Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Défense contre les menaces d'exfiltration de données

SÉRIE GESTIONNAIRES

Canada

Avant-propos

L'ITSM.40.110, *Défense contre les menaces d'exfiltration de données*, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, envoyez un courriel ou téléphonez au Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 12 avril 2023.

Historique des modifications

Version	Modifications	Date
1	Première version.	12 avril 2023

D97-4/40-110-2023F-PDF
978-0-660-48081-7

Aperçu

Le National Institute of Standards and Technology (NIST) définit l'exfiltration comme étant le transfert non autorisé de données d'un réseau, d'un système ou d'un appareil [1]. L'exfiltration de données est une tactique utilisée par les auteures et auteurs de menace pour atteindre leurs objectifs, notamment le vol de données, l'extorsion et les gains financiers (p. ex. les rançongiciels ou l'exploitation des menaces internes) et l'interruption de service. Les attaques par exfiltration de données peuvent prendre diverses formes, notamment l'espionnage de données, le vol d'identifiants d'utilisateur ou de système, le vol de données financières, la compromission d'identité numérique et la désanonymisation de données. Pour se protéger contre ces attaques, votre organisation devrait sécuriser ses processus de cycle de vie des données (p. ex. création, exploitation et destruction) de bout en bout. Le présent document traite de certaines techniques d'exfiltration de données connues et propose des stratégies de protection dont le déploiement permet d'atténuer les répercussions de ces menaces.

Une exfiltration de données peut être un indice de compromission réseau et la confirmation d'une activité menée par une auteure ou un auteur de menace dans votre réseau. La détection d'une exfiltration de données pourrait s'avérer la dernière ligne de défense pour protéger les données de votre organisation contre une compromission totale. Un événement d'exfiltration de données doit être traité comme une atteinte à la protection des données et devrait déclencher le processus de gestion des incidents de votre organisation. Selon l'ampleur et le secteur de l'industrie, un tel événement ayant des conséquences sur la productivité, la réputation ou les finances d'une organisation pourrait donner lieu à des exigences réglementaires et juridiques en matière de déclaration. Empêcher les auteures et auteurs de menace d'exécuter la phase d'exfiltration de données peut aider à contenir et à déjouer une attaque par compromission réseau en cours. Pour ce faire, l'organisation doit faire appel à une stratégie de protection des données multicouches qui repose sur des pratiques sécurisées de gouvernance des données, des contrôles de sécurité techniques pour renforcer les systèmes de données, le renforcement des mécanismes d'identification et d'authentification, et la formation visant à sensibiliser les utilisatrices et utilisateurs. L'hameçonnage, les maliciels, les rançongiciels et les menaces internes peuvent mener à un événement d'exfiltration de données. Par exemple, une auteure ou un auteur de menace détenant des moyens sophistiqués peut se servir d'attaques par harponnage et par maliciel pour infiltrer le réseau d'une organisation afin d'exfiltrer des secrets commerciaux ou nationaux. Des auteures et auteurs de menace motivés par l'appât du gain auront recours à des programmes malveillants pour voler l'information de cartes de paiement électronique des systèmes de traitement des paiements, une technique que l'on appelle le copiage de cartes de paiement (lorsque des auteures et auteurs de menace injectent du code sur mesure dans le site Web d'une organisation pour extraire de l'information de cartes de paiement).

Table des matières

Liste des figures

Liste des annexes

1 Introduction

Les données sont essentielles au bon fonctionnement de toute organisation. Ainsi, les risques liés à la cybersécurité à l'égard de la confidentialité, de l'intégrité et de la disponibilité des données qui ne sont pas réglés peuvent avoir des répercussions importantes sur les objectifs opérationnels de l'organisation. Les signalements d'incidents en lien avec l'atteinte à la protection des données sont en hausse puisque les auteures et auteurs de menace de même que les groupes cybercriminels exploitent de plus en plus les lacunes dans les stratégies en matière de gestion de la sécurité des données de nombreuses organisations. Beaucoup d'organisations ont de la difficulté à établir et à mettre en œuvre des contrôles techniques efficaces pour assurer la sécurité des processus de cycle de vie de leurs données. Les unités fonctionnelles et les utilisatrices et utilisateurs introduisent des risques pour la sécurité par la voie d'approches isolées de création et de gestion des données organisationnelles. Les auteures et auteurs de menace ciblent généralement l'information sensible, notamment :

- les renseignements exclusifs d'entreprise;
- les secrets commerciaux;
- la propriété intellectuelle;
- l'information nominative de membres de la clientèle ou du personnel;
- les renseignements opérationnels de nature délicate;
- les paramètres de configuration de système;
- les variables environnementales;
- les justificatifs d'authentification.

Les auteures et auteurs de menace lancent souvent une panoplie d'attaques contre des organisations, leur principal objectif étant généralement d'accéder sans autorisation aux données organisationnelles de nature délicate. Afin d'assurer la sécurité des données d'entreprise contre les menaces d'exfiltration, votre organisation doit être au fait des techniques d'attaque qui pourraient avoir des répercussions sur vos données. Votre organisation devrait adopter une approche de défense axée sur les menaces qui permet de repérer de manière proactive ces menaces et de mettre en œuvre des contrôles de sécurité pour protéger les données.

1.1 Exfiltration de données et cadres de sécurité

L'exfiltration de données est une tactique courante que l'on retrouve dans des cadres d'intrusion émanant d'auteures et auteurs de menace, comme la base de connaissances MITRE ATT&CK, les contrôles CIS et la chaîne cybercriminelle.
La section ci-dessous présente quelques cadres de sécurité et une analyse de l'exfiltration de données.

1.1.1 Processus de gestion des risques liés à la sécurité des technologies de l'information (ITSG-33)

Dans le cadre du processus de gestion des risques liés à la sécurité des TI, le gouvernement du Canada (GC) et ses ministères et organismes doivent adopter et tenir à jour des contrôles de sécurité pour protéger leurs activités opérationnelles des menaces liées aux TI. L'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2], définit un ensemble de processus et de profils de contrôle pour la conduite des activités opérationnelles des ministères et organismes du GC. Les ministères et organismes fédéraux doivent également mener une évaluation des menaces et des risques (EMR) pour leurs projets de TI. L'évaluation des menaces devrait établir les auteures et auteurs de menace ainsi que les contrôles correspondants afin de sécuriser leurs processus opérationnels et ainsi contrer les menaces d'exfiltration de données.

1.1.2 Cadre MITRE ATT&CK

Le cadre MITRE ATT&CK (pour *Adversarial Tactics, Techniques, and Common Knowledge*) est une base de connaissances des techniques et des tactiques employées par les auteures et auteurs de menace dans le cadre d'événements d'intrusion signalés publiquement. Le cadre décrit l'exfiltration de données comme étant une tactique des auteures et auteurs de menace visant à voler des données d'un réseau cible et impliquant souvent l'utilisation de méthodes complémentaires pour s'assurer que les activités de transfert de données ne sont pas détectées. MITRE divise la tactique d'exfiltration en plusieurs techniques détaillées, dont l'exfiltration par l'infrastructure de commande et de contrôle (C2), l'exfiltration par l'intermédiaire de référentiels de code logiciel et de services infonuagiques, ainsi que l'exfiltration par des canaux cachés. Pour en savoir plus sur les autres techniques d'exfiltration, veuillez consulter le site Web de MITRE [3].

