Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Les 10 mesures de sécurité des TI : Numéro 4 – Renforcer la sécurité des systèmes d'exploitation (SE)

Gestion

Canada

Avant-propos

La présente est une publication NON CLASSIFIÉ publiée avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

Centre d'appel
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur XX XXXX 2022.

Historique des révisions

Révision	Modifications	Date
1	Première version.	XX mois 2022

D97-4/10-090-2024F-PDF
978-0-660-71585-8

Sommaire

L'une des 10 mesures de sécurité des TI recommandées consiste à renforcer les systèmes d'exploitation (SE) et les applications. Une façon de renforcer les systèmes d'exploitation et les applications est en ajoutant des fonctions de sécurité à leur configuration. Le présent document traite des diverses mesures que vous pouvez lorsque vous renforcez la sécurité de vos systèmes d'exploitation et applications pour assurer la protection des réseaux et des systèmes de votre organisation contre les cybermenaces courantes. Les conseils formulés dans la présente sont fondés sur les contrôles de sécurité mentionnés dans le document intitulé La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) du Centre pour la cybersécurité [1].

La présente publication fait partie d'une série de documents axés sur les recommandations contenues dans le document Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089) [2]. Bien que la mise en œuvre de l'ensemble des 10 mesures de sécurité recommandées puisse rendre votre organisation moins vulnérable aux cybermenaces, vous devriez examiner les activités que vous menez sur le plan de la cybersécurité pour déterminer s'il convient de prendre des mesures supplémentaires.

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Introduction

Pour prévenir les compromissions d'actifs et d'infrastructures connectés à Internet, dix mesures de sécurité ont été recommandées dans le document Les 10 meilleures mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.189) [2]. Vous y trouverez des recommandations pour renforcer la sécurité des systèmes d'exploitation et des applications. Votre organisation devrait être au courant de toutes les applications utilisées et en faire l'inventaire dans le cadre de votre processus global d'inventaire de biens.

Pour vous assurer de bien protéger ces applications et l'information qu'elles utilisent, vous devriez mettre en place des contrôles de sécurité pour renforcer les systèmes d'exploitation et les applications. L'utilisation de la configuration par défaut (originale) ne fournit pas le niveau de sécurité adéquat pour la plupart des organisations. En mettant en place les contrôles de sécurité indiqués dans la présente publication, votre organisation sera en mesure d'optimiser la configuration et la protection de vos systèmes d'exploitation et applications. Pour de plus amples renseignements sur la sélection et l'application des contrôles de sécurité, prière de consulter le document La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [1].

Pour prévenir la compromission d'actifs et d'infrastructures connectés à Internet, votre organisation devrait désactiver tous les ports (par exemple, le protocole de contrôle de transmission [TCP pour *Transmission Control Protocol*] et le protocole de datagramme utilisateur [UDP pour *User Datagram Protocol*]) et les services non essentiels et supprimer les comptes inutiles. Évaluez toutes les applications de tierces parties pour déterminer si elles comportent des fonctions ou composants qui devraient être désactivés en raison de leur inutilité ou qui nécessiteraient une intervention humaine avant d'être activés, comme les macros. Vous devriez également procéder à une vérification au niveau de l'organisme et mettre en place une solution antivirus dans le cadre de la configuration sécurisée de vos systèmes.

Si vous utilisez des services infonuagiques ou gérés, il pourrait incomber à votre fournisseur de renforcer les systèmes d'exploitation et les applications, selon vos modèles de services et de déploiement. Par exemple, dans une infrastructure-service (IaaS pour *Infrastructure as a Service*) ou d'une plateforme-service (PaaS pour *Platform as a Service*), il incombe à votre organisation de renforcer les systèmes d'exploitation et les applications. Dans le cas d'un logiciel-service (SaaS pour *Software as a Service*), le fournisseur de services infonuagiques (FSI) est responsable de renforcer la sécurité des systèmes d'exploitation et des applications. Votre organisation est responsable de tout l'équipement sur site nécessaire pour intégrer des composants ou des solutions hybrides.

Faire appel à un fournisseur de services de sécurité gérés (FSSG) pourrait être bénéfique pour votre organisation. Un FSSG peut vous aider dans le cadre de vos efforts de renforcement de la sécurité, notamment pour déterminer et mettre en œuvre vos paramètres de configuration de référence, vos mesures de détection et de surveillance sur les terminaux, vos services gérés de pare-feu et d'antivirus.

Quel que soit votre environnement, vous devriez vous assurer auprès des fournisseurs qu'ils intègrent ce qui suit lors de la sélection des systèmes d'exploitation et des applications pour votre organisation :

- engagement à l'égard des contrôles de sécurité intégrés (par exemple, les principes de sécurité dès la conception)
- pratiques de sécurité démontrables (par exemple, la programmation sécurisée)
- maintenance continue et examen permanent de la sécurité de leurs produits

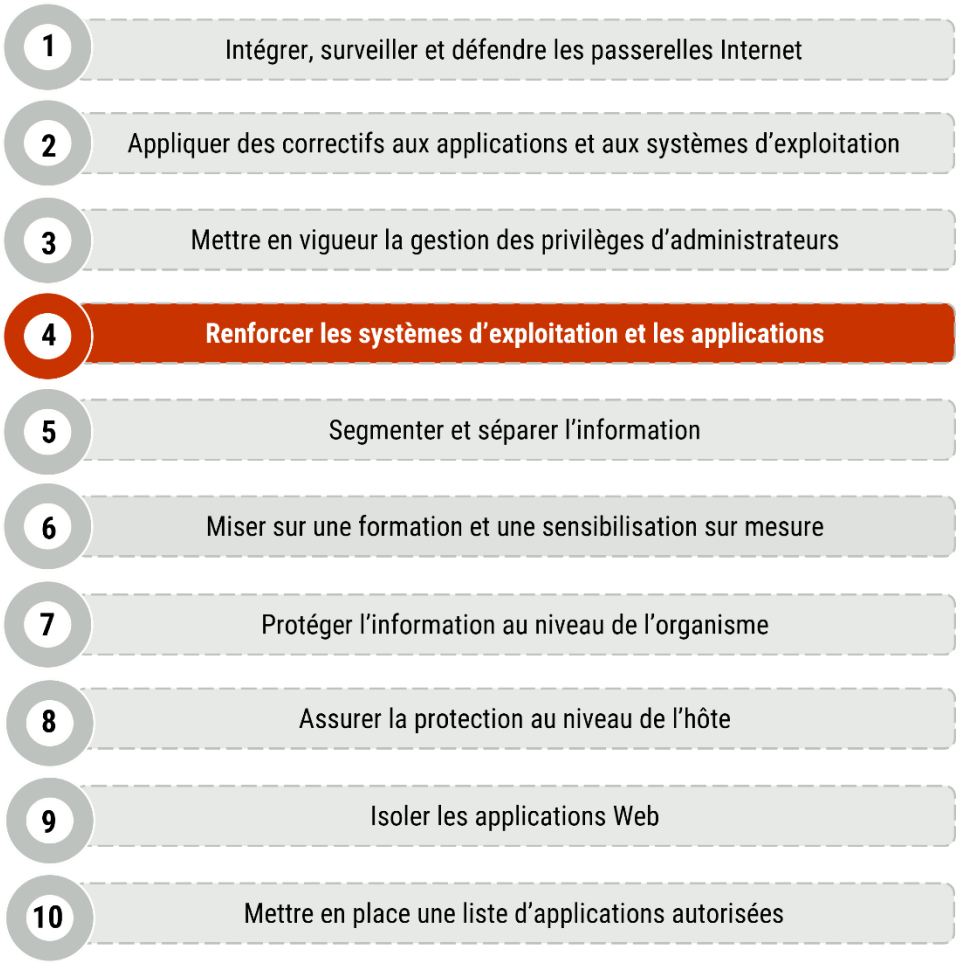
2 Les 10 mesures de sécurité des TI

Le présent document fournit de l'orientation sur le renforcement de la sécurité des systèmes d'exploitation et des applications. Renforcer les systèmes d'exploitation et les applications de votre organisation permet de réduire le degré d'exposition de votre organisation aux cybermenaces susceptibles de compromettre vos réseaux, vos systèmes et vos biens de TI. La présente est fondée sur les conseils formulés dans le document Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089) [2] et les contrôles de sécurité indiqués dans l'Annexe 3A - Catalogue de contrôles de sécurité (ITSG-33) [1].

Les 10 mesures de sécurité des TI recommandées par le Centre pour la cybersécurité, qui sont mentionnées à la figure 1 ci-dessous, sont fondées sur une analyse des tendances inhérentes aux activités de cybermenace et des répercussions de ces activités sur les réseaux connectés à Internet. La mise en œuvre des 10 mesures permettra de corriger la plupart des vulnérabilités liées à la sécurité des TI qui pèsent sur votre organisation.

