OBJECTIFS RELATIFS À L'ÉTAT DE PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ

SÉCURISER LES SYSTÈMES LES PLUS ESSENTIELS

VERSION 1.0

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Canada

Objectifs relatifs à l’état de préparation en matière de cybersécurité : Sécuriser les systèmes les plus essentiels

D96-122/2024F-PDF
978-0-660-73265-7

Date d’entrée en vigueur
Le présent document entre en vigueur le 29 octobre 2024.

Historique des révisions
29 octobre 2024 Première version

Message du dirigeant principal du Centre pour la cybersécurité

J'ai le plaisir d'annoncer la publication des Objectifs relatifs à l'état de préparation en matière de cybersécurité (OEPC) du Centre canadien pour la cybersécurité. Ces objectifs ont été élaborés en réponse à la vulnérabilité croissante des infrastructures essentielles (IE) aux cyberattaques. Ces objectifs intersectoriels visent à renforcer la cybersécurité et à minimiser les risques auxquels sont exposées la société, la sécurité publique et la stabilité globale de l'économie canadienne. Les infrastructures essentielles du Canada font face à un immense défi en ce qui a leur résilience à l'égard des cybermenaces.

Aider le Canada à devenir plus résilient est un aspect essentiel du rôle du Centre pour la cybersécurité en tant qu'autorité technique du Canada en matière de cybersécurité. Les OEPC présentent des mesures concrètes pour les infrastructures essentielles qui méritent d'être mises en œuvre en tout temps. Le Centre pour la cybersécurité est aussi à développer un cadre relatif à l'état de préparation en matière de cybersécurité (CRF pour Cyber Security Readiness Framework) qui réunira les objectifs intersectoriels et les objectifs liés à des secteurs spécifiques pour permettre aux infrastructures essentielles d'atténuer efficacement les cybermenaces. Le Centre pour la cybersécurité élabore ces ressources pour vous permettre (propriétaires et exploitants des systèmes) de protéger les systèmes qui sont indispensables aux infrastructures canadiennes, à la sécurité nationale et à la sécurité publique. Grâce à la mise en œuvre de ces mesures et à l'adoption d'une approche intersectorielle, nous mettons en place un mécanisme de défense solide et efficace pour faire face collectivement au contexte de la menace à la cybersécurité en constante évolution.

Notre plus grande priorité est d'assurer la sûreté, la sécurité et la prospérité du Canada et de la population canadienne. Les OEPC représentent une étape importante de nos efforts continus visant à protéger nos infrastructures, systèmes et services essentiels. Nous vous remercions sincèrement pour votre soutien et votre coopération, car sachez que vous jouez un rôle crucial dans le succès de ces initiatives. Nous recommandons que vous vous teniez informées et informés de nos activités de collaboration liées à la cybersécurité et que vous y preniez une part active.

Rajiv Gupta
Dirigeant principal du Centre canadien pour la cybersécurité
29 octobre 2024

Vue d'ensemble

Les OEPC consistent en 36 objectifs fondamentaux visant à renforcer la cybersécurité. Les objectifs sont groupés selon six piliers tirés du cadre Cybersecurity Framework 2.0 du National Institute of Standards and Technology[1] (NIST) (en anglais seulement). Chaque objectif est lié à des mesures recommandées concrètes qui, si elles sont prises, renforceront la posture de cybersécurité des infrastructures essentielles du Canada. Les objectifs sont aussi associés à ce qui suit :

- résultats
- risques gérés
- références au cadre Cybersecurity Framework 2.0
- orientation supplémentaire

Les OEPC s'adressent aux praticiennes et praticiens de la cybersécurité et ils sont présentés, au complet, dans la Boîte à outils des objectifs intersectoriels[2].

Bien que les OEPC ont été élaborés pour les infrastructures essentielles, toute organisation au Canada peut utiliser les recommandations formulées pour renforcer sa posture de cybersécurité. Les OEPC constituent un objectif commun et un langage partagé pouvant favoriser les liens qui permettent de renforcer la résilience des réseaux desquels dépend la population canadienne.

Le contexte des cybermenaces est en constante évolution. C'est la raison pour laquelle les OEPC seront mis à jour régulièrement pour soutenir les organisations dans leurs efforts visant à atténuer efficacement les cybermenaces émergentes. Ces mises à jour vont privilégier les objectifs liés à des secteurs particuliers et comprendront une rétroaction de la part de parties prenantes.