1.1.3 Contrôles du Center for Internet Security (CIS)

Le CIS recommande une série de contrôles de sécurité essentiels que les organisations devraient prioriser pour protéger leurs biens contre les attaques connues. Le CIS a publié la version 8 de sa liste de contrôles de sécurité essentiels, laquelle définit 18 contrôles prioritaires et 153 mesures de protection divisées en trois groupes de mise en œuvre (IG pour *Implementation Group*). L'utilisation du navigateur de contrôles de sécurité du CIS [4] et la mise en correspondance des contrôles et des techniques d'exfiltration ATT&CK ont permis d'établir 11 contrôles prioritaires et 25 mesures de protection pour atténuer les attaques par exfiltration de données. Pour obtenir plus d'information sur cette mise en correspondance, veuillez consulter l'annexe A.

2 Attaques par exfiltration de données

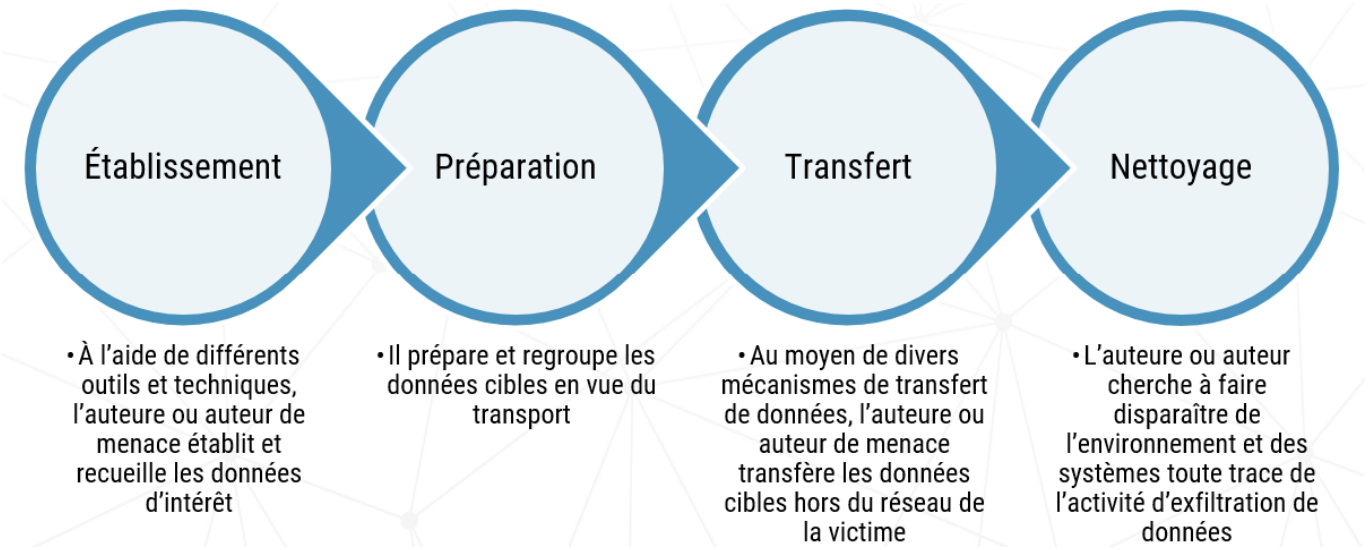
Il est important de comprendre les méthodes qu'emploient les auteures et auteurs de menace pour lancer les attaques par exfiltration de données dans le but de choisir les contrôles de détection et de prévention appropriés. Cette section porte sur les phases d'une attaque par exfiltration de données et les méthodes d'exfiltration.

2.1 Phases d'une attaque par exfiltration de données

Les auteures et auteurs de menace procèdent généralement à l'exfiltration de données en suivant les quatre phases générales suivantes :

1. **Établissement :** Cette phase consiste à établir et à recueillir des ensembles de données ou de l'information d'intérêt. Elle peut impliquer le déplacement latéral de l'auteure ou de l'auteur de menace dans l'environnement et la recherche dans les flux de données ou les référentiels pour établir et recueillir les données cibles. Dans certaines attaques par extorsion de données, cette phase s'effectue après que les données exfiltrées ont été transférées à une infrastructure contrôlée par le pirate.
2. **Préparation :** Cette phase englobe un ensemble d'activités ou de mécanismes exécutés pour préparer les données cernées avant l'exfiltration. Elle peut comprendre la compression, le chiffrement ou l'encodage des données, ou toute autre technique préalable visant à dissimuler les données avant qu'elles soient transférées hors de leur environnement.
3. **Transfert :** Cette phase implique l'utilisation de mécanismes de transport de données pour transmettre les données cibles de l'environnement où elles se trouvent à un système ou à un réseau contrôlé par le pirate. Elle peut également comprendre le recours à des protocoles réseau courants, à des outils de dissimulation ou à des capacités de supports physiques pour compléter cette étape.
4. **Nettoyage :** Cette phase est facultative selon le degré de sophistication des moyens détenus par l'auteure ou l'auteur de menace. Les adversaires peuvent prendre des mesures additionnelles pour effacer toutes traces de leurs activités, généralement peu de temps après l'intrusion initiale et de façon répétée au besoin, surtout lorsqu'il est impossible de désactiver les capacités de journalisation du système. Parmi les exemples d'activités de nettoyage, notons la suppression de copies originales, la suppression des journaux d'événements ou le déclenchement d'une attaque par diversion pour tromper les propriétaires de système.

Figure 1 : Phases d'une attaque par exfiltration de données



2.2 Méthodes d'exfiltration

Les auteures et auteurs de menace peuvent se servir de l'infrastructure réseau et des applications système d'une organisation pour faciliter le transfert illicite de données. Les systèmes et les outils légitimes d'entreprise peuvent être utilisés pour transférer des données à un environnement contrôlé par des auteures et auteurs de menace. La présente section porte sur les techniques qu'emploient les auteures et auteurs de menace pour exécuter ces activités.

