Devolutions

LES 5 PRINCIPAUX RISQUES EN CYBERSÉCURITÉ

POUR LES PROFESSIONNELS DE L'INFORMATIQUE EN 2025

15 JANVIER 2025

RÉSUMÉ

Tout au long de l'année 2025, nous assisterons à des avancées et des innovations remarquables dans le monde numérique qui réinventeront et redéfiniront ce qui est possible. Cependant, il existe également un aspect plus sombre à cette histoire. Dans les mois à venir, de nouvelles menaces en matière de cybersécurité feront leur apparition, tandis que les menaces existantes deviendront plus dangereuses et coûteuses.

Dans ce rapport, nous examinons cinq risques critiques de cybersécurité pour les professionnels de l'informatique en 2025. En plus d'explorer les causes et les conséquences, nous partageons également des stratégies pratiques et des conseils pour permettre aux professionnels de l'informatique d'être proactifs, de se préparer et de guider leur organisation de manière sûre et réussie.

RISQUE Nº1

LA MONTÉE DE L'AI ADVERSE

Selon le rapport CompTIA IT Industry Outlook 2024, 33% des organisations utilisent l'IA de manière limitée ou modérée, et 22% des organisations s'engagent activement dans l'intégration de l'IA à grande échelle dans divers flux de travail opérationnels — y compris ceux qui soutiennent et renforcent la cybersécurité elle-même.

En effet, de nombreuses organisations utilisent déjà (ou mettront bientôt en œuvre) l'IA pour améliorer la détection des menaces, optimiser la réponse aux incidents, effectuer une détection avancée des malwares et contrecarrer les tentatives de connexion non autorisées en analysant des données biométriques et les comportements des utilisateurs. Voilà la bonne nouvelle.

La mauvaise nouvelle est que les cybercriminels s'intéressent également de très près à l'IA ; non pas pour se protéger, mais pour mener des attaques. Cette approche malveillante, qui consiste à utiliser l'IA pour manipuler des systèmes d'IA en exploitant des vulnérabilités ou en introduisant des données malicieuses pour échapper à la détection, est connue sous le nom d'IA adverse — et elle a le potentiel de semer le chaos et de causer de nombreuses nuits blanches aux professionnels de l'informatique en 2025 et au-delà.

Voici certains types et exemples de menaces impliquant l'IA adverse :

- Brèches de sécurité qui volent des données et commettent des vols d'identité. Bien que ce type de menace ne soit pas nouveau, l'IA permet aux cybercriminels de mener des attaques à une vitesse, une précision et une échelle sans précédent. Par exemple, fin 2022, des cybercriminels ont attaqué T-Mobile en utilisant une API équipée d'IA pour accéder aux données privées d'environ 37 millions de dossiers clients, incluant leurs noms complets, numéros de contact et codes PIN.

- Botnets d'IA qui mènent des attaques par déni de service distribué (DDoS), exécutent des attaques de bourrage d'identifiants et effectuent des attaques à grande échelle contre des systèmes ciblés. Par exemple, il y a quelques années, des cybercriminels ont attaqué Pulse Secure VPN en utilisant des algorithmes d'IA pour scanner Internet à la recherche de serveurs vulnérables, les compromettre automatiquement et les ajouter à un botnet utilisé pour lancer des attaques DDoS contre diverses cibles de grande valeur.

- Manipulation des modèles d'IA (également appelée empoisonnement des données), de sorte qu'ils produisent finalement des résultats erronés ou prennent de mauvaises décisions. Bien qu'il ne s'agisse pas d'un type d'attaque conventionnel conçu pour voler des données ou commettre des vols d'identité, cela peut être extrêmement déstabilisant et coûteux pour les victimes qui ignorent totalement qu'elles ont été ciblées.

- Vol des modèles utilisés dans les systèmes d'IA, ce qui représente pour de nombreuses organisations une propriété intellectuelle précieuse et confidentielle.

