiser les processus complexes de gestion des risques exigeants en main-d'œuvre et sujets à des erreurs, traitant des volumes élevés de données structurées et non structurées (p. ex., le contrôle diligent de tiers, la gestion de l'identité et de l'accès, la gestion du risque de crédit et la gestion du risque de modèle), plus particulièrement les processus qui pourraient bénéficier d'un outil capable d'apprendre par lui-même au fil du temps.

Par où commencer

Bon nombre d'entreprises disposent d'une multitude de données précieuses enfouies sous d'innombrables processus d'affaires inefficaces et disparates, ce qui fait en sorte qu'il est difficile de s'y retrouver. Pour vous aider, Deloitte a élaboré un cadre fondé sur les capacités afin de déterminer les domaines précis où les technologies d'IA et la cyberanalytique peuvent être appliquées. Ce cadre est représenté sous forme de tableau qui porte sur toutes les phases de la cybersécurité (Figure 2).

Figure 2 : Tableau périodique des éléments de cybersécurité


1
St
Stratégie et modèle opérationnel
Numéro de la capacité
Symbole
Nom de la capacité
Résilience
Sécurité
Vigilance
32 Ip Préparation aux incidents
13 Es Sécurité des appareils d'utilisateurs
17 Idm Gestion du cycle de vie de l'identité
21 Dlp Prévention de la perte de données
25 Cti Renseignements sur les cybermenaces
29 Sp Administration de la plate-forme de sécurité
33 Ir Réponse en cas d'incident
14 Am Gestion des actifs
18 Pam Gestion des accès privilégiés
22 E Chiffrement
26 Bp Protection de la marque
30 Pvm Gestion des correctifs et des vulnérabilités
34 Bc Gestion de la continuité des activités et résilience
15 Ss Sécurité des systèmes
19 Rbac Contrôle d'accès en fonction des rôles
23 Dp Confidentialité des données
27 Td Détection des menaces
31 Pvi Tests de pénétration et identification des vulnérabilités
16 Ua Contrôle de l'accès par les utilisateurs
20 Ic Classement des informations
24 Ilm Gestion du cycle de vie de l'information
28 Th Recherche de menaces
Gestion des incidents
Résilience de l'entreprise
Identification des vulnérabilités
Sécurité de l'infrastructure
Gestion de l'identité et de l'accès
Sécurité des données
Renseignements sur les cybermenaces
Opérations de sécurité

Voici des cas d'utilisation éloquents d'automatisation dans des domaines précis de la cybersécurité, qui peuvent regrouper plusieurs éléments du tableau.

4
Rm
Gestion, paramètres et signalement des cyberrisques

Gouvernance, risques et conformité

Gouvernance et gestion des risques
Guider la stratégie globale et améliorer les capacités de production de rapports par l'utilisation de grands volumes de données contextuelles et de points de décision pour appuyer une prise de décision stratégique qui correspond à la tolérance au risque de l'organisation.

Synthèse et mise en correspondance des règles
Élaborer et maintenir le cadre intégré de contrôle de la sécurité d'une organisation; extraire de l'information de nombreuses sources et lignes directrices en matière de réglementation.

Déclenchement d'évaluations
Mener périodiquement des évaluations automatisées, ou déclenchées automatiquement par des changements aux applications ou aux processus d'affaires.

Automatisation des indicateurs de risque clés
Automatiser la collecte et la visualisation des mesures d'indicateurs de risque clés afin de permettre à l'organisation d'évaluer et de gérer son exposition au risque.

Attribution de responsabilités
Utiliser des processus libre-service pour attribuer des responsabilités liées à la cybersécurité au sein des équipes, afin d'améliorer l'efficience et de mieux les aligner sur les responsables des risques.

Tests des contrôles
Automatiser les tests des contrôles afin d'évaluer constamment l'efficacité des contrôles et de fournir des mises à jour en temps quasi réel de la situation de sécurité de l'organisation.