- **Mécanismes cryptographiques :** Le chiffrement et d'autres mécanismes cryptographiques peuvent être employés pour dissimuler les données cibles et pour neutraliser les contrôles de surveillance et de détection des données. Les auteures et auteurs de menace mettent à profit les algorithmes cryptographiques disponibles dans l'environnement cible ou déploient des solutions cryptographiques personnalisées qui sont conçues pour contourner les contrôles de détection. Les contrôles de surveillance de la sécurité des données reposant sur la recherche de chaîne de données peuvent être facilement neutralisés au moyen de cette technique.
- **Transformation des données :** Les auteures et auteurs de menace peuvent utiliser des méthodes de transformation des données comme la substitution de modèle de texte, l'encodage de données, le brouillage de données ou la compression personnalisée pour réduire la taille des données cibles avant tout traitement et toute exfiltration de données supplémentaires. Les technologies de transformation des données comme les outils de traitement texte-voix ou texte-image peuvent être employées pour éviter les systèmes de détection de texte. Il se peut que les outils de compression de données n'offrent pas les capacités nécessaires pour éviter les contrôles de détection, mais ils peuvent servir lors de la phase de préparation des données pour réduire la taille des données utiles avant le chiffrement et le transfert des données.
- **Protocoles réseau :** Compte tenu du fait qu'il est relativement facile de les configurer, les auteures et auteurs de menace utilisent souvent des protocoles réseau sur mesure pour exfiltrer et transférer les données volées. Les protocoles réseau courants, ainsi que les protocoles réseau non utilisés, peuvent également être exploités pour configurer des canaux cachés et utilisés pour transporter des données volées. Les auteures et auteurs de menace

peuvent également recourir à des techniques de tunnellisation de protocole et de mise en miroir de trafic réseau pour acheminer le trafic réseau légitime d'un dispositif de passerelle réseau compromis à un environnement contrôlé par une auteure ou un auteur de menace. Par exemple, le protocole DNS (pour *Domain Name System*; système d'adressage par domaines) peut être exploité de façon à exfiltrer des données par des requêtes DNS, une technique appelée « tunnellisation DNS ».

- **Stéganographie :** Ce concept consiste à incorporer des données dans un autre format de fichier pour qu'elles ne puissent pas être détectées. La stéganographie est utilisée à des fins légitimes comme dans les filigranes numériques. Toutefois, des auteures et auteurs de menace ont incorporé cette technique pour cacher des données volées dans des images ou des métadonnées de fichier avant de les exfiltrer du réseau de la victime.
- **Commande et contrôle (C2) :** Des canaux de commande et de contrôle peuvent être créés pour exécuter les commandes ou récupérer de l'information à distance à partir du réseau compromis. Il est possible pour les auteures et auteurs de menace d'intégrer des données aux communications d'un réseau de commande et de contrôle au moyen d'une infrastructure accessible au public ou contrôlée par un pirate.
- **Lecteurs physiques ou périphériques :** Les auteures et auteurs de menace qui ont un accès physique au réseau interne peuvent recourir à des lecteurs physiques ou à des lecteurs amovibles comme des clés USB, des lecteurs multimédias, et des appareils portatifs et mobiles pour sortir des données du réseau. Des procédures de mise hors service inadéquates pour les appareils et les lecteurs multimédias peuvent introduire des points de sortie de données accidentels si des techniques appropriées de nettoyage ne sont pas respectées. L'utilisation accrue des appareils intelligents connectés (personnels ou d'entreprise), des appareils de l'Internet des objets (IdO) et des appareils personnels (modèle BYOD pour *Bring your own Device*) dans des environnements d'entreprise pourrait également augmenter les points de sortie que peuvent exploiter les auteures et auteurs de menace.
- **Plateformes infonuagiques ou de stockage Web :** Les auteures et auteurs de menace peuvent profiter de l'utilisation croissante du stockage infonuagique et des services d'applications offerts pour les activités commerciales afin de cacher leurs transferts de données dans les modèles de trafic commercial existants. Une auteure ou un auteur de menace peut faire passer son transfert de données par l'entremise d'un fournisseur de services infonuagiques ou Web approuvé de l'organisation. Souvent, les organisations ont déjà un volume de trafic légitime qui passe par de telles plateformes, ce qui rend difficile la détection de transferts de données malveillantes.
- **Mauvaises configurations et vulnérabilités :** Des services d'applications sur site et hors site peuvent exposer les données d'une organisation et donner aux auteures et auteurs de menace l'accès à celles-ci. Des vulnérabilités du jour zéro ou des vulnérabilités de système connues non corrigées peuvent permettre aux auteures et auteurs de menace d'exploiter le système d'information et de contourner les mesures de protection pour cacher et exfiltrer des données du réseau.
- **Portes dérobées :** Les auteures et auteurs de menace peuvent compromettre le dispositif ou le service avant ou pendant les processus d'approvisionnement pour installer des portes dérobées dans les systèmes. Ces portes peuvent être utilisées pour obtenir et établir un accès non autorisé au réseau et transférer des données hors du réseau.

- **Hameçonnage ou piratage psychologique :** Une attaque par hameçonnage ou piratage psychologique réussie peut entraîner une divulgation volontaire de renseignements confidentiels de la part d'utilisatrices et utilisateurs, ou peut faire en sorte que ceux-ci fassent partie de l'infrastructure d'exfiltration d'une auteure ou d'un auteur de menace.
- **Services tiers ou clients :** Les auteures et auteurs de menace peuvent tirer avantage des relations de confiance qui existent entre des réseaux tiers ou clients et votre infrastructure pour exfiltrer des données. Ils peuvent faire passer des données volées par un réseau tiers de confiance.
- **Services sans fil et Wi-Fi :** Des services sans fil d'entreprise et d'invité conçus ou mis en œuvre sans mesures de sécurité pourraient ouvrir la voie à de l'écoute clandestine et ainsi permettre à des auteures et auteurs de menace de recueillir et d'exfiltrer des données. Les auteures et auteurs qui ont un accès physique aux installations d'une organisation peuvent être en mesure d'implanter des dispositifs de surveillance sans fil pour recueillir et exfiltrer des données.
- **Canaux cachés :** Les auteures et auteurs de menace peuvent utiliser des canaux cachés pour le vol de données à faible bande passante en exploitant les émissions de sons, de vibrations ou de signaux électromagnétiques. Ces techniques peuvent être très difficiles à détecter. Les auteures et auteurs parrainés par des États-nations dotés de moyens sophistiqués ont recours à des techniques telles que des canaux temporels cachés et des attaques de type TEMPEST[1].

[1] Une attaque TEMPEST est une méthode de capture distante de signaux électromagnétiques non intentionnels d'appareils afin d'obtenir de l'information sur les données ou le système observés.

3 Stratégies d'atténuation

Les stratégies de protection contre l'exfiltration de données nécessitent de multiples couches de contrôles de sécurité alignées pour assurer une protection en profondeur et une solution résiliente. Les contrôles de sécurité que vous déployez devraient compléter d'autres couches de protection existantes pour limiter les dommages. Les contrôles d'atténuation, quant à eux, devraient être choisis en fonction d'un équilibre entre les risques liés aux activités par rapport aux objectifs commerciaux et aux exigences en matière de prestation de service. Il est à noter que les contrôles de protection n'empêcheront pas tous les cas d'exfiltration de données; il est toutefois conseillé de concevoir une architecture sécurisée pour vos systèmes et processus dans le but de faire échouer les tentatives d'exfiltration des données sensibles de votre organisation.