COMMENT LES PROFESSIONNELS DE L'INFORMATIQUE PEUVENT CONTRER L'IA ADVERSE

Il n'existe pas de réponses faciles ni de solutions rapides pour faire face à l'IA adverse (ou à tout autre risque exploré dans ce rapport). Cependant, ne rien faire et « espérer ne pas être touché » n'est absolument pas une option.

Les coûts potentiels d'une cyberattaque sont plus élevés que jamais, et cela ne concerne pas uniquement les grandes entreprises. Les petites et moyennes entreprises (PME) sont de plus en plus ciblées par les cybercriminels, qui sont attirés par des défenses en cybersécurité relativement plus faibles (et dans

certains cas pratiquement inexistantes). Selon une étude d'Accenture, 43% de toutes les cyberattaques dans le monde visent désormais spécifiquement les PME. De plus, notre portrait sur la sécurité informatique chez les PME québécoises a révélé que 78% des PME sont plus préoccupées par la cybersécurité qu'il y a un an, et 69% ont subi au moins une cyberattaque au cours de la dernière année.

Plus loin dans ce rapport, nous examinerons de plus près comment les professionnels de l'informatique peuvent protéger leur organisation contre les coûts massifs — et dans certains cas catastrophiques — d'une violation. Pour l'instant, poursuivons notre discussion sur la manière dont ils peuvent lutter contre l'IA adverse. La firme mondiale de conseil Grant Thornton recommande une approche et un plan couvrant huit domaines clés :

- **Politiques et procédures :** Examiner et, si nécessaire, mettre à jour les politiques et procédures existantes pour définir des exigences de sécurité spécifiques à l'IA, désigner des rôles responsables des opérations d'IA et garantir la mise en œuvre des directives de sécurité.

- **Modélisation des menaces :** Réaliser des exercices de modélisation des menaces pour identifier et évaluer l'impact des menaces potentielles pesant sur les outils et systèmes d'IA (y compris les menaces décrites précédemment, comme les violations de la vie privée et les botnets d'IA).

- **Gouvernance des données :** S'assurer que les données sont correctement classifiées, protégées et gérées tout au long de leur cycle de vie. Les aspects de gouvernance incluent l'identification des rôles et responsabilités, les évaluations de la qualité des données, la validation des données et les usages acceptables des données.

- **Contrôle d'accès :** Mettre en place des politiques de gestion des identités et des accès (IAM) pour répondre aux questions clés telles que : qui doit avoir accès à quels systèmes et données d'IA? Comment et quand cet accès doit-il être réévalué? Quels types de rapports, journaux et alertes doivent être en place? Quels contrôles d'accès renforcés sont nécessaires si l'IA a accès à des informations personnellement identifiables (PII) ou à d'autres données sensibles?

- **Cryptage et stéganographie :** Utiliser des techniques telles que le filigrane numérique (ajout d'une signature numérique) ou des données radioactives (modifications mineures d'un fichier ou des données d'entraînement) pour suivre les modèles d'IA et garantir leur intégrité.

- **Sécurité des terminaux :** Les cybercriminels ont toujours privilégié les terminaux, comme les ordinateurs portables et les appareils mobiles. Ce qui est nouveau — et bien pire — c'est qu'ils utilisent désormais l'IA pour intensifier leurs attaques sur les terminaux tout en rendant les violations encore plus difficiles à détecter. Les solutions de sécurité des terminaux renforcées par des analyses comportementales et des entités utilisateur (UEBA) peuvent aider à repérer les premiers signes d'une attaque d'IA, afin qu'elles soient stoppées avant de s'intensifier.

- **Gestion des vulnérabilités :** Cela inclut des protocoles de sécurité robustes, des procédures de test et de validation, ainsi qu'une surveillance et une maintenance continues. Il est également crucial pour les professionnels de l'informatique d'appliquer régulièrement les mises à jour et correctifs logiciels, ainsi que de réaliser des évaluations régulières des composants d'infrastructure IA pour identifier et corriger les vulnérabilités.

- **Sensibilisation à la sécurité :** Enfin, et non des moindres, tout le personnel de l'organisation doit être conscient de tous les risques en cybersécurité (y compris ceux liés à l'IA) et formé en conséquence.