1 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
2 https://www.cyber.gc.ca/fr/objectifs-relatifs-letat-preparation-matiere-cybersecurite/boite-outils-objectifs-relatifs-letat-preparation-matiere-cybersecurite-intersectoriels

Table des matières

Liste des figures

Liste des annexes

LE CONTEXTE DES CYBERMENACES

La sécurité et la prospérité du Canada doivent pouvoir s'appuyer sur des infrastructures essentielles solides et résilientes. La population canadienne compte sur les IE pour lui procurer les besoins de la vie quotidienne, y compris l'eau, l'énergie et les services financiers. Une perturbation de ces infrastructures essentielles pourrait mener à la perte de services essentiels, compromettre la propriété intellectuelle, causer des torts à la population ou même se traduire par des pertes de vie. C'est pourquoi la protection des IE du Canada est essentielle à la sécurité nationale.

Les exploitants et propriétaires d'infrastructures canadiennes doivent faire face à un contexte de menaces en évolution alors que le degré de sophistication des cyberactivités malveillantes continue de prendre de l'ampleur. Le Centre pour la cybersécurité, qui fait partie du gouvernement du Canada (GC), travaille avec les ministères à l'interne, les propriétaires et exploitants d'infrastructures essentielles, les entreprises canadiennes et des partenaires internationaux pour se préparer, intervenir en cas d'incident ou atténuer les conséquences qui découlent des cyberincidents. Les OEPC permettent aux secteurs des infrastructures essentielles canadiennes de s'appuyer sur des objectifs réalistes et réalisables pour renforcer leur posture de cybersécurité. Les OEPC peuvent contribuer à réduire le nombre des cyberattaques et l'ampleur de celles-ci.

Cybermenaces auxquels font face les secteurs des infrastructures essentielles

Dans l'Évaluation des cybermenaces nationales 2023-2024[3], le Centre pour la cybersécurité a indiqué que les infrastructures essentielles sont exposées à des risques croissants en raison d'activités de cybermenace émanant de cybercriminelles et cybercriminels et d'auteures et auteurs de menace parrainés par des États. Nous estimons que dans les deux prochaines années, des cybercriminelles et cybercriminels motivés par l'appât du gain continueront presque certainement à cibler des organisations de grande valeur œuvrant dans les secteurs des infrastructures essentielles du Canada et partout dans le monde.[1]

↘ Cyberactivités malveillantes cautionnées par des nations

Les infrastructures essentielles sont des cibles de choix des cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord. Les auteures et auteurs de cybermenace qui agissent pour le compte d'États adversaires ont principalement recours à des activités de cybermenace pour :

- mener à bien leurs objectifs géopolitiques;
- exécuter des opérations de cyberespionnage;
- se prépositionner en cas d'éventuelles hostilités;
- faire acte de force et intimider d'autres pays.

En février 2022, des cyberactivités malveillantes parrainées par la Russie contre l'Ukraine ont perturbé ou ont tenté de perturber les activités dans les secteurs publics, financiers et énergétiques, et elles coïncidaient souvent avec des opérations militaires conventionnelles. Ces attaques se sont étendues au-delà de l'Ukraine pour impliquer également les IE européennes. Par exemple, l'attaque de la Russie visant un fournisseur de services Internet par satellite européen a entraîné une importante panne dans plusieurs pays d'Europe.[2] Des opérations de désinformation coordonnées en appui au discours de la Russie au sujet de l'invasion ont également accompagné les activités militaires et les cyberactivités.[3]

En mai 2023, le groupe Volt Typhoon, associé à la République populaire de Chine, a été détecté dans des réseaux d'IE des États-Unis.[4] Les principales tactiques, techniques et procédures (TTP) du groupe impliquent l'attaque d'exploitation des ressources locales, qui fait appel à des outils intégrés d'administration réseau pour atteindre les buts escomptés et permettre au groupe d'avoir une présence soutenue et d'échapper à la détection. En février 2024, les États-Unis ont confirmé que Volt Typhoon avait compromis les environnements informatiques de plusieurs organisations des infrastructures essentielles aux États-Unis, principalement dans les secteurs des communications, de l'énergie, des systèmes de transport, ainsi que des systèmes d'aqueduc et d'égout.[5]