17
Idm
Gestion du cycle de vie de l'identité

18
Pam
Gestion des accès privilégiés

Gestion de l'identité et de l'accès (GIA)

Gestion des rôles
Utiliser un moteur d'IA pour fournir des recommandations sur la gestion des rôles, simplifiant ainsi la tâche difficile, coûteuse et fastidieuse de tenir à jour les définitions de rôles pour l'organisation.

Moteur d'extraction de rôles
Élargir le moteur de gestion des rôles pour couvrir l'extraction de rôles auprès de sources de données multiples, avec recommandation de nouveaux rôles et droits.

Moteur de recommandation d'accès
Simplifier le processus de demande d'accès par l'analyse de sources de données variées, notamment les demandes d'accès de groupe de pairs et les demandes d'accès traditionnel, et recommander le niveau d'accès requis pour un utilisateur.

Analyse de la certification des accès
Analyser différents ensembles de données et appliquer l'analytique pour améliorer le processus de certification par la préapprobation d'éléments de certification en fonction des données de la demande d'accès, la détection des anomalies dans le cycle d'attestation et l'utilisation des données du groupe de pairs pour calculer un indice de confiance permettant aux examinateurs de prendre des décisions éclairées.

Données sur l'utilisation des accès pour le moteur d'analytique
Incorporer les données sur l'utilisation des accès au moteur d'analytique pour l'aider à générer davantage de perspectives éclairées et efficaces.

À l'extrémité la plus sophistiquée du spectre des technologies, voici quelques utilisations potentielles des technologies d'IA et d'analytique aux fins de cybersécurité.

Sécurité des systèmes

Efficacité des contrôles
Augmenter et évaluer l'efficacité des outils testés, comme les pare-feux, les passerelles de procuration et les solutions de prévention de la perte de données, en surveillant les données de journal disponibles pour ensuite repérer et corriger les mauvaises configurations.

Renseignements sur les cybermenaces

Détection des cyberrisques
Déterminer ou prévoir les risques que les humains et les systèmes fondés sur des règles ont souvent de la difficulté à repérer, y compris les nouvelles catégories de risques, les signaux diffus et les sources potentielles de futurs risques, comme l'utilisation accrue des médias sociaux.

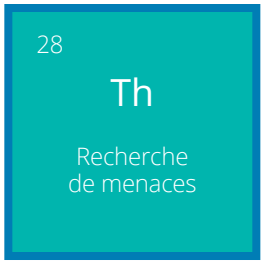
Détection des menaces

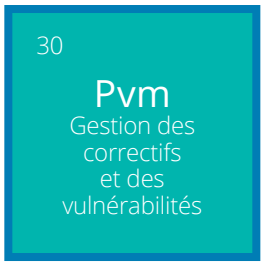
Détection des comportements anormaux
Aider à repérer les activités inusitées d'accès aux données et les activités malveillantes au sein des applications en se concentrant sur les ouvertures de session, les changements de comportement des utilisateurs et les changements non approuvés.

Découverte de menaces
Surveiller les activités et les entités pour établir les comportements normaux, et détecter les sources d'anomalies qui pourraient entraîner des risques potentiels, comme la fraude, le blanchiment d'argent et les menaces internes.

Nettoyage et priorité des alertes
Utiliser l'apprentissage machine pour automatiser considérablement le premier niveau de tri en fonction de facteurs comme le type d'attaque, la fréquence et l'expérience antérieure.

Enquête et soutien ciblés
Utiliser une plate-forme de données massives pour générer de nouvelles perspectives à l'aide de l'analyse historique, permettant ainsi de tenir rapidement et efficacement des enquêtes sur les incidents basées sur des données courantes et historiques.





Recherche de menaces et gestion de la vulnérabilité

Recherche de menaces
Repérer rapidement les nouvelles menaces par l'importation de tactiques, techniques, procédures et schémas d'attaque connus ainsi que les renseignements sur les vulnérabilités et les mesures correctives, afin de neutraliser les menaces tôt dans le cycle d'attaque.