RISQUE Nº2

LA MONTÉE DES ATTAQUES D'HAMEÇONNAGE AVEC « DEEPFAKES »

La pratique consistant à envoyer des emails et autres messages frauduleux prétendant provenir d'entreprises réputées ou de personnes de confiance — mieux connue sous le nom de hameçonnage — reste une menace majeure.

Selon l'*Index IBM X-Force Threat Intelligence 2023*, l'hameçonnage demeure le principal vecteur d'infection, jouant un rôle dans 41% des attaques. Par ailleurs, le *Rapport Verizon 2024 sur les enquêtes sur les violations de données* a révélé que le taux global de signalement d'hameçonnage a augmenté au cours des dernières années, et que le temps médian nécessaire pour qu'un utilisateur tombe dans le piège est inférieur à une minute.

Aujourd'hui, les cybercriminels ont ajouté une nouvelle arme puissante à leur arsenal : les « deepfakes », qui utilisent des technologies avancées pour rendre les attaques plus difficiles à détecter — et donc plus difficiles à prévenir. Voici quelques exemples :

- Créer de faux profils pour piéger des victimes. Une analyse réalisée en 2022 par des chercheurs du Stanford Internet Observatory a identifié plus de 1000 faux profils LinkedIn qui semblaient générés par une IA.

- Utiliser des technologies d'échange de visages pour usurper l'identité de quelqu'un lors d'appels vidéo — ce qu'un cybercriminel a précisément fait en 2023 pour inciter une victime à transférer 622 000 $.

- Cloner la voix d'une personne et laisser des messages vocaux à une victime, ou dans certains cas, interagir directement avec elle en temps réel. On estime que 37% des organisations ont déjà été ciblées par une tentative de fraude vocale utilisant des « deepfakes ».

CE QUE LES PROFESSIONNELS DE L'INFORMATIQUE PEUVENT FAIRE POUR DÉTECTER ET CONTRER L'HAMEÇONNAGE AVEC « DEEPFAKES »

Les professionnels de l'informatique qui souhaitent protéger leur organisation contre les attaques d'hameçonnage avec « deepfakes » — et empêcher les cybercriminels de s'introduire — devraient mettre en œuvre les actions suivantes :

- Mettre en place une authentification multifacteur. Idéalement, celle-ci devrait combiner des données biométriques avec d'autres formes de vérification, telles que des mots de passe, des codes PIN ou des confirmations verbales via des canaux sécurisés.

- Former les utilisateurs finaux à repérer les signes potentiels d'hameçonnage avec « deepfakes », et les sensibiliser à signaler immédiatement et efficacement leurs préoccupations — même si cela implique d'interrompre des flux de travail ou de manquer des échéances. Concernant les vidéos, les utilisateurs finaux devraient prêter attention à des éléments comme des mouvements des lèvres non synchronisés, des poils faciaux d'apparence artificielle, un clignement des yeux excessif ou insuffisant, ainsi que des ombres ou reflets lumineux étranges ou absents (à ce jour, de nombreux « deepfakes » ont encore du mal à reproduire correctement les lois naturelles de la physique dans une scène). Concernant l'audio, les utilisateurs devraient être attentifs à des bruits de fond ou des ambiances incohérentes, des pauses ou changements d'intonation inhabituels, ainsi qu'à des modèles de discours robotiques ou rigides. Bien sûr, tous ces éléments ne sont que des indices — et non des preuves. Cependant, les utilisateurs finaux devraient être formés à privilégier la prudence.

- Appliquer le principe du moindre privilège, qui limite les utilisateurs finaux à n'avoir accès qu'aux ressources nécessaires pour accomplir leur travail quotidien — et rien de plus.

- Utiliser une solution de gestion des accès privilégiés pour restreindre et encadrer l'accès des utilisateurs finaux aux systèmes, comptes, processus et utilisateurs. Nous aborderons l'importance du PAM plus en détail plus loin dans ce rapport.