3 https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

↘ Rançongiciels

Les infrastructures essentielles sont des cibles particulièrement attrayantes en ce qui a trait aux rançongiciels. En effet, les cybercriminelles et cybercriminels perçoivent les exploitants d'infrastructures essentielles comme étant prêts à payer de lourdes rançons pour limiter ou éviter les interruptions et les répercussions subséquentes sur leur clientèle. Aussi connues sous le nom de « chasse au gros gibier », les attaques ciblées par rançongiciel ont touché des milliers de fournisseurs de soins de santé et d'autres infrastructures essentielles, de gouvernements et de grandes entreprises au Canada et à travers le monde.

↘ Technologie opérationnelle connectée

Les fournisseurs d'IE adoptent de plus en plus les technologies de l'information (TI) pour connecter leur environnement de technologies opérationnelles (TO). Les TO connectées à Internet peuvent rendre les processus plus efficaces grâce à un partage de données, une gestion centralisée et une automatisation plus efficaces. Le marché mondial des TO intelligentes devrait atteindre plus de quatre billions de dollars d'ici 2030.[6] Des améliorations technologiques ont permis d'accélérer l'adoption des TO connectées, ce qui rend plus facile la connexion de dispositifs à distance et à grande échelle; on peut penser notamment au réseau 5G et à l'infrastructure Internet par satellite. Bien que les TO connectées apportent de nombreux avantages, elles augmentent également la vulnérabilité des fournisseurs d'IE à l'égard des activités de cybermenace.

↘ Technologies facilitées par l'intelligence artificielle

Les propriétaires et exploitants d'infrastructures essentielles adoptent également des technologies de l'intelligence artificielle (IA) pour rendre leurs processus et opérations plus efficaces. Toutefois, le recours à des technologies de l'IA sans protection adéquate peut exposer les infrastructures essentielles à des risques nouveaux. Les mêmes technologies qui permettent aux exploitants des infrastructures essentielles de simplifier leurs méthodes de travail, par exemple, le contrôle à distance d'un système par une interface Web peut permettre à des auteures et auteurs de cybermenace de détourner des systèmes de TO et de provoquer dommages et destruction.

Toutes les technologies de l'IA, comme ChatGPT d'Open AI, peuvent être exploitées par des auteures et auteurs de cybermenace pour concevoir des attaques plus sophistiquées, comme l'hameçonnage, le piratage psychologique, la mésinformation ou la désinformation et l'usurpation d'identité. Les auteures et auteurs de menace peuvent aussi se servir de l'IA pour développer des maliciels évolués qui peuvent éviter les systèmes de surveillance et les logiciels antivirus traditionnels.

Le fait qu'elles puissent permettre aux auteures et auteurs de menace d'exercer une influence considérable suscite de grandes inquiétudes quant aux technologies de l'IA. Par exemple, une manipulation délibérée du code sous-jacent et des outils qui l'utilisent risque de permettre à des menaces internes de s'attaquer à la chaîne d'approvisionnement à toutes les étapes, de la conception jusqu'à la distribution et à la correction des logiciels.

Attaques par rançongiciel ciblant les infrastructures essentielles

MAI 2021

Des attaques par rançongiciel commises contre Colonial Pipeline aux États-Unis, et les activités nord-américaines et australiennes de JBS Foods, ont rapporté plusieurs millions de dollars en gains aux auteurs de menace. Ces attaques ont causé des perturbations majeures au sein de la chaîne d'approvisionnement en carburant et de la chaîne agroalimentaire.[7][8]

OCTOBRE 2021

Le réseau du système de santé de Terre-Neuve-et-Labrador a été victime d'une attaque par rançongiciel. Le groupe de rançongiciel Hive est responsable de l'attaque qui a causé une panne de systèmes de TI;[9] la panne a touché plus d'une personne sur dix dans la province et causé des dommages d'un peu moins de 16 millions de dollars.[10]

DÉCEMBRE 2022

L'hôpital SickKids de Toronto a été attaqué par un partenaire du groupe de rançongiciel LockBit. L'attaque a eu peu de répercussions sur les patientes et patients, et leur famille, mais elle a quand même causé des retards de diagnostic ou de traitement.[11]