L'architecture de votre organisation joue un rôle important dans votre stratégie générale de sécurité. Les réseaux d'entreprise hérités ont été conçus en se basant sur l'hypothèse habituelle selon laquelle le flux de trafic provenant de systèmes internes est sécurisé alors que le flux de trafic entrant ne l'est pas. Cependant, l'évolution vers un modèle d'architecture hybride (locale et infonuagique) remet en question cette prémisse. La capacité d'une auteure ou d'un auteur de menace à exfiltrer des données de votre réseau avec peu ou aucune contrainte peut être appuyée par l'architecture de votre entreprise et le choix des outils système dans l'environnement de votre entreprise. Par conséquent, il est donc recommandé d'adopter les pratiques suivantes :

- **Établir un modèle de gouvernance pour les données de l'organisation.** La gestion des données est une responsabilité partagée et les organisations peuvent parfois involontairement introduire des risques de sécurité supplémentaires en favorisant des pratiques isolées de gestion des données. Un modèle de gouvernance centralisée guidera les activités permettant de créer et de gérer les données dans l'ensemble de l'organisation. Les éléments de ce modèle comprennent la mise en place de politiques et de procédures liées à la création, au stockage, à la transmission et à l'élimination des données. Favorisez l'utilisation de championnes et champions de la sécurité des données pour encourager la responsabilisation. Assurez-vous de donner la priorité à la sécurité des données durant la conception et le déploiement des projets. Tenez compte de sujets tels que la collecte de données, la propriété des données, le traitement de différentes formes de données (structurées ou non structurées), la gestion des accès, la classification des données, la conformité et les exigences réglementaires.
- **Architecturer le réseau et les biens de TI de l'organisation pour les rendre résilients.** Concevez l'architecture réseau de votre entreprise pour qu'elle devienne résiliente face aux attaques entraînant des fuites de données. Concevez des contrôles de sécurité pour vos systèmes et processus d'un point de vue d'intrusion présumée. Le principe d'intrusion présumée se fonde sur la notion que vos systèmes et biens d'entreprise pourraient déjà être compromis. Concevez des systèmes et des contrôles basés sur les principes d'architecture à vérification systématique et éliminez la notion de confiance implicite pour vos systèmes. Structurez des services et des systèmes ayant la capacité de fournir une surveillance continue, une authentification continue et une revalidation des droits et des privilèges. Mettez en œuvre des contrôles de sécurité en utilisant des principes qui permettant de revalider et de vérifier les relations de confiance. Appliquez des niveaux supplémentaires de contrôles aux données et aux systèmes de nature délicate et de valeur plus élevée. Pour en savoir plus sur l'architecture à vérification systématique, consultez l'ITSAP.10.008, Modèle à vérification systématique (ou architecture zéro confiance) [5].

- **Effectuer une évaluation des menaces.** Évaluez les menaces et les risques auxquels font face les données de votre organisation et qui sont associés à votre environnement commercial. Déterminez les biens les plus sensibles de l'organisation et identifiez les zones d'attaque. Effectuez régulièrement une évaluation des menaces et des risques (EMR) de votre environnement pour cerner les lacunes de votre réseau et les vulnérabilités qui pourraient être exploitées pour exfiltrer les données de ce réseau. À l'aide de techniques de modélisation, recensez les menaces pour les données de votre organisation. La modélisation des menaces doit permettre d'établir les menaces provenant du flux de données, de l'utilisation de technologies déficientes et des relations avec des tiers. Utilisez des renseignements à jour sur les menaces pour identifier de potentiels auteurs et auteures de menace susceptibles de cibler votre organisation. Ces renseignements vous permettent également de vous défendre contre ceux-ci. Servez-vous de l'évaluation des menaces comme guide pour faire une sélection et une mise en œuvre délibérées des contrôles de sécurité. Les résultats de l'évaluation des risques vous permettent de placer par ordre de priorité les contrôles à appliquer aux dispositifs et aux systèmes présentant un risque plus élevé. Testez périodiquement l'efficacité des contrôles mis en place et déterminez les lacunes qu'il convient de régler. Pour obtenir plus de détails sur l'évaluation des menaces, consultez la Méthodologie harmonisée d'EMR (TRA-1) [6].
- **Établir et maintenir un système de classification des données pour l'organisation.** Le système de classification doit s'appliquer tant aux données structurées qu'aux données non structurées. Ce système de classification devrait être appuyé par une politique et des directives définissant comment les utilisatrices et utilisateurs peuvent accéder aux données ou les utiliser. Mettez en œuvre une stratégie d'accès aux données cohérente qui permet de localiser les données de votre organisation et d'en faire le suivi. Il faut tenir compte de la nature délicate des données au moment de définir un ensemble minimal de contrôles. Par exemple, la sécurité et le stockage des authentifiants ou des identifiants d'utilisateur ou de système peuvent nécessiter des contrôles additionnels.
- **Concevoir et mettre en œuvre un programme de protection contre les fuites de données (DLP).** Le programme DLP (*Data Leakage Protection*) doit aborder la question des risques qui pèsent sur vos données sur le plan technique, des processus et du comportement des utilisatrices et utilisateurs. Dans le cadre du processus global du programme, déployez des contrôles techniques pour protéger vos données à tous les points d'entrée et de sortie. Déployez la solution DLP pour protéger vos applications sensibles et leurs flux de données connexes. Avant de choisir une solution DLP, il est conseillé de réaliser des tests poussés pour vous assurer qu'elle répond bien à vos besoins et aux projections à venir en matière d'architecture. Menez une campagne de sensibilisation et d'éducation pour former les utilisatrices et utilisateurs avant le déploiement complet. Évaluez périodiquement la fiabilité de votre solution DLP en analysant son efficacité et son rendement.
- **Mettre en œuvre des solutions de sécurité des données sur les terminaux.** Il arrive souvent qu'une fuite de données se produise sur un terminal. Des contrôles techniques faisant appel à des antimaliciels, à des antivirus, à des pare-feux sur les terminaux, et à des solutions de détection et d'intervention sur les terminaux (EDR pour *Endpoint Detection and Response*) peuvent être envisagés pour détecter et bloquer les tentatives d'exfiltration de données. Le Centre pour la cybersécurité recommande d'activer la surveillance des événements sur les terminaux pour consigner les événements.
- **Renforcer les systèmes et déployer des mesures de protection réseau.** Les auteures et auteurs de menace ciblent les systèmes vulnérables et utilisent l'accès à ceux-ci pour s'infiltrer dans votre réseau. Empêchez votre environnement d'être aux prises avec des intrusions réseau. Mettez en œuvre une segmentation réseau visant à

limiter les répercussions d'activités malveillantes sur votre réseau. Déployez des mesures de protection contre les intrusions dans le réseau comme des solutions basées sur la reconnaissance de la signature ou le comportement et appliquez des mesures de protection contre les attaques par injection de code ou par exploitation des services Web. Déployez ainsi des solutions de prévention des maliciels, de passerelle de messagerie sécurisée et de pare-feu d'applications Web (WAF pour *Web Application Firewall*). Isolez les systèmes infectés et nettoyez-les le plus rapidement possible. Limitez les communications entre les réseaux de données sensibles. Dressez une liste des sites Web malveillants et bloquez l'accès à ces sites. Sécurisez vos sauvegardes de données. Désactivez l'utilisation de protocoles non sécurisés. Retirez les mots de passe par défaut des systèmes et désactivez tous les comptes, tous les services et toutes les applications qui ne sont pas nécessaires.