- Adopter des systèmes de détection des « deepfakes » alimentés par l'IA, incluant ceux qui utilisent la photopléthysmographie pour détecter en temps réel les variations du volume sanguin dans les vidéos, ainsi que des outils de médecine légale audio pour analyser le spectrogramme des enregistrements vocaux et repérer des manipulations synthétiques.

Nous ne sommes qu'au début de l'ère de l'hameçonnage avec « deepfakes », et l'ampleur des tentatives que feront les cybercriminels reste à découvrir. Cependant, les professionnels de l'informatique qui prennent les devants en équipant et en préparant leurs organisations et leurs utilisateurs finaux seront bien mieux armés dans les mois et années à venir que ceux qui adoptent une approche passive d'attente — une attitude qui pourrait coûter très cher à leur organisation.

RISQUE Nº3

PRESSION POUR SE CONFORMER AUX NOUVELLES RÉGLEMENTATIONS EN MATIÈRE DE CYBERSÉCURITÉ

En 2024, plusieurs nouvelles réglementations en matière de cybersécurité sont entrées en vigueur à travers le monde, et de nombreux professionnels de l'informatique (notamment en Europe) se sont retrouvés à courir pour répondre aux exigences de conformité avant diverses échéances. Parmi les principales réglementations introduites, on peut citer :

- La directive sur les réseaux et systèmes d'information (NIS2), qui est entrée en vigueur le 16 janvier 2023 et que les États membres de l'UE devaient transposer dans leurs législations nationales avant le 17 octobre 2024. La NIS2, qui met à jour la directive NIS de 2016, uniformise les pratiques en matière de cybersécurité au sein des États membres de l'UE et vise à renforcer les défenses, à rationaliser la réponse aux incidents et à améliorer la coopération au sein de l'Union européenne.

- Le Cyber Resilience Act (CRA) de l'UE, adopté par le Conseil de l'UE le 10 octobre 2024. Le CRA impose des mesures de cybersécurité renforcées pour une grande variété de produits matériels et logiciels.

- Le règlement sur la résilience opérationnelle numérique, qui établit un cadre réglementaire en matière de résilience opérationnelle numérique. Les entités financières de l'UE doivent garantir qu'elles peuvent résister, répondre et se remettre de tous les types de perturbations et menaces liées aux technologies de l'information et de la communication (TIC). Il entrera pleinement en vigueur en janvier 2025.

- Aux États-Unis, de nouvelles règles de divulgation de la SEC sont entrées en vigueur en 2024, obligeant les organisations de toutes tailles à signaler les incidents de cybersécurité, ainsi qu'à divulguer leurs politiques de gestion des risques, leurs stratégies de sécurité et leur gouvernance.

- Les organisations actuellement certifiées selon la norme ISO 27001:2013 ont jusqu'au 31 octobre 2025 pour effectuer la transition vers la norme ISO/IEC 27001:2022 (faute de quoi leur certification expirera ou sera retirée). Bien qu'il existe un chevauchement significatif entre les deux normes, certains changements notables concernent la planification, la définition des critères de processus et la surveillance.

Veuillez noter que la liste ci-dessus n'a pas vocation à être exhaustive en ce qui concerne toutes les nouvelles règles et réglementations en matière de cybersécurité introduites en 2024 ou entrant en vigueur en 2025 et au-delà. Cependant, elle met en évidence certains des changements les plus importants et souligne que les professionnels de l'informatique ne subissent pas seulement la pression des cybercriminels pour renforcer les défenses de cybersécurité de leur organisation — ils sont également sous la surveillance des législateurs et des régulateurs, qui n'hésitent pas à imposer des amendes et des sanctions en cas de non-conformité.

CE QUE LES PROFESSIONNELS DE L'INFORMATIQUE PEUVENT FAIRE POUR SE CONFORMER AUX NOUVELLES RÉGLEMENTATIONS EN MATIÈRE DE CYBERSÉCURITÉ

CompTIA conseille aux organisations de mettre en place un Programme de Conformité en Cybersécurité en couvrant les activités essentielles suivantes :

- Créer une équipe de conformité, qui doit inclure des personnes extérieures au service informatique afin de s'assurer que la cybersécurité fait partie de la culture de l'organisation, et pas seulement de la responsabilité des professionnels de l'informatique.