L'incidence des menaces à la cybersécurité les plus courantes pourrait varier d'une organisation à l'autre. Pour satisfaire vos besoins en matière de sécurité, vous devez examiner les activités menées actuellement par votre organisation sur le plan de la sécurité et de la gestion des risques.

Figure 1: Les 10 mesures de sécurité des TI – Nº 4, Renforcer la sécurité des systèmes d'exploitation et des applications



Description longue : La figure 1 dresse une liste des 10 mesures de sécurité des TI. Numéro d'élément 4. « Renforcer les systèmes d'exploitation et les applications » est en surbrillance étant donné que la publication porte sur cette mesure. La figure 1 contient une liste des dix éléments suivants :

1. Intégrer, surveiller et défendre les passerelles Internet
2. Appliquer des correctifs aux applications et aux systèmes d'exploitation
3. Mettre en vigueur la gestion des privilèges d'administrateur
4. **Renforcer les systèmes d'exploitation et les applications**
5. Segmenter et séparer les informations
6. Miser sur une formation et une sensibilisation sur mesure
7. Protéger l'information au niveau de l'organisme
8. Assurer la protection au niveau de l'hôte
9. Isoler les applications Web
10. Mettre en place une liste d'applications autorisées

2.1 Rapport avec le processus de gestion des risques liés à la sécurité des TI

Les 10 mesures de sécurité des TI du CST découlent des contrôles de sécurité mentionnés à l'annexe 3A de l'ITSG-33 [2]. L'ITSG-33 [2] décrit les rôles, les responsabilités et les activités qui aident les organisations à gérer leurs risques liés à la sécurité des TI. Il comprend également un catalogue de contrôles de sécurité, comme les exigences de sécurité normalisées visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI. Ces contrôles de sécurité sont divisés dans les 3 classes suivantes, qui sont à leur tour divisées en plusieurs familles (ou groupes) de contrôles de sécurité connexes :

- **Contrôles de sécurité techniques :** contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels.
- **Contrôles de sécurité opérationnels :** contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies comme les logiciels de soutien.
- **Contrôles de sécurité de gestion :** contrôles de sécurité misant sur la gestion de la sécurité des TI et des risques liés à la sécurité des TI.

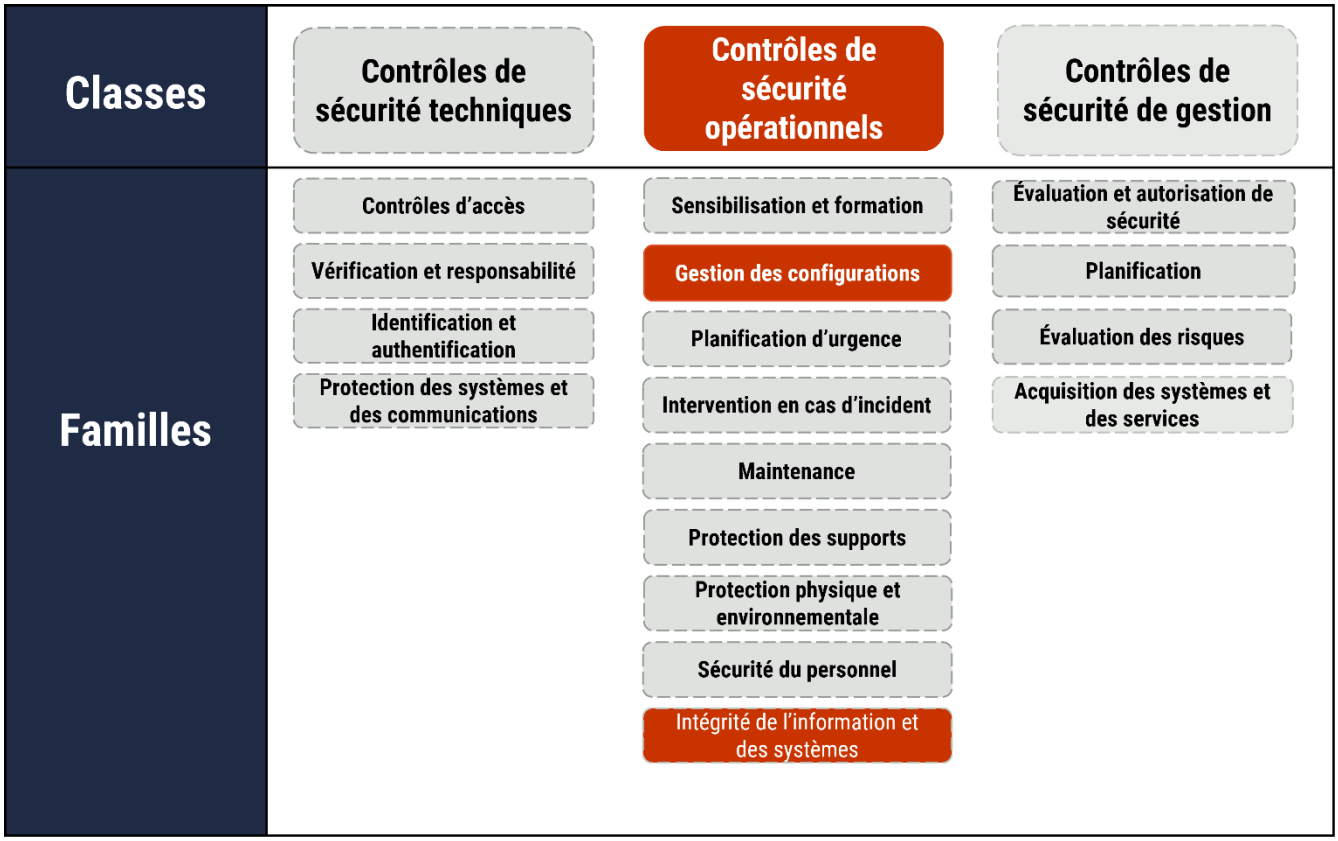
Tel qu'il est indiqué à la figure 2 ci-dessous, ce document aborde les contrôles de sécurité opérationnels associés aux familles Gestion des configurations (CM pour *Configuration Management*) et Intégrité de l'information et des systèmes (SI pour *System and Information Integrity*), comme :

- **CM-2 Configuration de référence**
- **CM-6 Paramètres de configuration**
- **CM-7 Fonctionnalité minimale**

- **SI-3 Protection contre les codes malveillants**
- **SI-4 Surveillance des systèmes d'information**

De plus amples renseignements sur les contrôles CM-2, CM-6, CM-7, SI-3 et SI-4. sont fournis à l'annexe A du présent document.

Figure 2: Classes et familles de contrôles de sécurité décrites dans l'ITSG-33



Description longue : Tel que le texte en surbrillance dans la figure 2 l'indique, cette publication est axée sur les contrôles de sécurité techniques, opérationnels et de sécurité de gestion. Elle fait mention des quelques mesures associées aux familles de contrôle « Contrôle de l'accès » et « Protection des systèmes et des communications ».

La liste complète des classes de contrôles de sécurité et de leurs familles ou groupes de contrôle connexes est aussi présentée dans la figure 2 comme suit :

Contrôles de sécurité techniques

- Contrôle de l'accès
- Vérification et responsabilité
- Identification et authentification
- Protection des systèmes et des communications

Contrôles de sécurité opérationnels

- Sensibilisation et formation
- **Gestion des configurations**
- Planification d'urgence
- Intervention en cas d'incident
- Maintenance
- Protection des supports
- Protection physique et environnementale
- Sécurité du personnel
- **Intégrité de l'information et des systèmes**

Contrôles de sécurité de gestion

- Évaluation et autorisation de sécurité
- Planification
- Évaluation des risques
- Acquisition des systèmes et des services

3 Une introduction sur la façon de renforcer la sécurité des systèmes d'exploitation et des applications

Pour protéger votre réseau, vos systèmes et vos données, nous recommandons à votre organisation de renforcer la sécurité des systèmes d'exploitation et des applications utilisés. Le renforcement de la sécurité est un processus conçu pour neutraliser la capacité d'une auteure ou d'un auteur de menace à profiter des vecteurs d'attaque en corrigeant les vulnérabilités et en désactivant les services non essentiels. Votre organisation devrait appliquer des mises à jour de sécurité, des correctifs et un ensemble de modifications provisoires à ses systèmes d'exploitation et applications, y compris ceux qui sont fournis par un tiers dès qu'ils sont disponibles. Votre approche à l'égard de la gestion des vulnérabilités devrait être fondée sur l'évaluation des risques de votre organisation. L'automatisation de ces processus permettra d'alléger certaines contraintes liées aux besoins en ressources pour surveiller et appliquer ces processus, et assurer que vos systèmes d'exploitation fonctionnent en étant les moins vulnérables possibles.