NOVEMBRE 2023

Moneris, une entreprise de technologie canadienne spécialisée dans les solutions de traitement des paiements, a fait l'objet d'une tentative de rançongiciel. Le groupe de rançongiciel Medusa a revendiqué la responsabilité, mais selon Moneris, aucune donnée sensible n'a été touchée par l'attaque.[12]

CE QUI A MENÉ AUX OEPC

Le GC reconnaît l'importance de la collaboration pour protéger les cybersystèmes essentiels. Deux publications consécutives de la Stratégie nationale de cybersécurité (en 2010 et en 2018) ont mis l'emphase sur le rôle de leadership et de facilitation du gouvernement dans le soutien du secteur privé dans le cadre de son rôle de gérance et de mise en œuvre.[13][14] Cette approche d'équipe est essentielle pour permettre d'augmenter le niveau de base de la cybersécurité.

Le Centre pour la cybersécurité a élaboré les OEPC pour soutenir les investissements qui revalorisent la posture de cybersécurité dans les IE. Les OEPC ont été conçus pour répondre aux besoins des propriétaires et exploitants des systèmes au Canada. Les OEPC sont aussi en accord avec les travaux récents réalisés par les partenaires internationaux du Centre pour la cybersécurité. Par exemple :

- Le National Cyber Security Centre du Royaume-Uni a compilé un ensemble de ressources pour les organisations qui jouent un rôle déterminant dans la vie quotidienne au Royaume-Uni, à savoir les organisations désignées comme faisant partie des infrastructures essentielles nationales. Cet ensemble, appelé Cyber Assessment Framework[4] (en anglais seulement) et ayant d'abord été publié en 2018, propose des principes concernant la cybersécurité et la résilience, ainsi que des conseils sur la façon d'appliquer ces principes.
- En juillet 2021, le gouvernement américain a lancé une initiative relative à la cybersécurité des systèmes de contrôle industriels et a invité la Cybersecurity and Infrastructure Security Agency (CISA) à élaborer des objectifs de performance de la cybersécurité pour les IE. Le document Cross-Sector Cybersecurity Performance Goals[5] (CPGs) de la CISA a été publié la première fois en octobre 2022.

Importance des OEPC

Les OEPC constituent un point de départ pour conduire les IE canadiennes vers une posture de cybersécurité plus résiliente.

Votre organisation pourra tirer parti de ces conseils pour améliorer son état de préparation en matière de cybersécurité. Lorsque vous mettrez en œuvre les OEPC, vous serez en mesure de constater la pertinence de leur harmonisation avec d'autres modèles. Les OEPC sont manifestement liés à des cadres existants, par exemple, les CPG de la CISA et le NIST CSF 2.0, ce qui permet à votre organisation de concentrer ses efforts sur la mise en œuvre de ces objectifs, plutôt que d'intégrer un nouveau modèle à ses activités courantes. Cette option est particulièrement avantageuse pour les organisations exerçant des activités transfrontalières entre le Canada et les États-Unis.

Votre organisation gagnera également à s'associer avec d'autres organisations de façon collective. Toutes les organisations profiteront des objectifs partagés des OEPC. Une fois les objectifs atteints, ils renforceront l'ensemble de la cyberposture de tous les secteurs au Canada. En plus d'offrir un objectif commun, les OEPC fournissent aussi un langage commun qui favorise la discussion, l'apprentissage collectif et l'amélioration continue. En adoptant cette forme d'échange, les OEPC permettront de mieux établir et soutenir les liens qui peuvent renforcer la résilience des infrastructures qui sont essentielles à la sécurité nationale du Canada et à son bien-être.

La section qui suit propose des conseils sur l'utilisation des OEPC pour soutenir la cybersécurité dans votre organisation.

4 https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
5 https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

EXPLICATION DES OEPC

Les objectifs relatifs à l'état de préparation en matière de cybersécurité intersectoriels sont un sous-ensemble des priorités liées aux recommandations fondamentales pouvant servir à toute organisation d'IE au Canada. Il s'agit de mesures que, si elles sont prises, peuvent considérablement renforcer la cybersécurité dans tous les secteurs des infrastructures essentielles. Chaque objectif est associé à des résultats de cybersécurité prévus.