- **Inspecter les communications réseau pour repérer le trafic chiffré suspect.** Les auteures et auteurs de menace se servent du vaste appui qu'apportent les services HTTPS (pour *Hypertext Transfer Protocol Secure*; protocole de transfert hypertexte sécurisé) et TLS (pour *Transport Layer Security*; sécurité de la couche transport) pour éviter les contrôles de détection sur le réseau. Nous recommandons la mise en œuvre d'une solution d'inspection du trafic réseau d'entreprise pour inspecter et surveiller les tunnels chiffrés entre hôtes internes et externes. L'inspection du trafic chiffré permettra d'améliorer l'efficacité de votre solution DLP. Utilisez l'intelligence artificielle pour repérer le trafic ou les protocoles suspects dans votre environnement. Surveillez la présence d'une tunnellisation DNS, d'une utilisation non autorisée d'un logiciel RPV ou de techniques similaires susceptibles d'être utilisées de manière abusive pour créer un canal caché pour le trafic sortant.
- **Protéger toutes les connexions d'accès à distance.** Beaucoup d'organisations se fient à des technologies distantes pour permettre aux employées et employés de télétravailler, et pour offrir des services et y accéder. Il faut savoir que ces services amplifient l'environnement de menace, ce qui peut accroître la surface d'attaque de votre organisation. Sécurisez toutes les connexions à distance, notamment celles des tiers et des télétravailleurs. Veillez à ce que toutes les connexions à distance soient authentifiées avec des justificatifs d'authentification à au moins deux facteurs. Appliquez les contrôles DLP pour également sécuriser les connexions d'accès à distance.
- **Déployer des mécanismes de contrôle d'accès pour gérer l'accès aux données sensibles.** Utilisez des listes de contrôle d'accès (LCA) aux données pour limiter et gérer l'accès aux données sensibles de votre organisation. On recommande le recours au principe du droit d'accès minimal pour attribuer les droits d'accès à vos données. Les utilisatrices et utilisateurs ne devraient avoir que les droits minimaux nécessaires à l'exécution des tâches requises. Lorsque trop de droits sont octroyés, les comptes d'utilisateur deviennent une cible intéressante pour les auteures et auteurs de menace. Séparez les fonctions administratives et protégez les interfaces administratives. Limitez l'utilisation des comptes administratifs aux tâches administratives qui sont réalisées dans une limite de temps approuvée. Les comptes administratifs ne doivent pas servir aux activités quotidiennes. Mettez en œuvre le contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*). Lorsque la situation le permet, appliquez l'authentification multifacteur (AMF) à tous les services et comptes d'utilisateur ou d'administrateur.
- **Limiter l'utilisation d'outils système et de sites Web pouvant faciliter une exfiltration de données.** Utilisez des contrôles de filtrage de domaine pour limiter l'accès aux applications Web, aux outils et aux sites Web qui pourraient servir à exfiltrer des données de votre réseau. Limitez ou bloquez l'installation et l'utilisation d'applications logicielles et d'applications de stockage externe qui pourraient faciliter le transfert non autorisé de données. Il est également recommandé de limiter l'accès aux applications de vidéoconférence ou de réunion en ligne, aux

plateformes de messagerie, aux courriels internes et Web, aux plateformes de messagerie sécurisée et aux plateformes de médias sociaux.

- **Utiliser des mesures de protection cryptographiques pour appliquer les contrôles de confidentialité des données.** Vous pouvez utiliser le chiffrement comme couche de protection pour atténuer le risque de divulgation non autorisée ou accidentelle de vos données. Toutefois, vous devez évaluer l'impact que peut avoir le chiffrement des données sur vos activités commerciales légitimes. Assurez-vous que les mesures de gestion des clés de chiffrement mises en œuvre sont sûres et adéquates. Envisagez l'application du chiffrement sur l'ensemble de la chaîne de valeur de vos données au repos, en traitement et en transit. Pour ce qui est du transport de données vers des environnements en nuage, tenez compte du chiffrement du côté client pour vous assurer que vos données sont protégées. Utilisez des protocoles TLS pour assurer la protection des communications réseau, et servez-vous uniquement de bibliothèques cryptographiques à jour et approuvées.
- **Protéger les données sensibles à l'aide d'enclaves de données sécurisées.** Configurez des enclaves de données sécurisées en mettant en place des environnements spécialisés pouvant offrir un accès contrôlé et un stockage sécurisé pour vos données sensibles. Ces environnements hébergeront les données confidentielles et sensibles de l'organisation, et l'accès à ces données ne devrait être permis que pour des opérations précises. Toutes les interactions dans ces types d'environnements sont journalisées et vérifiées. Mettez en place des contrôles rigoureux sur la façon dont les données entrent et sortent des enclaves. Les enclaves de données doivent être configurées de manière à former un environnement fermé sans accès à Internet. Assurez-vous que les sauvegardes de données, les activités de reproduction et les autres opérations de gestion du système dans cet environnement sont sécurisées.
- **Veiller à ce que les contrôles de surveillance saisissent divers types de données.** Les progrès dans les technologies de transformation de données numériques au moyen de l'intelligence artificielle, du traitement de pointe de vidéo et d'image, du traitement automatique du langage naturel (TALN) et d'autres technologies semblables présentent de nouvelles capacités. En tirant profit de ces technologies, les auteures et auteurs de menace sont en mesure de convertir des types de données comme un texte en vidéo, en audio, en images ou en d'autres types de médias numériques. Élargissez vos contrôles de surveillance pour repérer différentes formes de flux de données et mettez en œuvre des capacités permettant de détecter et de prévenir les tentatives d'exfiltration de données de vos systèmes. Testez et vérifiez ces contrôles pour vous assurer qu'ils demeurent efficaces même si le format de vos données sensibles change.
- **Mettre en place des mesures de journalisation et de surveillance réseau.** Surveillez activement les flux de données sur l'ensemble de votre réseau en mettant en œuvre des mécanismes de journalisation des activités et de détection des flux de données suspects. Envisagez l'adoption de mesures pour vous permettre de détecter les flux de données suspects et les augmentations imprévues dans les données aux points de sortie. Vous devriez également considérer le recours à une surveillance géographique et temporelle pour détecter et contrecarrer les tentatives d'exfiltration de données. Des techniques comme le déclenchement, la réauthentification, le masquage de données et la surveillance des comportements en sont quelques exemples. Mettez en place des contrôles pour surveiller l'apparition de nouveaux services et de nouveaux protocoles sur votre réseau. Examinez périodiquement les protocoles réseau dans votre environnement et veillez à analyser les services suspects. Mettez en œuvre une architecture de journalisation conçue pour assurer une résilience en cas d'attaques. Les journaux des systèmes

essentiels doivent être recueillis en temps réel et stockés à l'extérieur de l'appareil, dans un endroit hautement sécurisé. Tirez profit des solutions de gestion des informations et des événements de sécurité (GIES) pour mettre en corrélation les activités et les événements, et améliorer vos capacités de détection.