Il peut arriver que des mises à jour et des correctifs appliqués à vos systèmes d'exploitation et qui ne sont pas liés à la sécurité aient un impact global négatif sur la posture de sécurité des services de votre organisation, car ces mises à jour peuvent ajouter de nouveaux services ou changer le comportement de services existants.

Le renforcement implique également d'assurer une gestion de la configuration adéquate lors du déploiement de nouvelles applications et de nouveaux systèmes. Bien que le fait de permettre l'installation et les configurations par défaut des systèmes d'exploitation et des applications peut faire gagner du temps et sembler plus pratique, ce déploiement et cette utilisation peuvent présenter des risques importants.

Le document National Checklist Program for IT products: Guidelines for checklist users and developers (SP 800-70 Rev. 4) du National Institute for Standards and Technology (NIST) [3] renferme un référentiel de listes de vérification de la sécurité ou des repères qui offrent aux organisations des conseils sur le réglage des configurations de sécurité pour les SE et les applications. Le recours à ces listes de vérification peut minimiser la surface d'attaque, réduire les vulnérabilités touchant votre réseau, diminuer la répercussion des attaques réussies sur votre organisation, et déterminer les changements qui devraient être apportés ou qui autrement n'auraient pas été détectés.

Bien que les configurations devraient se faire au début du cycle de déploiement des systèmes d'exploitation ou des applications, il pourrait aussi être nécessaire de reconfigurer ces composants à mesure qu'évoluent vos besoins opérationnels et vos exigences de sécurité. Avant de reconfigurer ou de mettre à niveau les systèmes de TI ou ses composants, votre organisation devrait tenir compte des exigences de sécurité et des besoins opérationnels qui lui sont propres en faisant ce qui suit :

- définir toutes les exigences liées à la sécurité et la conception de l'architecture d'entreprise
- réaliser une évaluation des menaces et des risques
- déterminer les composants matériels et micrologiciels des points terminaux
- contrôler toutes les applications qu'utilise l'organisation

3.1 Exigences liées à la sécurité et à la conception de l'architecture d'entreprise

Toutes les exigences liées à la sécurité et la conception de l'architecture d'entreprise doivent être définies avant d'appliquer les recommandations formulées dans le présent document. Une image complète de l'architecture d'entreprise permettra à votre organisation de déterminer les outils et les fonctions de sécurité qui conviennent à ses besoins opérationnels et à ses exigences en matière de sécurité. Votre organisation devrait continuer de surveiller les outils et les fonctions de sécurité après leur mise en œuvre dans le cadre de ses activités permanentes de gestion des risques. Une surveillance régulière permettra ainsi d'assurer l'efficacité des contrôles de sécurité.

3.2 Lignes directrices et cadres pour le renforcement de la sécurité

Les conseils relatifs au renforcement de la sécurité des SE et des applications de votre organisation doivent être suivis le plus fidèlement possible, car ils ont été élaborés dans le but d'atténuer ou de bloquer des vecteurs de menace particuliers. Si, pour une raison quelconque, il est nécessaire de dévier de ces conseils, votre équipe de sécurité des TI doit bien comprendre les risques associés à la déviation et être prête à atténuer les vecteurs de menace potentiels qui pourraient en résulter. Votre organisation doit faire preuve de prudence si elle décide s'écarter des conseils de renforcement de la sécurité.

Plusieurs lignes directrices ou cadres sur le renforcement de la sécurité sont offerts. Les sous-sections suivantes donnent un aperçu des trois plus importantes lignes directrices offertes aux organisations.

3.2.1 Lignes directrices du Center for Internet Security

Le Center for Internet Security (CIS) a établi des repères relatifs au renforcement de la sécurité pour les organisations de toutes tailles et dans tous les emplacements géographiques. En suivant ces repères, il sera possible de renforcer la sécurité des biens de TI. Les repères se veulent des pratiques exemplaires et des configurations de référence recommandées pour configurer de manière sécuritaire une application ou un système. Ils sont « axés sur le consensus », ce qui signifie que ces repères sont établis et convenus par un grand nombre de spécialistes de la cybersécurité et de spécialistes en la matière de l'industrie. Ces repères sont en général acceptés partout au sein des gouvernements, des entreprises, de diverses industries et des milieux universitaires.

3.2.2 Lignes directrices de la Defense Information Systems Agency

La Defense Information Systems Agency (DISA) publie des guides appelés *Security Technical Implementation Guides* (STIG) qui offrent des conseils et des outils de conformité à l'intention des organisations. Bien que les STIG répondent à des exigences spécifiques pour les ministères du gouvernement américain, comme le Department of Defense, ils sont considérés comme des points de départ utiles pour toutes les organisations. Les STIG sont fiables et ils sont tirés de recherches exhaustives réalisées par des spécialistes en la matière. Ces STIG donnent des bases de référence et des conseils sur beaucoup de systèmes d'exploitation, d'applications et de dispositifs. Ces bases de référence sont censées rendre le matériel et les logiciels aussi sécuritaires que possible. Les STIG donnent aussi des conseils sur la gestion, la configuration et la surveillance des réseaux. Il est important de noter que ce ne sont pas tous les objectifs ou toutes les bases de référence des STIG qui s'appliquent aux organisations canadiennes.

3.2.3 Conseils de la National Security Agency et de la Cybersecurity and Infrastructure Security Agency

La National Security Agency (NSA) et la Cybersecurity and Infrastructure Security Agency (CISA) ont publié plusieurs documents d'orientation sur le renforcement de la sécurité des dispositifs, des SE et des applications. Elles ont entre autres publié conjointement le rapport technique Kubernetes Hardening Guide [4]. La CISA a aussi publié le document Key Findings to Improve Monitoring and Hardening of Networks [5] et un rapport technique conjoint.

Le Kubernetes Hardening Guide [5] donne des recommandations sur la configuration et le renforcement de la sécurité pour établir et sécuriser une grappe Kubernetes. Kubernetes est un système de source ouverte, souvent hébergé dans un environnement infonuagique, qui automatise le déploiement, la mise à l'échelle et la gestion d'applications exécutées dans des conteneurs. Un conteneur est un environnement d'exécution qui contient un progiciel et ses dépendances.

Le document *Key Findings to Improve Monitoring and Hardening of Networks* [5] donne des détails sur les activités et les principales conclusions tirées d'une évaluation effectuée par l'équipe rouge du CISA. Les conseils comprennent des recommandations visant à améliorer votre posture de cybersécurité. Le document propose également des mesures importantes de renforcement de la sécurité à pendre immédiatement et qui permettront d'améliorer la sécurité de l'environnement de votre organisation. Les mesures immédiates recommandées sont les suivantes :

- Établir la ligne de base de sécurité pour une activité réseau normale, ajuster le réseau et les appliances sur hôte de façon à détecter tout comportement inhabituel.
- Effectuer régulièrement des évaluations pour s'assurer que des mesures appropriées sont créées et qu'elles puissent être suivies par le personnel de sécurité.
- Appliquer autant que possible l'authentification multifacteur (AMF) résistante à l'hameçonnage.

Pour obtenir de plus amples renseignements sur la mise en œuvre et le renforcement de l'authentification multifacteur, prière de consulter le document Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.105) [6].

La CISA a noté plusieurs mesures d'atténuation qui s'alignent avec leurs objectifs de performance de la cybersécurité CPG intersectoriels Ces objectifs offrent un ensemble minimal de pratiques et de protections que la CISA et le NIST recommandent à toutes les organisations de mettre en place. Les CPG recommandés par la CISA et le NIST sont basés sur des cadres et des conseils visant à assurer une protection contre les menaces, les tactiques les techniques et les procédures les plus courantes et percutantes. Pour obtenir de plus amples renseignements sur les CPG, voir Cross-Sector Cybersecurity Performance Goals [7].

3.3 Matériel et micrologiciels

Votre organisation devrait tenir compte de ses composants matériels et micrologiciels lors de l'achat et de la mise en œuvre de dispositifs d'extrémité, comme des serveurs, des portables, des dispositifs mobiles et des tablettes. Les nouveaux dispositifs d'extrémité devraient être configurés au moyen des composants matériels et micrologiciels mentionnés dans vos lignes directrices.