- Mettre en place un processus d'analyse des risques comprenant l'identification, l'évaluation, l'analyse et la définition des tolérances.

- Établir des contrôles de sécurité pour atténuer ou transférer les risques en cybersécurité.

- Documenter les politiques concernant les contrôles ou les directives que les équipes informatiques, les utilisateurs finaux et les autres parties prenantes doivent respecter.

- Surveiller le programme à mesure que de nouvelles réglementations apparaissent ou que des règles existantes sont mises à jour.

De plus, l'une des actions les plus importantes et impactantes que les professionnels de l'informatique peuvent entreprendre pour soutenir les exigences de conformité de leur organisation est de se concentrer sur la centralisation, la protection et la surveillance des points d'accès critiques. Cela implique de mettre en œuvre des solutions permettant :

- Une gestion sécurisée des accès à distance, renforcée par l'enregistrement des sessions afin de capturer et de superviser ce que les utilisateurs finaux font lorsqu'une connexion à distance est active.

- Une gestion sécurisée des mots de passe, incluant des coffres pour protéger les identifiants et autres données sensibles de l'entreprise. Un chiffre stupéfiant : 86% des violations impliquent des identifiants volés.

- Des rapports administratifs complets, ainsi que des fonctions d'audit et de journalisation.

- L'authentification multifacteur.

- Un système d'enregistrement et de fin d'accès pour les comptes privilégiés (par exemple, numéro de ticket, accès juste-à-temps, justification de l'accès et durée de l'accès).

Il est également crucial que les professionnels de l'informatique choisissent des solutions faciles à implémenter et à utiliser, et qui réduisent — plutôt que de créer — des frictions pour les équipes travaillant à la conformité. Cela leur permet de se concentrer sur les objectifs et obligations principaux en matière de sécurité de leur organisation, plutôt que de consacrer un temps et des efforts considérables à démanteler des silos et à gérer des urgences.

RISQUE Nº4

LA MENACE CROISSANTE DES RANÇONGICIELS

> Selon le portrait de la sécurité informatique chez les PME québécoises en 2023-2024 , les rançongiciels représentent la principale menace cybernétique qui préoccupe les PME — et cela n'a rien de surprenant. Voici quelques chiffres alarmants tirés du rapport *Sophos State of rançongiciel 2024* :

Au cours de l'année écoulée, **59%** des organisations ont été ciblées par une attaque par rançongiciel.

- **70%** des attaques par rançongiciel ont entraîné le chiffrement des données.
- **32%** des victimes de rançongiciel dont les données ont été chiffrées se sont également fait voler des données.
- La demande moyenne de rançon initiale a grimpé à **2 millions de dollars**.
- **34%** des victimes de rançongiciel ont mis plus d'un mois à se remettre de l'attaque.

De plus, le *National Cyber Security Centre* (NCSC) du Royaume-Uni a émis un avertissement selon lequel la menace mondiale des rançongiciels devrait augmenter avec l'utilisation de l'IA, ce qui augmentera à la fois le volume et l'impact des attaques de rançongiciel au cours des deux prochaines années.

CE QUE LES PROFESSIONNELS DE L'INFORMATIQUE PEUVENT FAIRE POUR PRÉVENIR LES ATTAQUES PAR RANÇONGICIEL

Les rançongiciels resteront une menace majeure pendant des années (et probablement des décennies). Cependant, les professionnels de l'informatique peuvent et doivent prendre des mesures pour réduire les risques. Le *Center for Internet Security* (CIS) recommande les 15 actions suivantes :

1. Créer un plan de réponse aux incidents complet qui identifie quoi faire en cas d'attaque par rançongiciel, qui doit agir et à quel moment.