- **Mettre en œuvre des mesures adéquates d'élimination des données.** Les supports ayant des capacités de stockage de données devraient être nettoyés au moyen de techniques de suppression de données certifiées ou ils devraient être physiquement détruits. Utilisez des pratiques sécurisées d'élimination des données comme la réécriture cryptographique qui se fait à l'aide de protocoles et de suites de chiffrement approuvés, le nettoyage des supports et la destruction physique des appareils. Il est ainsi possible d'éviter une exfiltration de données involontaire ou le vol de données par des appareils ayant été mis hors service. Vous devez également vous assurer que les appareils ne pouvant plus être utilisés sont mis hors service.
- **Développer des dossiers d'exploitation de gestion des incidents d'exfiltration de données.** Les dossiers d'intervention en cas d'incident d'exfiltration de données aideront à fournir un ensemble de directives vérifiées et réalisables sur la gestion d'un incident d'exfiltration de données. Développez des processus, des procédures et des plans d'action techniques expliquant comment enquêter sur un événement d'exfiltration de données, le contenir et s'en remettre. Les procédures d'intervention vérifiées permettent de s'assurer que les mesures visant à contenir les événements n'ont pas accidentellement de répercussions sur les enquêtes et fournissent des moyens d'éliminer de façon sécurisée les auteures et auteurs de menace de votre système.
- **Mettre à profit l'automatisation pour accélérer les processus d'intervention en cas d'incident.** Procédez à l'automatisation pour faciliter la détection et l'intervention en cas d'intrusion dans le réseau ou d'activités malveillantes dans votre environnement. Déployez des outils de prévention des intrusions dans le réseau. La rapidité avec laquelle vous déployez vos activités d'intervention en cas d'incident peut contribuer à contrecarrer la progression des attaques sur votre réseau. Par conséquent, faites appel à des solutions d'orchestration, d'automatisation et d'intervention en matière de sécurité (SOAR pour *Security Orchestration, Automation, and Response*) pour procurer aux équipes de sécurité un soutien automatisé. Mettez à profit les systèmes de détection des anomalies et les techniques d'apprentissage automatique pour analyser et repérer les déviations suspectes dans les communications sur votre réseau.
- **Déployer des contrôles de sécurité infonuagiques pour protéger les données dans le nuage.** N'accordez pas une confiance aveugle au trafic des services infonuagiques qui traverse votre réseau. Vous devriez présumer que votre fournisseur ou instance de services infonuagiques peut être compromis. Mettez en œuvre des contrôles pour valider les données d'entrée et de sortie de votre infrastructure infonuagique. Ayez recours à des passerelles sécurisées d'accès au nuage (CASB pour *Cloud Access Security Broker*) pour appliquer vos politiques de sécurité des données dans le nuage. Utilisez le CASB pour limiter les applications infonuagiques qui interagissent avec vos données et inspecter les flux de données pour assurer la conformité aux politiques de sécurité. Vous devriez également veiller à ce que vos données soient chiffrées lorsqu'elles sont au repos dans le nuage.
- **Appliquer les correctifs aux systèmes et mettre en œuvre des pratiques exemplaires de base en matière de sécurité.** Appliquez les correctifs et les mises à jour à vos systèmes de même qu'à vos applications afin de diminuer les risques d'exploitation de vulnérabilités connues. Envisagez le recours à un modèle de déploiement de gestion des correctifs centralisé permettant d'automatiser et d'accélérer le déploiement de correctifs. Assurez-vous que les micrologiciels des appareils sont protégés contre tout changement non autorisé. Envisagez la possibilité de

mettre en œuvre un régime d'essais pour valider les mises à jour logicielles avant qu'elles soient appliquées. Utilisez des versions sécurisées de protocoles Internet courants comme les extensions de sécurité du système d'adressage par domaines (DNSSEC pour *Domain Name System Security Extensions*).

- **Limiter et surveiller l'utilisation d'outils administratifs dans votre environnement.** Limitez le déploiement et l'emploi d'outils administratifs aux cas d'utilisation approuvés uniquement. Les exceptions à cette règle devraient faire l'objet d'une surveillance et d'une enquête. Lorsque ces outils sont utilisés, ne laissez pas de copies sans surveillance sur les appareils cibles. Séparez les applications et les systèmes administratifs de l'environnement utilisateur et mettez en œuvre des contraintes d'exécution pour limiter la façon dont ces outils sont exécutés dans votre environnement.
- **Éduquer les utilisatrices et utilisateurs, et mettre à profit les renseignements sur les menaces.** La façon de limiter les courriels malveillants qui sont des vecteurs d'attaque passe par l'éducation et l'utilisation de la technologie. Sensibilisez vos utilisatrices et utilisateurs aux menaces récentes associées aux courriels d'hameçonnage. Mettez en place des solutions antihameçonnages perfectionnées pour analyser les courriels entrants, notamment en déployant des solutions DKIM (pour *DomainKeys Identified Mail*) ou DMARC (pour *Domain-based Message Authentication, Reporting & Conformance*). Il faut également mettre en œuvre des contrôles pour surveiller les canaux de courrier électronique afin de repérer les tentatives d'exfiltration de données. De plus, il est recommandé de mettre à profit les indicateurs de renseignements sur les menaces pour traquer toute activité malveillante connue pouvant se produire sur votre réseau. Pour de plus amples renseignements sur les protocoles DKIM and DMARC, consultez l'ITSP.40.065, Directives de mise en œuvre – protection du domaine de courrier [7].

4 Conclusion

La protection des données sensibles de votre organisation devrait être au cœur de votre stratégie de sécurité. Bien qu'il puisse s'avérer difficile de protéger toutes les données contre une exfiltration ou une fuite de données, l'évaluation proactive de votre environnement et la mise en œuvre de contrôles de sécurité actifs permettront de limiter les répercussions sur vos activités en cas d'incident. Vous devriez envisager une approche holistique qui accroît la visibilité des flux de données, qui applique les pratiques exemplaires en cybersécurité à vos biens de données et qui met en place des mécanismes de surveillance et de journalisation des activités sur votre réseau. Ces mesures importantes vous permettront de limiter les répercussions sur votre organisation et d'améliorer votre posture de sécurité globale.