Pour tirer parti des fonctions de sécurité de vos dispositifs et SE, les composants matériels et micrologiciels suivants devraient être mis en place :

- l'interface micrologicielle extensible unifiée (UEFI pour *Unified Extensible Firmware Interface)* pour permettre le démarrage sécurisé
    - l'UEFI est non configurée pour être exécutée en mode de système d'entrée-sortie de base (BIOS pour *Basic Input and Output System*) patrimonial
    - l'UEFI doit prendre en charge les mises à jour micrologicielles sécurisées
- le module de plateforme sécurisée 2.0 (TPM pour Trusted Platform Module) (les dispositifs qui utilisent TPM 1.2 peuvent être mis à niveau)
- le formatage du disque dur avec la table de partition d'identificateur global unique (GUID pour *Global Unique Identifier*) (et non l'enregistrement de démarrage principal [MBR pour *Master Boot Record*])
- l'intégrité du code protégé par hyperviseur conformément à votre SE, comme Device Guard pour Windows
- une unité centrale de traitement (UCT) de 64 bits avec la technologie de virtualisation Intel (VT-x) ou Advanced Micro Dynamics (AMD-V), et les tables de pages étendues (aussi appelées traduction d'adresse de second niveau [SLAT pour *Second Level Address Translation*])

Les dispositifs mobiles et les tablettes doivent également être intégrés aux plans de renforcement de la sécurité de votre organisation. Les conseils formulés dans la présente publication sont aussi applicables aux dispositifs sur site et mobiles.

3.4 Systèmes d'authentification

Votre organisation devrait renforcer ses systèmes d'authentification en sécurisant les voies d'authentification des applications. Pour ce faire, vous devez effectuer ce qui suit :

- Modifier les mots de passe par défaut du serveur
- Passer en revue le flux d'authentification et identifier les erreurs logiques que pourraient utiliser les auteures et auteurs de menace pour exploiter vos systèmes
- Supprimer les algorithmes désuets
- Désactiver ou supprimer les comptes inutiles
- Mettre en œuvre une solution de gestion des accès privilégiés (PAM pour *Privilege Access Management*)
- Interdire aux utilisatrices et utilisateurs de contourner une étape s'inscrivant dans un processus d'authentification à plusieurs étapes
    - Remarque : Ceci ne pourrait pas s'appliquer aux capacités liées à un accès d'urgence (ou à des comptes « bris de glace ») pour des utilisatrices et utilisateurs privilégiés
- Mettre en place des contrôles de gestion efficaces relatifs aux sessions
- Déployer des mesures visant la protection d'applications Web, comme des pare-feu d'applications Web (WAF pour *Web Application Firewalls*) ou des mandataires d'applications Web (WAP pour *Web Application Proxies*) pour atténuer l'exploitation de vulnérabilités

3.5 Contrôle des applications

Contrôler l'installation, l'utilisation et la connectivité des applications dans votre environnement est un élément clé du renforcement de la sécurité de vos applications et de la protection de votre réseau, de vos systèmes et de vos données. Vous devez vous assurer que ces applications sont gérées et que leur utilisation est contrôlée conformément à l'évaluation des menaces et des risques ainsi qu'aux politiques et procédures subséquentes de votre organisation. Il serait utile pour votre organisation de mettre en place des listes d'applications autorisées pour que vous puissiez avoir un certain contrôle sur les applications qui peuvent s'exécuter sur vos systèmes. Pour de plus amples renseignements, prière de consulter le document Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées (ITSM.10.095) [8].

Les utilisatrices ou utilisateurs qui ne détiennent pas de privilèges d'administrateur ne devraient pas être autorisés à installer des applications sur un dispositif organisationnel ou dans votre environnement organisationnel. Beaucoup d'applications peuvent être ciblées par des auteures et auteurs de menace qui ont recours au piratage psychologique et à d'autres tactiques pour tromper les employées et employés et les inciter à installer des applications infectées par des maliciels. On recommande à votre organisation d'avoir à sa disposition une suite d'applications préapprouvées que le personnel peut télécharger. Cela a pour effet d'alléger le fardeau de vos administratrices et administrateurs de TI et de permettre à vos utilisatrices et utilisateurs de trouver des applications qui leur sont utiles pour accomplir leurs tâches au sein de l'organisation. Nous recommandons également à votre organisation d'avoir une suite de logiciels et d'applications obligatoires qui ne pourront pas être désactivés, désinstallés ou supprimés par des utilisatrices ou utilisateurs qui ne bénéficient pas de privilèges d'administrateur. Pour les administratrices ou administrateurs, nous conseillons à votre organisation d'utiliser une station de travail administrative dédiée, par exemple, un poste de travail avec accès privilégié (PAW pour *Privileged Access Workstation*) ou un poste de travail administratif sécurisé (SAW pour *Secured Administrative Workstation*) qui ne donne pas accès à des applications ou qui n'est pas connecté à Internet.

3.6 Enjeux liés aux applications

Même si le renforcement de la sécurité de vos SE et applications est l'une des principales mesures de sécurité recommandées, sa mise en œuvre ne va pas sans comporter certains risques. Plus particulièrement lorsqu'il est question d'applications, le renforcement de la sécurité peut être difficile à réaliser, car il y a un immense volume d'applications offertes. Nous recommandons d'effectuer un examen de toutes les applications offertes dans votre environnement, y compris les applications standard et de tierces parties, et de désactiver ou de supprimer celles qui ne sont pas nécessaires.

4 Contrôles de sécurité pour le renforcement de la sécurité

Annexe 3A - Catalogue des contrôles de sécurité (ITSG-33) [2] présente les contrôles de sécurité suivants qui conviennent et sont applicables pour renforcer la sécurité de vos SE et applications utilisés dans l'ensemble de votre organisation. Les sous-sections suivantes donnent en détail le contrôle de sécurité et les mesures connexes que devrait prendre votre organisation pour renforcer la sécurité de vos SE et applications.

4.1 Configuration de référence (CM-2)

Votre SE et vos applications ne devraient pas être déployés à l'état établi par défaut. En veillant à ce que votre organisation ajuste les paramètres de configuration de votre SE et de vos applications, vous obtenez une meilleure posture de sécurité et faites en sorte qu'il soit plus difficile pour les auteures et auteurs de menace de compromettre votre environnement. Vous pouvez également consulter et utiliser des paramètres de sécurité recommandés du fournisseur et de sources de confiance, comme les objectifs repères du CIS.

Votre organisation devrait élaborer, documenter et maintenir une configuration de référence courante pour tous ses systèmes et composants de systèmes, y compris les communications et les composants liés à la connectivité. Vos configurations de référence devraient comporter des détails sur les composants des systèmes d'information, dont les composants des logiciels, des réseaux et les déploiements de dispositifs mobiles. Des configurations de référence devraient également être établies pour votre SE, y compris l'historique des versions et des rustines. Votre organisation doit s'assurer que les versions les plus récentes de votre SE et de vos applications sont déployées dès qu'une mise à jour est disponible. Exécuter d'anciennes versions ou des versions qui ne sont pas prises en charge par votre SE peut exposer votre organisation à des vulnérabilités et à des techniques d'exploitation qui ont été atténuées dans la version la plus récente. Pour s'assurer que les composants sont à jour et que vous déployiez les versions les plus récentes ou de nouvelles fonctions additionnelles, votre organisation pourrait envisager d'affecter une ou un propriétaire à chaque composant. Cette ou ce propriétaire serait chargé de la configuration du composant.

Il est nécessaire de revoir vos paramètres de configuration de référence régulièrement pour assurer qu'ils répondent aux besoins changeants de votre environnement, notamment les versions, les publications et les changements à venir concernant vos systèmes ou vos opérations. Ils doivent toujours refléter l'architecture d'entreprise courante.

Votre organisation doit établir des paramètres de configuration à l'échelle de l'organisation puis les paramètres propres aux systèmes d'information. Une fois établis, ces paramètres deviennent une partie intégrante de la base de référence de la configuration de vos systèmes.

4.2 Paramètres de configuration (CM-6)

La gestion des configurations comprend les contrôles de sécurité qui permettent la gestion et le contrôle de tous les composants de vos systèmes d'information, comme des éléments matériels, logiciels et de configuration). Les paramètres de configuration représentent l'ensemble des paramètres que l'on peut modifier dans le matériel, les logiciels, les

micrologiciels, le SE, les composants du réseau et les applications qui ont une incidence sur la posture de sécurité ou les fonctions du système. Les paramètres de configuration sécurisée doivent inclure certains des éléments suivants :

- les ressources de configuration, par dossiers ou applications
- les paramètres d'accès aux comptes, aux dossiers et aux répertoires
- les paramètres de fonctions, de ports, de protocoles, de services et de connexion à distance
- le contrôle des applications

Vous devriez établir et documenter les produits de TI qui seront utilisés pour vous assurer de déployer le mode le plus rigoureux sur le plan des exigences opérationnelles. S'il est nécessaire de s'éloigner de ces paramètres de configuration prédéterminés, votre organisation devrait mettre en place un processus d'approbation pour s'assurer que l'équipe de gestion examine, documente et approuve chaque cas d'utilisation pendant une période définie pour appuyer les exigences opérationnelles. Les politiques et les procédures organisationnelles de votre organisation devraient également permettre de garantir que les changements apportés à vos paramètres de configuration sont surveillés et contrôlés, et que toutes les anomalies constatées sont documentées et font l'objet d'une enquête.