Balayage de vulnérabilités
Utiliser des robots pour lancer et effectuer un balayage des applications, des systèmes et d'autres actifs aux fins de détection des vulnérabilités, évaluer les risques et établir les priorités du calendrier des correctifs.

Examen des configurations
Utiliser des robots pour examiner les configurations de système afin d'assurer le renforcement de base et l'absence de mauvaises configurations.

Modélisation des trajectoires d'attaque
Effectuer une analyse prédictive des données de sécurité pour établir les points d'entrée vulnérables et la trajectoire probable qu'un attaquant pourrait utiliser pour accéder aux systèmes.

Des promesses à la réalisation

Ces temps-ci, les technologies d'IA génèrent beaucoup d'effervescence. Il est maintenant temps de passer de la parole aux actes. Voici sept mesures que vous pouvez commencer à prendre dès maintenant pour rehausser les cybercapacités de votre organisation grâce à l'utilisation des technologies d'IA et d'analytique.

1

Tournez-vous vers l'avenir
Collaborez avec votre écosystème pour contribuer à mieux définir l'avenir de ces nouvelles et puissantes cybertechnologies.

2

Renseignez-vous et informez vos équipes
Comprenez les occasions d'affaires associées aux technologies d'IA et à l'analytique liées à la cybersécurité, en participant activement à des tribunes internes et à des processus de prise de décisions afin d'apporter une contribution inestimable.

3

Réévaluez le contexte des risques et des menaces
Comprenez bien les répercussions des nouvelles technologies et établissez des interventions appropriées aux fins de gestion des risques.

4

Redéfinissez votre modèle de responsabilisation
Songez à l'incidence qu'auront les changements apportés à l'environnement d'exploitation sur le contexte des risques et les contrôles nécessaires; puis, modifiez en conséquence les rôles et responsabilités des membres de votre équipe de cybersécurité.

5

Simplifiez votre cadre de contrôle
Favorisez une conception avisée en matière de risques pour les nouveaux systèmes, technologies et cadres de contrôle afin de réduire les niveaux de contrôle superflus, et de créer des capacités plus préventives et mieux automatisées dès le départ.

6

Commencez à petite échelle et progressez rapidement
Élaborez une stratégie pratique pour appliquer les technologies d'IA et l'analytique à la cybersécurité en recherchant des occasions à forte incidence et à faible complexité, dont les données sont disponibles immédiatement, et dont les capacités actuelles sont insuffisantes.

7

Repensez votre stratégie en matière de talents spécialisés en cybersécurité
Révisez votre stratégie en matière de talents, en prenant des mesures pour vous assurer que des professionnels très compétents en la matière sont aux commandes de votre démarche de cybersécurité.

Les technologies d'IA et l'analytique peuvent propulser les cybercapacités de votre entreprise au prochain niveau. En prenant les devants pour appliquer ces innovations perturbatrices à la cybersécurité, vous pouvez faire pencher la balance en votre faveur et rester à l'abri des menaces.

Personnes-ressources

Nick Galletto
Leader mondial et canadien
Services liés aux cyberrisques
ngalletto@deloitte.ca
416-601-6734

Marc MacKinnon
Leader national
Stratégies de cyberrisques
mmackinnon@deloitte.ca
416-601-5993

Dina Kamal
Leader
Cyberintelligence artificielle, Omnia
dkamal@deloitte.ca
416-775-7414

Beth Dewitt
Leader nationale
Cybersécurité
bdewitt@deloitte.ca
416-643-8223

Rocco Galletto
Leader national
Cybervigilance
rgalletto@deloitte.ca
416-643-8718

Kevvie Fowler
Leader national
Cyberrésilience
kfowler@deloitte.ca
416-867-8149

Paul Hanley
Leader national
Cyberinnovation
phanley@deloitte.ca
416-956-9090

Deloitte.

www.deloitte.ca

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans de nombreux secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500[MD] par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte ont une influence marquante – y compris les 9 400 professionnels au Canada – veuillez nous suivre sur LinkedIn, Twitter ou Facebook.

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.

Conçu et produit par le Service de conception graphique de Deloitte au Canada. 18-5679M