5 Contenu complémentaire

5.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Expression au long
AMF	Authentification multifacteur
CASB	Passerelle sécurisée d'accès au nuage (*Cloud Access Security Broker*)
CST	Centre de la sécurité des télécommunications
DKIM	Protocole DKIM (*DomainKeys Identified Mail*)
DMARC	Protocole DMARC (*Domain-based Message Authentication, Reporting & Conformance*)
DNSSEC	Extensions de sécurité du système d'adressage par domaines (*Domain Name System Security Extensions*)
GC	Gouvernement du Canada
GIES	Gestion des informations et des événements de sécurité
HTTPS	Protocole de transfert hypertexte sécurisé (*Hypertext Transfer Protocol Secure)*
RBAC	Contrôle d'accès basé sur les rôles (*Role-Based Access Control*)
SOAR	Orchestration, automatisation et intervention en matière de sécurité (*Security Orchestration, Automation, and Response*)
TI	Technologies de l'information
TLS	Protocole de sécurité de la couche transport (*Transport Layer Security*)

5.2 Glossaire

Terme	Définition
Authentification multifacteur	Tactique pouvant ajouter une couche supplémentaire de sécurité aux appareils et aux comptes. L'authentification multifacteur exige une vérification supplémentaire (comme un NIP ou une empreinte digitale) pour accéder aux appareils ou aux comptes. L'authentification à deux facteurs est un type d'authentification multifacteur.
Canal temporel caché	Fonction d'un système permettant à une entité de système de signaler de l'information à une autre entité en modulant sa propre utilisation d'une ressource de système de façon à affecter le temps de réponse du système observé par la deuxième entité. (Source : NIST)
Contrôle d'accès basé sur les rôles	Modèle visant à contrôler l'accès aux ressources lorsque les mesures autorisées sur les ressources sont établies en fonction de rôles plutôt qu'en fonction d'identités individuelles de sujet.
Défense en profondeur	Concept de sécurité des TI (aussi appelé approche *Castle*) en vertu duquel plusieurs couches de sécurité sont utilisées pour protéger l'intégrité de l'information. Ces couches peuvent comprendre des antivirus, des antimaliciels, des pare-feux, des mots de passe hiérarchiques, la détection d'intrusion et l'identification biométrique.
Jour zéro	Vulnérabilité du jour zéro : vulnérabilité logicielle dont l'existence n'est pas encore connue du fournisseur et qui n'a donc pas été atténuée. Exploit du jour zéro : attaque dirigée vers une vulnérabilité du jour zéro.

Terme	Définition
Porte dérobée	Moyen non documenté, privé ou moins détectable d'accéder à distance à un ordinateur, de contourner les mesures d'authentification et d'obtenir un accès au texte clair.
TEMPEST	Sigle représentant les spécifications et les normes visant à réduire la force des émanations électromagnétiques provenant de l'équipement électrique et électronique, ce qui contribue par le fait même à réduire la vulnérabilité à l'écoute clandestine. Le département de la Défense des États-Unis est à l'origine de ce terme.

5.3 Références

Numéro	Référence
1	National Institute of Standards and Technology. SP.800-53 Security and Privacy Controls for Information Systems and Organizations, septembre 2020.
2	Centre canadien pour la cybersécurité. La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33), novembre 2012.
3	Att&ck.MITRE.org. Exfiltration, juillet 2019.
4	Center For Internet Security. Critical Security Controls Navigator.
5	Centre canadien pour la cybersécurité. Modèle à vérification systématique (ou architecture zéro confiance) (ITSAP.10.008), novembre 2022.
6	Centre canadien pour la cybersécurité. Méthodologie harmonisée d'évaluation des menaces et des risques (EMR) (TRA-1), octobre 2007.
7	Centre canadien pour la cybersécurité. Directive de mise en œuvre : protection du domaine de courrier (ITSP.40.065), août 2021.

Annexe A Exfiltration : Contrôles du CIS v8 et techniques ATT&CK correspondantes

Nº	Contrôles du CIS v8	Mesures de protection du CIS	Type de bien	Titre	Description
1	**Contrôle 2 du CIS** - Inventaire et contrôle des biens logiciels	2.3	Applications	Gérer les logiciels non autorisés	Veiller à ce que les logiciels non autorisés soient retirés des biens d'entreprise ou reçoivent une exception documentée. Réexaminer au moins une fois par mois.
2	**Contrôle 2 du CIS** - Inventaire et contrôle des biens logiciels	2.5	Applications	Utiliser une liste des logiciels autorisés	Se servir de contrôles techniques, tels qu'une liste d'applications autorisées, pour veiller à ce que l'on puisse accéder uniquement aux logiciels autorisés ou que seuls ces logiciels puissent être exécutés. Réexaminer au moins deux fois par année.
3	**Contrôle 3 du CIS** - Protection des données	3.3	Données	Configurer des listes de contrôle d'accès aux données	Configurer des listes de contrôle d'accès aux données en fonction du besoin de connaître de chaque utilisatrice ou utilisateur. Appliquer des listes de contrôle d'accès, que l'on appelle également autorisations d'accès, aux applications, aux bases de données et aux systèmes de fichiers locaux et distants.
4	**Contrôle 3 du CIS** - Protection des données	3.1	Données	Chiffrer les données sensibles en transit	Chiffrer les données sensibles en transit. Les exemples de mise en œuvre peuvent comprendre la sécurité de la couche transport (TLS) et OpenSSH (*Open Secure Shell*).
5	**Contrôle 4 du CIS** - Configuration sécurisée des biens et des logiciels d'entreprise	4.1	Applications	Établir et tenir à jour un processus de configuration sécurisée	Établir et tenir à jour un processus de configuration sécurisée pour les biens d'entreprise (appareils d'utilisateur final, y compris les ordinateurs portables et les appareils mobiles; appareils IdO et non informatiques; et serveurs) et les logiciels (systèmes d'exploitation et applications). Examiner et mettre à jour la documentation chaque année ou lorsque sont apportés des changements d'entreprise considérables qui pourraient avoir des répercussions sur cette mesure de protection.
6	**Contrôle 4 du CIS** - Configuration sécurisée des biens et des logiciels d'entreprise	4.2	Réseau	Établir et mettre à jour un processus de configuration sécurisée pour l'infrastructure réseau	Établir et mettre à jour un processus de configuration sécurisée pour les dispositifs réseau. Examiner et mettre à jour la documentation chaque année ou lorsque sont apportés des changements d'entreprise considérables qui pourraient avoir des répercussions sur cette mesure de protection.
7	**Contrôle 4 du CIS** - Configuration sécurisée des biens et des logiciels d'entreprise	4.4	Dispositifs	Mettre en œuvre et gérer un pare-feu sur les serveurs	Mettre en œuvre et gérer un pare-feu sur les serveurs, dans la mesure du possible. Les exemples de mise en œuvre comprennent un pare-feu virtuel, un pare-feu de système d'exploitation ou un agent de pare-feu.
8	**Contrôle 4 du CIS** - Configuration sécurisée des biens et des logiciels d'entreprise	4.6	Réseau	Gérer de façon sécurisée les biens et les systèmes d'entreprise	Gérer de façon sécurisée les biens et les systèmes d'entreprise. Les exemples de mise en œuvre comprennent la gestion de la configuration au moyen d'une infrastructure en tant que code avec contrôle des versions et l'accès aux interfaces administratives par l'intermédiaire de protocoles réseau sécurisés tels que le protocole SSH (pour *Secure Shell*) et le protocole HTTPS (pour *Hypertext Transfer Protocol Secure*; protocole de transfert hypertexte sécurisé). Ne pas utiliser de protocoles de gestion non sécurisés tels que le protocole Telnet (pour *Teletype Network*) et le protocole HTTP (pour *HyperText Transfer Protocol*; protocole de transfert hypertexte).