Si votre organisation fait appel à un fournisseur de services infonuagiques (FSI, vous devez vous assurer d'examiner et de contrôler le versionnage dans l'environnement IaaS et PaaS. Conformément aux éléments SaaS, nous recommandons à votre organisation de travailler avec son FSI pour s'assurer que les plus récentes versions sont utilisées et que le fournisseur soit en mesure d'intervenir rapidement et adéquatement advenant le moindre problème ou la moindre inquiétude.

4.3 Fonctionnalité minimale (CM-7)

Il est possible que votre organisation ait, dans son environnement, un large éventail de systèmes d'information à sa disposition. Vous devriez vous assurer d'examiner les fonctions et les services qu'ils fournissent pour déterminer ceux qui sont nécessaires pour la prise en charge de vos besoins organisationnels. Pour les opérations sur les nuages, passez en revue les stratégies d'accès et les capacités des comptes.

Vos systèmes doivent être configurés de manière à fournir uniquement les fonctions et les capacités essentielles pour répondre aux exigences opérationnelles. Le fait d'interdire ou de restreindre l'utilisation de certains éléments peut grandement améliorer votre posture de sécurité et permettre à votre organisation de mieux protéger son environnement opérationnel. Pour empêcher une connexion de dispositifs, un transfert d'information ou une tunnellisation non autorisés, vous devriez envisager d'empêcher ou de restreindre certains des éléments suivants :

- des fonctions, comme auto-exécution ou partage de fichiers;
- des ports ou des protocoles, comme FTP et HTTP;
- des services, comme le système de noms de domaine (DNS pour *Domain Name Service*), les agents de transfert de courrier (MTA pour *Mail Transport Agents*), ou le protocole DHCP (*Dynamic Host Configuration Protocol*)

De plus, bien qu'il puisse être pratique de fournir plusieurs services à partir d'un seul composant de système, cela peut contribuer à accroître les risques pour votre organisation. Vous pourriez causer un dépassement des services fournis par un

composant. Lorsque la situation le permet, votre organisation devrait limiter la fonctionnalité des composants à une seule fonction par dispositif, comme lorsqu'il y a des serveurs de courriel et des serveurs Web distincts.

Votre organisation doit développer des politiques et des procédures qui déterminent les fonctions et les services qui seront autorisés pour vos systèmes et ceux qui seront désactivés ou supprimés. Ces politiques et procédures devraient aider votre organisation à déterminer les applications nécessaires et les plus utiles, et fournir des lignes directrices sur la façon de supprimer de votre environnement les applications qui ne sont plus nécessaires.

Vous pouvez tirer parti des outils d'analyse de réseau, des systèmes de détection et de prévention d'intrusions et des mécanismes de protection de point terminal (pare-feu, systèmes de détection des intrusions sur l'hôte) pour identifier les fonctions, les ports, les protocoles et les services interdits et en empêcher l'utilisation.

4.4 Protection contre les codes malveillants (SI-3)

Utiliser des mécanismes de protection contre les codes malveillants, comme un antivirus et un antimaliciel, permettra d'améliorer la posture de cybersécurité de votre organisation. Vous devriez déployer ces outils à des points d'entrée et de sortie du système, comme les pare-feu, les serveurs et les dispositifs pour détecter et éradiquer les codes malveillants de vos systèmes. Le recours à un antivirus et à un antimaliciel peut aider votre organisation à détecter et à mettre en quarantaine un code malveillant soupçonné ou connu avant qu'il n'entre dans votre environnement. Il est primordial de mettre à jour ces outils de sécurité dès qu'une nouvelle version est disponible, comme il est prévu dans la politique de gestion des configurations de votre organisation.

Lorsque vous travaillez dans un environnement infonuagique, il convient de déterminer les fonctions et fonctionnalités de sécurité qu'offre votre FSI et de collaborer avec celui-ci afin d'identifier et de mettre en œuvre les services additionnels dont vous avez besoin pour sécuriser votre environnement.

Beaucoup de ces produits de sécurité doivent avoir recours à des signatures pour détecter les codes malveillants. Bien que cette approche est efficace lorsqu'un code malveillant a été identifié et qu'une signature est disponible, votre organisation ne bénéficiera pas pour autant d'une protection robuste. Vous devriez aussi déployer un système de prévention des intrusions sur l'hôte (HIPS pour *Host-Based Intrusion Prevention System*) et un SDIH afin de protéger les systèmes de votre organisation contre les attaques malveillantes connues ou inconnues. Les systèmes HIDS et HIPS peuvent détecter des anomalies dans des comportements associés à vos utilisatrices et utilisateurs ou à vos applications. Un système HIPS permettra d'améliorer votre protection globale contre les codes malveillants, car il peut détecter les codes malveillants axés sur les signatures et mettre en œuvre des mesures pour protéger votre environnement. Le système HIPS peut identifier et bloquer un comportement anormal et détecter des codes malveillants qui n'ont pas encore été décelés par les fournisseurs de services de sécurité. Mettre en œuvre et maintenir un HIPS peut s'avérer complexe et des ressources dédiées seront nécessaires pour son exécution. Lors du déploiement d'outils de détection sur hôte, votre organisation doit déterminer les stations de travail et les serveurs les plus importants pour vos opérations qui devront recevoir le déploiement des HIPS et HIDS.

Vous devez également veiller à ce que votre organisation utilise un SE qui a été récemment lancé ou est la plus récente version disponible chez le fournisseur. Votre organisation devrait mettre hors service ou remplacer les anciennes versions

de son SE dès que l'occasion se présente, plus particulièrement s'ils ne sont plus pris en charge par votre fournisseur. Les anciennes versions peuvent créer des vulnérabilités que les auteures et auteurs de menace peuvent exploiter.

Lorsque votre SE utilise une nouvelle version, l'organisation doit mettre à jour ses mécanismes de protection contre les codes malveillants pour s'assurer que son environnement est protégé. Ces mécanismes peuvent être configurés conformément à vos politiques de gestion des configurations. Ils doivent être en mesure d'effectuer des analyses périodiques de vos systèmes et des analyses fréquentes ou en temps réel du trafic externe et des données qui tentent d'accéder à votre environnement. Ces mécanismes doivent aussi pouvoir mettre en quarantaine, bloquer ou alerter vos administratrices et administrateurs de système lors de la détection de codes malveillants. Pour les faux positifs, assurez-vous que vos politiques organisationnelles traitent la réception de tout faux positif pendant que vous détectez, enquêtez ou supprimez les codes malveillants, ainsi que toute répercussion potentielle ou réelle sur la disponibilité de vos systèmes.

Dans les cas où les mécanismes de code malveillant mis en place par votre organisation ne détectent pas les codes malveillants (par exemple, des bombes logiques ou des attaques par porte dérobée), les autres protections traitées dans la présente publication veilleront à ce que les composants des logiciels et des systèmes n'effectuent que les fonctions qui leur ont été définies.

4.5 Surveillance des systèmes d'information (SI-4)

Votre organisation devrait surveiller son réseau et ses systèmes pour s'assurer que son environnement demeure protégé. Le principal objectif de la surveillance de système est de détecter des anomalies liées au trafic, au rendement du système ou au comportement des utilisatrices et utilisateurs et de mettre rapidement en œuvre des mesures d'atténuation pour empêcher une auteure potentielle ou un auteur potentiel de menace de compromettre votre environnement. Votre surveillance de système devrait comprendre des capacités permettant de détecter les attaques et les indicateurs d'attaques potentielles, ainsi que les connexions locales, réseau et distantes non autorisées. Les points d'entrée des systèmes, comme les pare-feu, doivent aussi faire l'objet d'une surveillance et les journaux connexes doivent régulièrement faire l'objet d'un examen. La surveillance des points d'extrémité est également une pratique exemplaire qui demande de traiter ces points comme des cibles très prisées, car ils peuvent fournir l'accès à des hôtes en cas de compromission.

Pour bénéficier d'une surveillance inclusive, votre organisation doit d'abord identifier sa base de référence en matière de sécurité pour déterminer ce à quoi devrait ressembler un trafic normal sur le réseau. À partir de là, il vous est possible d'étendre ou d'affiner les paramètres de vos outils de surveillance pour vous assurer d'avoir les données nécessaires pour effectuer une surveillance active du réseau et des systèmes et les protéger.