2. Mettre en place un système de sauvegarde prenant en charge plusieurs itérations ou des données archivées. Cela est essentiel au cas où une copie de la sauvegarde contiendrait des fichiers infectés ou chiffrés. Les sauvegardes doivent également être régulièrement testées pour vérifier l'intégrité des données et leur état opérationnel.

3. Utiliser des logiciels antivirus et ajouter une bannière ou une signature d'avertissement sur tous les emails pour rappeler aux utilisateurs les dangers de cliquer sur des liens et d'ouvrir des pièces jointes.

4. Si possible, désactiver les macros de script et forcer les utilisateurs finaux à visualiser les fichiers transmis par email au lieu de les ouvrir. L'intégration de malwares dans des macros est une tactique courante des attaques par rançongiciel.

5. Maintenir tous les appareils, logiciels, matériels et applications (y compris les emplacements dans le nuage) à jour et appliqués avec les derniers correctifs. Il est recommandé d'utiliser un système centralisé de gestion des correctifs.

6. Utiliser des listes blanches d'applications et des politiques de restriction logicielle. Cela permet de bloquer l'exécution de programmes dans des emplacements courants des rançongiciels (par exemple, les dossiers temporaires).

7. Utiliser un serveur proxy pour l'accès à Internet.

8. Utiliser un logiciel de blocage de publicités.

9. Restreindre l'accès aux vecteurs courants des rançongiciels, comme les réseaux sociaux et les comptes email personnels.

10. Appliquer le principe du moindre privilège (POLP).

11. Mettre en œuvre une segmentation du réseau et une architecture zéro confiance (*zero-trust*).

12. Évaluer et surveiller les tiers ayant accès au réseau, et s'assurer qu'ils respectent toutes les meilleures pratiques en matière de cybersécurité.

13. Participer à des programmes et organisations de partage d'informations sur la cybersécurité (par exemple, *MS-ISAC* et *InfraGard*).

14. Fournir aux utilisateurs finaux une formation continue en cybersécurité sur des sujets tels que l'ingénierie sociale et l'hameçonnage, y compris comment repérer les signes de « deepfakes » vidéo et audio, comme discuté précédemment.

15. Mettre en œuvre un plan de signalement qui informe les utilisateurs finaux sur la manière et le moment de signaler une activité inhabituelle ou suspecte.

RISQUE Nº5

RISQUER LA RUINE FINANCIÈRE APRÈS UNE CYBERATTAQUE

> Toutes les cyberattaques réussies sont déstabilisantes et coûteuses. Mais pour les PME, le risque peut être bien plus grand. Un rapport d'IBM et du Ponemon Institute a révélé que le coût moyen d'une violation de données pour les PME a grimpé à 2,98 millions de dollars par incident. Par ailleurs, des recherches distinctes ont montré que 6 PME sur 10 cessent leurs activités dans les six mois suivant une attaque. En d'autres termes : les PME risquent non seulement de perdre leurs ventes, économies, clients, parts de marché et réputation. Elles risquent de tout perdre.

CE QUE LES PROFESSIONNELS DE L'INFORMATIQUE PEUVENT FAIRE POUR ÉVITER D'ÊTRE ANÉANTIS PAR UNE CYBERATTAQUE

Les professionnels de l'informatique devraient utiliser les recommandations décrites dans ce rapport pour orienter leurs efforts en matière de cybersécurité et servir de liste de contrôle. Certes, en raison de contraintes budgétaires, de nombreuses PME ne pourront pas tout mettre en œuvre (par exemple, l'installation de systèmes de détection des « deepfakes » alimentés par l'IA). Cependant, plusieurs mesures fondamentales devraient faire partie de leur stratégie et de leur plan, notamment :

- Appliquer le principe du moindre privilège, une architecture zéro confiance et la segmentation du réseau.
- Utiliser un gestionnaire de mots de passe robuste.
- Former et tester les utilisateurs finaux.
- Déployer une solution de gestion des accès privilégiés (PAM) pour surveiller et encadrer les comptes privilégiés.