Les organisations de toute taille et de n'importe quel secteur devraient être en mesure d'atteindre les OEPC. Les objectifs visent à établir une norme générale pour les pratiques en matière de cybersécurité, soit une base de référence qui s'harmonise avec d'autres conseils et cadres existants, au Canada et chez nos partenaires internationaux. Les OEPC constituent des actions intentionnelles visant à renforcer la posture de cybersécurité de votre organisation. Ils ne doivent pas être considérés comme un cadre exhaustif régissant la cybersécurité ou une approche universelle à l'égard de la cybersécurité.

Étant donné que les OEPC se veulent un point de départ, nous encourageons votre organisation à prendre des décisions éclairées en fonction du risque basées sur un contexte donné. Par exemple, votre organisation doit préciser selon quelle fréquence les objectifs identifiés dans les OEPC devraient être réévalués. Votre organisation devrait aussi donner priorité aux objectifs en se basant sur la maturité de son programme de cybersécurité, en cherchant toujours à renforcer la cybersécurité en mettant en œuvre autant de mesures recommandées que le permettent les ressources.

Principales caractéristiques des OEPC

- **Objectif :** Les OEPC sont des lignes directrices facultatives pour renforcer la cybersécurité des IE et ne constituent pas une liste exhaustive d'exigences ou de mesures imposées.
- **Étendue :** Les OEPC sont un sous-ensemble des priorités liées aux recommandations fondamentales en matière de cybersécurité pour les TI et les TO. Les objectifs ne suffisent pas à eux seuls pour assurer une pleine protection contre tous les risques liés à la cybersécurité.
- **Applicabilité :** On peut appliquer les OEPC dans tous les secteurs des infrastructures essentielles au Canada, car ils ne sont pas spécifiquement adaptés à des secteurs ou systèmes individuels.

OEPC intersectoriels par piliers

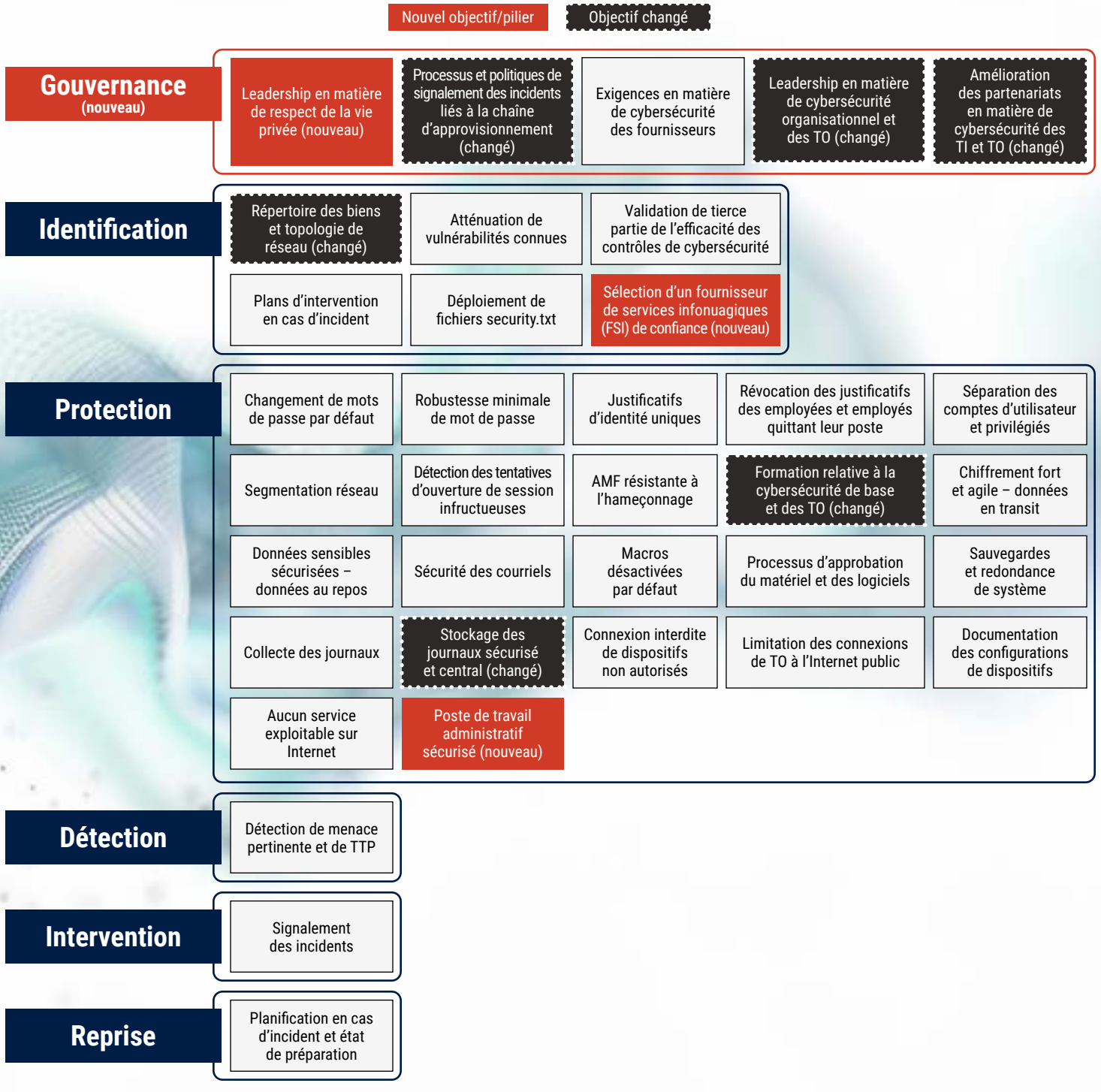
Dans ce document d'orientation, les OEPC sont décrits dans un profil visuel abrégé qui compare les OEPC du Centre pour la cybersécurité et les CPG de la CISA (voir la figure 1). Lorsqu'il est indiqué « modifié » ou « nouveau » pour les composants du modèle (indication en gris foncé ou orange, respectivement), ceux-ci sont en comparaison avec les CPG. Le contraste visuel permet d'illustrer l'étendue des similitudes par rapport au modèle de la CISA pour soutenir les exploitants transfrontaliers et les exploitants qui connaissent déjà les CPG. Se reporter à l'annexe A : Différences entre les OEPC et les CPG pour avoir une description complète des différences entre les OEPC et les CPG.