Votre organisation doit déployer un système de détection d'intrusion (SDI) et un système de prévention d'intrusion (SPI) qui travaillent en complémentarité afin d'améliorer la sécurité globale des systèmes. L'information recueillie par vos outils de surveillance d'intrusion doit être protégée et l'accès limité à celles et ceux qui en ont besoin pour accomplir les tâches associées à leur poste ou rôle. Il faut vérifier et protéger vos outils de surveillance afin de s'assurer qu'ils n'ont pas fait l'objet d'un accès, de modifications ou d'une suppression non autorisés. Vous pouvez également envisager le recours à un HIDS ou un HIPS pour détecter des anomalies dans le trafic qui pourraient indiquer des techniques de persistance ou certains types de déplacement, comme un déplacement latéral.

Dans le cadre des mesures de contrôle des applications à la section 3.5, votre organisation devrait assurer une capture et un examen des journaux d'événements pour déterminer s'il est possible de déterminer des comportements potentiellement malveillants. Ces journaux peuvent compléter vos journaux système et vous aider à enquêter et à intervenir à mesure que se produisent des incidents.

En plus de surveiller le trafic, le système de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) peut être déployé pour surveiller qui a accès à vos ressources, à partir de quels endroits et à quelle heure. La GIJIA peut aussi contribuer à déterminer une base de référence dans les comportements des utilisatrices et utilisateurs, et elle peut permettre de prévenir en cas de comportements anormaux dans votre environnement. Elle permet à votre organisation de réduire le risque de cyberattaques en empêchant les accès non autorisés à vos réseaux, à vos systèmes et à vos données. Pour obtenir plus de renseignements, consultez l'ITSAP.30.018, Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) [9].

5 Résumé

Le renforcement des systèmes d'exploitation et des applications ne représente qu'un aspect de la démarche pour améliorer votre posture de cybersécurité. En vous assurant d'avoir des paramètres de configuration de référence qui sont maintenus et examinés régulièrement, en suivant le principe du droit d'accès à une fonctionnalité minimale, et en vous protégeant et en faisant un suivi pour empêcher les attaques malveillantes d'auteures et auteurs de menace, votre organisation pourra renforcer la sécurité de son environnement.

Pour améliorer davantage votre environnement et offrir une protection optimale à votre organisation contre les cybermenaces, consultez et mettez en œuvre toutes les mesures recommandées dans le document 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089) [1]. Parmi les autres mesures que votre organisation devrait prendre, on retrouve

- la sensibilisation des employés à la cybersécurité
- la protection des points terminaux par l'application de correctifs
- la segmentation de vos réseaux
- la mise en œuvre d'une liste d'applications autorisées
- l'isolation des applications Web

6 Contenu complémentaire

6.1 Liste d'abréviations, d'acronymes et de sigles

Abréviation, acronyme ou sigle	Définition
Chef associé	Contrôle d'accès (*Access Control*) (famille de contrôles de sécurité)
CIS	Center for Internet Security
CISA	Cybersecurity & Infrastructure Security Agency
CPG	Objectifs de performance de la cybersécurité intersectoriels (*Cross-Sector Cybersecurity Performance Goals*)
DHCP	Protocole DHCP (*Dynamic Host Configuration Protocol*)
DISA	Defense Information Systems Agency
DNS	Service de noms de domaine (*Domain Name Service*)
FSI	Fournisseur de services infonuagiques
FSG	Fournisseur de services gérés
GC	Gouvernement du Canada
HIPS	Système de prévention des intrusions sur l'hôte (*Host-based Intrusion Prevention System*)
IA	Identification et authentification (famille de contrôles de sécurité)
IaaS	Infrastructure-service (*Infrastructure as a Service*)
NIP	Numéro d'identification personnel
NCP	*National Checklist Program*
NSA	*National Security Agency*
PaaS	Plateforme-service (*Platform as a Service*)
PAM	Gestion des accès privilégiés (*Privileged Access Management*)
PAW	Poste de travail avec accès privilégié (*Privilege Access Workstation*)
SaaS	Logiciel-service (*Software as a Service*)
SAW	Poste de travail administratif sécurisé (*Secure Administrative Workstation*)
SC	Protection des systèmes et des communications (familles de contrôles de sécurité)
SDIH	Système de détection des intrusions sur l'hôte (*Host-based Intrusion Detection System*)
SE	Système d'exploitation
SLAT	Traduction d'adresses de second niveau (*Second Level Address Translation*)
STIG	Guide de mise en œuvre technique de sécurité (*Security Technical Implementation Guide*)
TCP	Protocole de contrôle de transmission (*Transmission Control Protocol*)
TI	Technologies de l'information

Abréviation, acronyme ou sigle	Définition
UDP	Protocole de datagramme utilisateur (*User Datagram Protocol*)

6.2 Glossaire

Abréviation, acronyme ou sigle	Définition
Authentification multifacteur	Mécanisme pouvant ajouter une couche supplémentaire de sécurité aux appareils et aux comptes. L'authentification multifacteur exige une vérification supplémentaire (comme un numéro d'identification personnel [NIP] ou une empreinte digitale) pour accéder aux appareils ou aux comptes. L'authentification à deux facteurs est un type d'authentification multifacteur.
Bien de TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
Compte bris de glace	Un compte « bris de glace » est un compte à accès d'urgence qui comporte un accès de niveau privilégié élevé et qui n'est pas directement attribué à des personnes en particulier. Les comptes à accès d'urgence se limitent aux urgences ou aux scénarios « bris de glace » là où des comptes d'administrateur réguliers ne peuvent pas être utilisés.
Confidentialité	Valeur qui est accordée à un ensemble d'information pour indiquer son niveau de sensibilité et les restrictions d'accès mises en place pour empêcher les utilisateurs non autorisés d'y accéder.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des biens de TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des stratégies, des pratiques et des procédures de sécurité.
Contrôle de sécurité de gestion	Classe de contrôles de sécurité qui porte principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.
Contrôle de sécurité opérationnel	Classe de contrôles de sécurité qui est principalement mise en œuvre et exécutée par des personnes, mais habituellement fondée sur l'utilisation de la technologie, par exemple, un logiciel de soutien.
Contrôle de sécurité technique	Classe de contrôles de sécurité qui est mise en œuvre et exécutée par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité intégrés aux composants matériels, logiciels et micrologiciels.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à infiltrer un système informatique, un réseau ou un dispositif.
Défense en profondeur	L'utilisation de multiples couches de contrôles de sécurité et de mesures pour contribuer à réduire la possibilité d'une cyberattaque fructueuse.

Abréviation, acronyme ou sigle	Définition
Détection des intrusions	Service de sécurité qui surveille et analyse les événements réseau ou système afin d'émettre des alertes lorsqu'il détecte des tentatives d'accès non autorisé. Les résultats sont fournis en temps réel (ou quasi réel).
Disponibilité	Valeur qui est accordée aux biens d'information, aux logiciels et au matériel (l'infrastructure et ses composantes). Les données ayant la cote de disponibilité la plus élevée doivent être accessibles en permanence. Il est également entendu que la disponibilité comprend la protection des biens contre les accès non autorisés et les compromissions.
Droit d'accès minimal	Principe selon lequel une personne ne reçoit que l'ensemble des privilèges dont elle a besoin pour accomplir des tâches autorisées. Ce principe limite les dommages pouvant résulter d'une utilisation non autorisée, incorrecte ou accidentelle d'un système d'information.
Évaluation des menaces et des risques	Processus qui permet d'établir les actifs du système et la façon dont ils peuvent être compromis, d'évaluer le niveau de risque que posent les menaces pour les actifs et de recommander des mesures de sécurité pour atténuer les menaces.
Hameçonnage	Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les usurpant ou en imitant une marque commerciale connue, souvent dans le but de réaliser des gains financiers. Les hameçonneuses et hameçonneurs incitent les utilisatrices et utilisateurs à fournir leurs renseignements personnels (numéros de carte de crédit, données bancaires en ligne ou autres renseignements sensibles) afin de s'en servir pour commettre des actes frauduleux.
Intégrité	Valeur qui est accordée à l'information pour indiquer dans quelle mesure elle est susceptible à la perte de données. Il est également entendu que l'intégrité comprend l'aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice à l'information et aux biens de TI.
Pare-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre. Les ressources du système local sont ainsi protégées contre un accès de l'extérieur.
Point terminal	Dispositif informatique distant (p. ex. un portable, un ordinateur de bureau, un téléphone mobile) qui communique avec un réseau auquel il est connecté.

Abréviation, acronyme ou sigle	Définition
Rançongiciels	Type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'il ait payé une rançon.
Risque	Degré de probabilité qu'une auteure ou un auteur de menace exploite une vulnérabilité pour accéder à un bien, et répercussions connexes.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée par une auteure ou un auteur de menace en vue de compromettre les actifs ou les activités d'une organisation.