À PROPOS DE LA GESTION DES ACCÈS PRIVILÉGIÉS (PAM)

De nombreuses organisations se tournent vers l'assurance cybersécurité comme moyen de se protéger contre les coûts potentiellement catastrophiques d'une violation. En réponse, un nombre croissant de fournisseurs d'assurance exigent que des contrôles PAM soient en place comme condition préalable à la couverture. En général, au minimum, ces assureurs souhaitent une preuve des éléments suivants :

- Authentification multifacteur pour les accès à distance, soit via des fonctionnalités intégrées, soit via l'intégration avec des outils tiers (la MFA par SMS est progressivement abandonnée en raison du grand nombre d'attaques réussies par échange de carte SIM).

- Comptes administrateurs et configurations par défaut mis à jour, pour empêcher les cybercriminels et les initiés malveillants d'exploiter des identifiants couramment disponibles.

- Suppression des droits administrateurs locaux sur les ordinateurs de bureau/portables, et gestion des comptes locaux des postes de travail.

- Utilisation de délais d'inactivité pour éviter les sessions d'accès à distance prolongées, qui ne devraient être ouvertes que pendant la durée strictement nécessaire.

- Remplacement des comptes administrateurs ultra-puissants par plusieurs comptes privilégiés définissant les permissions nécessaires pour chaque système auquel les administrateurs doivent accéder.

Contrôles avancés exigés par certains assureurs

En plus des éléments ci-dessus, certaines compagnies d'assurance demandent que les souscripteurs disposent de contrôles PAM plus avancés, notamment :

- Des options d'authentification telles que la correspondance numérique (number matching) pour tous les utilisateurs (et pas seulement les utilisateurs privilégiés).

- Des capacités de check-out, incluant des approbations intégrées pour limiter qui peut demander l'accès à un compte privilégié, et pour combien de temps.

- L'élévation de privilèges juste-à-temps (JIT), transformant les comptes précédemment hautement privilégiés en comptes sans privilèges permanents, et le provisionnement des utilisateurs JIT (les comptes privilégiés sont créés au besoin pour une durée spécifique, puis supprimés une fois les tâches terminées).

LE MOT DE LA FIN

Le paysage des cybermenaces est volatile, et prédire quoi que ce soit avec une certitude absolue est rarement une bonne idée — les choses évoluent sur une base mensuelle, hebdomadaire, et parfois même quotidienne. Cependant, il est indéniable que les professionnels de l'informatique qui, avec leurs collègues, adoptent et appliquent les recommandations de ce livre blanc renforceront considérablement leur profil de cybersécurité et réduiront de manière significative leurs risques.

Et les professionnels de l'informatique travaillant dans des PME pourraient aller encore plus loin : leurs efforts en cybersécurité, leur leadership et leur vigilance pourraient faire la différence entre le fait que leur organisation reste en sécurité et prospère en 2025 — ou qu'elle soit victime d'une attaque majeure, ce qui pourrait entraîner sa disparition complète. Les enjeux sont vraiment aussi élevés. Et ils ne cessent d'augmenter.

EN SAVOIR PLUS ET ALLER PLUS LOIN

Devolutions propose une suite de solutions qui aident les professionnels de l'informatique à relever et à atténuer tous les risques abordés dans ce livre blanc, en appliquant la gestion des accès privilégiés (PAM), en établissant une segmentation du réseau, en protégeant les mots de passe, en permettant l'enregistrement des sessions, et bien plus encore. De plus, nos solutions sont abordables pour les PME, qui disposent généralement de budgets limités en matière de sécurité informatique. Elles s'intègrent également rapidement et facilement dans l'environnement, soutiennent les exigences de conformité, et augmentent la productivité, l'efficacité et l'expérience quotidienne des utilisateurs finaux.

Pour en savoir plus et aller plus loin, envoyez un email à **sales@devolutions.net** et demandez une consultation pour discuter de vos défis et objectifs en matière de cybersécurité. Découvrez comment nos solutions peuvent vous aider à établir visibilité et contrôle, réduire les risques, répondre aux exigences de conformité, améliorer la productivité des utilisateurs finaux et faire avancer votre organisation!