Nº	Contrôles du CIS v8	Mesures de protection du CIS	Type de bien	Titre	Description
9	**Contrôle 4 du CIS** - Configuration sécurisée des biens et des logiciels d'entreprise	4.7	Utilisateurs	Gérer les comptes par défaut sur les biens et les logiciels d'entreprise	Gérer les comptes par défaut sur les biens et les logiciels d'entreprise tels que les comptes racines, d'administrateur ou d'autres comptes préconfigurés de fournisseurs. Les exemples de mise en œuvre peuvent comprendre la désactivation des comptes par défaut ou la modification de ces comptes pour les rendre inutilisables.
10	**Contrôle 4 du CIS** - Configuration sécurisée des biens et des logiciels d'entreprise	4.8	Dispositifs	Désinstaller ou désactiver les services non nécessaires sur les biens et les logiciels d'entreprise	Désinstaller ou désactiver les services non nécessaires sur les biens et les logiciels d'entreprise, tels qu'un service de partage de fichiers, un module d'application Web ou une fonction de service non utilisés.
11	**Contrôle 5 du CIS** - Gestion des comptes	5.3	Utilisateurs	Désactiver les comptes inactifs	Supprimer ou désactiver les comptes inactifs après 45 jours d'inactivité, dans la mesure du possible.
12	**Contrôle 6 du CIS** - Gestion du contrôle d'accès	6.1	Utilisateurs	Établir un processus d'autorisation d'accès	Établir et suivre un processus, préférablement automatisé, pour accorder l'accès aux biens d'entreprise au moment de l'embauche, de l'octroi de droits d'accès ou d'un changement de rôle d'une utilisatrice ou d'un utilisateur.
13	**Contrôle 6 du CIS** - Gestion du contrôle d'accès	6.2	Utilisateurs	Établir un processus de révocation d'accès	Établir et suivre un processus, préférablement automatisé, pour révoquer l'accès aux biens d'entreprise en désactivant les comptes dès la cessation d'emploi, la révocation des droits d'accès ou le changement de rôle d'une utilisatrice ou d'un utilisateur. Désactiver les comptes, au lieu de les supprimer, peut s'avérer nécessaire pour préserver les pistes de vérification.
14	**Contrôle 6 du CIS** - Gestion du contrôle d'accès	6.8	Données	Définir et tenir à jour le contrôle d'accès basé sur les rôles	Définir et tenir à jour le contrôle d'accès basé sur les rôles en déterminant et en documentant les droits d'accès nécessaires pour chaque rôle dans l'entreprise afin d'exécuter les tâches attribuées. Au moins une fois par année, examiner le contrôle d'accès pour les biens d'entreprise afin de confirmer que tous les privilèges sont autorisés.
15	**Contrôle 7 du CIS** - Gestion continue des vulnérabilités	7.6	Applications	Réaliser une analyse automatisée des vulnérabilités sur les biens d'entreprise exposés à l'extérieur	Au moins une fois par mois, réaliser une analyse automatisée des vulnérabilités sur les biens d'entreprise exposés à l'extérieur à l'aide d'un outil d'analyse des vulnérabilités conforme au protocole SCAP (pour *Security Content Automation Protocol*).
16	**Contrôle 7 du CIS** - Gestion continue des vulnérabilités	7.7	Applications	Corriger les vulnérabilités détectées	Corriger au moins une fois par mois les vulnérabilités détectées dans les logiciels au moyen de processus et d'outils en fonction du processus de correction.
17	**Contrôle 9 du CIS** - Mesures de protection du courrier électronique et des navigateurs Web	9.2	Réseau	Utiliser des services de filtrage DNS	Utiliser des services de filtrage de système d'adressage par domaines (DNS) sur tous les biens d'entreprise pour bloquer l'accès aux domaines malveillants connus.
18	**Contrôle 10 du CIS** - Mesures de défense contre les maliciels	10.3	Dispositifs	Désactiver le lancement automatique des supports amovibles	Désactiver la fonction de lancement automatique des supports amovibles.
19	**Contrôle 12 du CIS** - Gestion de l'infrastructure réseau	12.2	Réseau	Établir et tenir à jour une architecture de réseau sécurisée	Établir et tenir à jour une architecture de réseau sécurisée. Une architecture de réseau sécurisée doit appliquer les principes de segmentation, de droit d'accès minimal et de disponibilité, au minimum.
20	**Contrôle 12 du CIS** - Gestion de l'infrastructure réseau	12.8	Dispositifs	Établir et tenir à jour des ressources informatiques dédiées pour toutes les tâches administratives	Établir et tenir à jour des ressources informatiques dédiées, avec une séparation physique ou logique, pour toutes les tâches administratives ou les tâches nécessitant un accès administratif. Les ressources informatiques devraient être segmentées du réseau principal de l'entreprise et ne pas être autorisées à accéder à Internet.
21	**Contrôle 13 du CIS** - Surveillance et défense réseau	13.3	Réseau	Déployer une solution de détection d'intrusion réseau	Déployer une solution de détection d'intrusion réseau sur les biens d'entreprise, selon le cas. Les exemples de mise en œuvre comprennent l'utilisation d'un système de détection d'intrusion réseau (SDIR) ou d'un service

Nº	Contrôles du CIS v8	Mesures de protection du CIS	Type de bien	Titre	Description
					équivalent offert par un fournisseur de services infonuagiques (FSI).
22	**Contrôle 13 du CIS** - Surveillance et défense réseau	13.4	Réseau	Filtrer le trafic entre les segments de réseau	Filtrer le trafic entre les segments de réseau, selon le cas.
23	**Contrôle 13 du CIS** - Surveillance et défense réseau	13.8	Réseau	Déployer une solution de prévention d'intrusion réseau	Déployer une solution de prévention d'intrusion réseau, selon le cas. Les exemples de mise en œuvre comprennent l'utilisation d'un système de prévention d'intrusion réseau (SPIR) ou d'un service équivalent offert par un FSI.
24	**Contrôle 18 du CIS** - Tests de pénétration	18.3	Réseau	Corriger les lacunes découvertes lors des tests de pénétration	Corriger les lacunes découvertes lors des tests de pénétration en fonction de la politique de l'entreprise concernant la portée et la priorisation des mesures de correction.
25	**Contrôle 18 du CIS** - Tests de pénétration	18.5	s.o.	Réaliser des tests de pénétration périodiques en interne.	Au moins une fois par année, réaliser des tests de pénétration périodiques en interne en fonction des exigences du programme. Les tests peuvent être fonctionnels ou structurels.