6.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33), novembre 2012.
2	Centre canadien pour la cybersécurité, Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089), septembre 2021.
3	National Institute of Standards and Technology, National Checklist Program for IT products: Guidelines for checklist users and developers (SP 800-70 Rev. 4), février 2018.
4	Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), Kubernetes Hardening Guide, août 2022.
5	Cybersecurity and Infrastructure Security Agency, Key Findings to Improve Monitoring and Hardening of Networks, février 2023.
6	Centre canadien pour la cybersécurité, Étapes à suivre pour déployer efficacement l'authentification - ITSAP.00.105), mai 2023.
7	Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals, mars 2023.
8	Centre canadien pour la cybersécurité, Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées - ITSM.10.095, août 2022.
9	Centre canadien pour la cybersécurité, Gestion de l'identité, des justificatifs d'identité et de l'accès (ITSAP.30.018), août 2022.

Annex A Catalogue des contrôles de sécurité de l'ITSG-33

A.1 Contrôles de sécurité opérationnels : Gestion des configurations

Le tableau 1 décrit les contrôles **CM-2 Configuration de référence** et **CM-7 Fonctionnalité minimale**, tels qu'ils sont décrits à l'annexe 3A de l'ITSG-33 [2].

Table 1: Contrôles de sécurité opérationnels de l'ITSG-33 : CM-2, CM-6 et CM-7

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
CM-2	Configuration de référence	(A) L'organisation élabore, consigne et tient à jour une configuration de référence courante du système d'information dans le cadre du contrôle des configurations.	**Examens et mises à jour :** L'organisation examine et met à jour la configuration de référence du système d'information : i. [*fréquence définie par l'organisation*]; ii. au besoin, selon [*circonstances définies par l'organisation*]; iii. dans le cadre des installations et des mises à niveau des composants du système d'information. Voir le contrôle connexe CM-5. **Automatisation du soutien aux fins d'exactitude et d'actualité :** L'organisation utilise des mécanismes automatisés pour assurer le maintien d'une configuration de référence à jour, complète, exacte et facilement accessible. Voir les contrôles connexes CM-7 et RA-5. **Conservation des configurations antérieures :**	CM-3 CM-6 CM-8 CM-9 SA-10

			L'organisation conserve [*versions de configurations de référence antérieures définies par l'organisation* du *système d'information*] pour permettre le retour à la version précédente. **Environnements de test et de développement :** L'organisation conserve pour les environnements de développement et de tests des systèmes d'information une configuration de référence gérée séparément de la configuration de référence opérationnelle. Voir les contrôles connexes CM-4 et SC-3. **Configuration de systèmes, de composants ou de dispositifs pour des secteurs à risques élevés :** i. L'organisation remet [*systèmes d'information, composants de système ou dispositifs définis par l'organisation*] dotés de [*configurations définies par l'organisation*] aux personnes qui se rendent dans des endroits que l'organisation juge très risqués. ii. L'organisation applique [*mesures de protection de sécurité définies par l'organisation*] aux dispositifs lors du retour de ces personnes.	
CM-6	Paramètres de configuration :	(A) L'organisation établit et documente les paramètres de configuration pour les produits de technologie de l'information intégrés au système d'information en utilisant [des listes de vérification concernant la configuration de sécurité définies par l'organisation] qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles. (B) L'organisation met en œuvre les paramètres de configuration. (C) L'organisation détermine, documente et approuve tout écart en ce qui a trait aux paramètres de configuration établis pour	**Gestion, application et vérification centralisées automatisées :** L'organisation a recours à des mécanismes d'automatisation pour gérer, appliquer et vérifier les paramètres de configuration de [*composants de système d'information définis par l'organisation*]. Voir les contrôles connexes CA-7 et CM-4. **Intervention lorsque des changements non autorisés sont apportés :** L'organisation a recours à [*mécanismes de sécurité définis par l'organisation*] pour intervenir lorsque des	AC-19 CM-2 CM-3 CM-7 SI-4

		[*composants de système d'information définis par l'organisation*] en tenant compte de [*exigences opérationnelles définies par l'organisation*]. (D) L'organisation surveille et contrôle les changements apportés aux paramètres de configuration conformément à ses politiques et procédures.	changements non autorisés sont apportés aux [*paramètres de configuration définis par l'organisation*]. Voir les contrôles connexes IR-4 et SI-7.	
CM-7	Fonctionnalité minimale	(A) L'organisation configure le système d'information pour qu'il ne fournisse que les capacités essentielles. (B) L'organisation interdit ou restreint l'utilisation des fonctions, des ports, des protocoles et des services suivants : [*fonctions, ports, protocoles ou services définis par l'organisation*].	**Examen périodique :** L'organisation examine le système d'information [*fréquence définie par l'organisation*] pour identifier les fonctions, ports, protocoles ou services non requis et non sécurisés. L'organisation désactive [*fonctions, ports, protocoles et services du système d'information jugés inutiles et non sécurisés définis par l'organisation*]. Voir les contrôles AC18, CM-7 et IA-2 connexes. **Prévention de l'exécution des programmes :** Le système d'information empêche l'exécution des programmes conformément aux [*sélection d'un choix ou plus : politiques sur l'utilisation de programmes logiciels et restrictions connexes définies par l'organisation; règles d'autorisation des modalités d'utilisation d'un programme*]. Voir le contrôle connexe CM-8. **Conformité aux exigences d'enregistrement :** L'organisation assure le respect des [*exigences d'enregistrement définies par l'organisation concernant les fonctions, ports, protocoles et services*]. **Logiciel non autorisé et liste d'exclusion :**	AC-6 CM-2 RA-5 SA-5 SC-7

			L'organisme détermine [*les programmes logiciels non autorisés à s'exécuter sur le système d'information*]. L'organisation a recours à une politique tout permettre, interdire par exception pour empêcher l'exécution des programmes logiciels non autorisés sur le système d'information. L'organisation examine et met à jour la liste des programmes logiciels non autorisés [*fréquence définie par l'organisation*]. Voir les contrôles connexes CM-6 et CM-8. **Logiciel autorisé et mise sur liste d'autorisation :** L'organisme détermine [*les programmes logiciels autorisés à s'exécuter sur le système d'information*]. L'organisation a recours à une politique tout permettre, interdire par exception pour permettre l'exécution des programmes logiciels autorisés sur le système d'information. L'organisation examine et met à jour la liste des programmes logiciels autorisés [*fréquence définie par l'organisation*]. Voir les contrôles CM-2, CM-6, CM-8, SA-10, SC-34 et SI-7 connexes.	

A.2 Contrôles de sécurité opérationnels : Intégrité de l'information et des systèmes

Le tableau 2 décrit les contrôles **SI-3 Protection contre les codes malveillants** et **SI-4 Surveillance des systèmes d'information**, tels qu'ils sont décrits à l'annexe 3A de l'ITSG-33 [2].

Table 2: Contrôles de sécurité opérationnels de l'ITSG-33 : SI-3 et SI-4

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SI-3	Protection contre les codes malveillants	(A) L'organisation utilise des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie du système d'information afin de détecter et d'éradiquer les codes malveillants. (B) L'organisation met à jour ses mécanismes de protection contre les codes malveillants dès la diffusion de nouvelles versions, conformément à sa stratégie et à ses procédures de gestion des configurations. (C) L'organisation configure les mécanismes de protection contre les codes malveillants de manière à : i. effectuer des analyses périodiques du système d'information [*fréquence définie par l'organisation*] et des balayages en temps réel des fichiers de sources externes [*sélection (un choix ou plus) : points d'extrémité, point d'entrée ou point de sortie du réseau*] lors de leur téléchargement, de leur ouverture ou de leur exécution, conformément à sa politique de sécurité; et	**Gestion centrale :** L'organisation centralise la gestion des mécanismes de protection contre les codes malveillants. Voir les contrôles connexes AU-2 et SI-8. **Mises à jour automatiques :** Le système d'information met automatiquement à jour les mécanismes de protection contre les codes malveillants. Voir le contrôle connexe SI-8. **Mises à jour seulement par utilisatrices et utilisateurs privilégiés :** Le système d'information met à jour les mécanismes de protection contre les codes malveillants uniquement lorsqu'un utilisateur privilégié le demande. Voir les contrôles connexes AC-6 et CM-5. **Tests et évaluations :** L'organisation teste les mécanismes de protection contre les codes malveillants [*fréquence définie par l'organisation*] en en introduisant dans le système	CM-3 MP-2 SA-4 SA-8 SA-12 SA-13 SC-7 SC-26 SC-44 SI-2 SI-4 SI-7

		ii. [*Sélection (un ou plusieurs) mesures définies par l'organisation* : *bloque le code malveillant; met le code malveillant en quarantaine, envoie une alerte à l'administratrice ou administrateur*] en réponse à la détection d'un code malveillant. (D) L'organisation traite les faux positifs résultant de la détection et de l'éradication de codes malveillants et leurs répercussions potentielles sur la disponibilité des systèmes d'information.	d'information un scénario de test anodin connu et non invasif. L'organisation vérifie qu'il y a effectivement, comme il se doit, détection du scénario et signalement des incidents qui lui sont associés. Voir les contrôles CA-2, CA-7 et RA-5 connexes. **Détection non axée sur les signatures :** Le système d'information met en œuvre des mécanismes non axés sur les signatures de détection de codes malveillants. **Détection des commandes non autorisées :** Le système d'information détecte [*commandes non autorisées du système d'exploitation définies par l'organisation*] dans l'interface de programmation d'application du noyau dans [*composantes matérielles du système d'information définies par l'organisation*] et [*sélection d'un choix ou plus : émet un avertissement; vérifie l'exécution de la commande, empêche l'exécution de la commande*]. Voir le contrôle connexe AU-6. **Authentification des commandes à distance :** Le système d'information met en œuvre [mécanismes de sécurité définis par l'organisation] afin d'authentifier [*commandes à distance désignées par l'organisation*]. Voir les contrôles SC-12, SC-13 et SC-23 connexes. **Analyse des codes malveillants :** L'organisation emploie [*outils et techniques définis par l'organisation*] pour analyser les caractéristiques et les comportements des codes malveillants.	

			L'organisation intègre les résultats des analyses des codes malveillants à son plan des interventions en cas d'incident et à ses processus de correction des anomalies.	
SI-4	Surveillance des systèmes d'information	(A) L'organisation surveille le système d'information pour y détecter : i. des attaques et des signes indiquant de possibles attaques conformément à des [*objectifs de surveillance définis par l'organisation*], ii. des connexions locales, réseau ou à distance non autorisées. (B) L'organisation détermine qu'il y a une utilisation non autorisée de son système d'information [*techniques et méthodes définies par l'organisation*]. (C) L'organisation déploie dans le système d'information des dispositifs de surveillance à la fois i. stratégiquement pour collecter l'information; ii. de manière aléatoire pour faire le suivi des types de transactions qui l'intéressent particulièrement. (D) L'organisation protège l'information obtenue des outils de surveillance des intrusions contre tout accès non autorisé et toute modification et suppression. (E) L'organisation élève le niveau des activités de surveillance du système d'information dès qu'il y a indication de risque accru pour les activités et les biens de l'organisation, les personnes, les autres organisations ou le	**Système de détection d'intrusion dans l'ensemble du système :** L'organisation connecte et configure les outils individuels de détection d'intrusion en un système organisationnel unique. **Outils automatisés aux fins d'analyse en temps réel :** L'organisation utilise des outils automatisés pour prendre en charge l'analyse des événements en temps quasi réel. **Intégration d'outils automatisés :** L'organisation utilise des outils automatisés pour intégrer les outils de détection d'intrusion aux mécanismes de contrôle d'accès et de flux afin de permettre la reconfiguration de ces mécanismes en vue d'isoler et d'éliminer rapidement les attaques. **Trafic de communications entrantes et sortantes :** Le système d'information surveille les communications entrantes et sortantes [*fréquence définie par l'organisation*] pour détecter toute activité ou condition inhabituelle ou non autorisée. **Alertes générées par le système** Le système d'information produit des alertes [*personnel ou rôles définis par l'organisation*] lorsque	AC-3 AC-4 AC-8 AC-17 AU-2 AU-7 AU-9 AU-12 CA-7 IR-4 PE-3 RA-5 SC-7 SC-26 SC-35 SI-3 SI-7

		Canada selon l'information mise à sa disposition (information relative au contrôle d'application de la loi, découlant du renseignement ou provenant d'autres sources crédibles). (F) L'organisation obtient un avis juridique concernant les activités de surveillance du système d'information conformément aux lois et aux politiques, directives et normes du gouvernement. (G) L'organisation fournit [*types de renseignements liés à la surveillance du système d'information définis par l'organisation*] à [*personnel ou rôles définis par l'organisation*], et ce, [*sélection (un choix ou plus) : au besoin]; [fréquence définie par l'organisation*].	les indications de compromission réelle ou potentielle se présentent. Voir les contrôles connexes AU-5 et PE-6. **Réponse automatisée à des événements suspects :** Le système d'information informe [*le personnel chargé d'intervenir en cas d'incident défini par l'organisation, identifié par nom ou rôle*] des événements suspects et prend [*les mesures les moins perturbatrices définies par l'organisation pour mettre fin aux événements suspects*]. **Outils de surveillance des tests :** L'organisation teste les outils de surveillance des intrusions [*fréquence définie par l'organisation*]. Voir le contrôle connexe CP-9. **Visibilité des communications chiffrées :** L'organisation prend les mesures nécessaires pour rendre [*trafic de communications chiffrées défini par l'organisation*] visible aux [*outils de surveillance du système d'information définis par l'organisation*]. **Analyse des anomalies du trafic de communication :** L'organisation analyse le trafic des communications sortantes à la frontière externe du système [*certains de ses points intérieurs, comme des sous-réseaux et des sous-systèmes définis par l'organisation*] pour découvrir des anomalies. **Alertes automatisées :** L'organisation utilise des mécanismes automatisés pour alerter le personnel de sécurité des répercussions	

			potentielles des activités inhabituelles ou inappropriées [q*ui déclenchent des alertes définies par l'organisation*]. Voir les contrôles connexes AC-18 et IA-3. **Analyse du trafic et de la tendance des événements :** L'organisation analyse le trafic des communications ou la tendance des événements pour le système d'information. L'organisation développe des profils représentant les modèles de trafic ou les événements communs. L'organisation utilise le trafic / les profils des événements pour calibrer les dispositifs de surveillance afin de réduire le nombre de faux positifs et le nombre de faux négatifs. Voir les contrôles connexes AC-18 et IA-3. **Système de détection d'intrusion sans fil** L'organisation utilise un système de détection d'intrusions sans fil pour identifier les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions ou infractions potentielles liées au système d'information. Voir les contrôles connexes : AC-18 et IA-3. **Communications entre un réseau sans fil et un réseau filaire :** L'organisation utilise un système de détection d'intrusions pour surveiller le trafic de communications sans fil lorsqu'il passe d'un réseau sans fil à un réseau filaire. Voir le contrôle connexe AC-18.	

			Corrélations entre les résultats des activités de surveillance : L'organisation établit des corrélations entre les informations provenant des outils de surveillance employés dans l'ensemble du système d'information. Voir le contrôle connexe AU-6. **Connaissance intégrée de la situation :** L'organisation met en corrélation les résultats de la surveillance des activités physiques, des cyberactivités et des activités de la chaîne d'approvisionnement pour développer une connaissance intégrée de la situation à l'échelle organisationnelle. Voir le contrôle connexe SA-12. **Analyse du trafic et exfiltrations masquées :** L'organisation analyse le trafic des communications sortantes à la frontière externe du système (par exemple, un périmètre du système) et à [*certains de ses points intérieurs (comme des sous-réseaux ou des sous-systèmes) définis par l'organisation*] pour y détecter des exfiltrations masquées d'informations. **Personnes qui posent un grand risque :** L'organisation met en œuvre [*surveillance supplémentaire définie par l'organisation*] des personnes qui ont été identifiées par [*sources définies par l'organisation*], car elles représentent un plus grand risque. **Utilisatrice ou utilisateur privilégié :** L'organisation met en œuvre [*surveillance supplémentaire définie par l'organisation*] des utilisatrices et utilisateurs privilégiés.	

			Périodes d'essai : L'organisation met en œuvre [*surveillance supplémentaire définie par l'organisation*] des personnes pendant [*période probatoire définie par l'organisation*]. **Services de réseau non autorisés :** Le système d'information détecte les services de réseau qui n'ont pas été autorisés ou approuvés par [*autorisation ou processus d'approbation définis par l'organisation*] et [*sélection (un choix ou plus) : vérifications; alertes; personnel ou rôles désignés par l'organisation*]. Voir les contrôles AC-6, CM-7, SA-5 et SA-9 connexes. **Dispositifs au niveau de l'hôte :** Les organisations mettent en œuvre [*mécanismes de surveillance au niveau de l'hôte définis par l'organisation*] à [*composants des systèmes d'information désignés par l'organisation*]. **Indicateurs de compromission :** Le système d'information découvre, recueille, distribue et utilise les indicateurs de compromission.	