La figure montre les 36 OEPC classés en six piliers. Consultez la Boîte à outils des objectifs intersectoriels[6] pour l'intégralité des OEPC.

Les OEPC et la Boîte à outils des objectifs intersectoriels ont été conçus pour les praticiennes et praticiens qui sont en mesure d'appliquer les conseils détaillés à leurs systèmes.

6 https://www.cyber.gc.ca/fr/objectifs-relatifs-letat-preparation-matiere-cybersecurite/boite-outils-objectifs-relatifs-letat-preparation-matiere-cybersecurite-intersectoriels

Figure 1 : Objectifs relatifs à l'état de préparation en matière de cybersécurité par pilier



LE MODÈLE OEPC

Les OEPC sont conformes aux cadres et aux conseils existants, au Canada et auprès de nos partenaires internationaux. La présente section vise à faire connaître ce que les OEPC offrent pour les IE au Canada, outre les modèles actuels.

Conformité aux objectifs de rendement en matière de cybersécurité intersectoriels de la CISA

Dans de nombreux secteurs, des entreprises canadiennes travaillent étroitement avec des homologues américains. Certaines de ces entreprises disposent d'infrastructures qui traversent la frontière internationale. Compte tenu de ces interdépendances, le Centre pour la cybersécurité a consulté la CISA durant l'élaboration des OEPC pour s'assurer que les objectifs pouvaient être facilement mis en œuvre dans tous les secteurs des infrastructures essentielles en Amérique du Nord.

Actuellement, la version 1.0.1 des CPG de la CISA comporte 38 objectifs de cybersécurité. Les OEPC du Centre pour la cybersécurité comportent 36 objectifs de cybersécurité. Il y a des différences importantes entre les OEPC et les CPG. Aux fins d'harmonisation avec la version la plus récente du NIST CSF 2.0, les OEPC comprennent un pilier « gouvernance », avec des objectifs qui mettent en lumière l'importance d'établir des politiques et procédures au sein de l'organisation. Comme c'est le cas pour d'autres mises à jour apportées au CSF, le pilier gouvernance comporte un objectif en lien à l'atteinte à la vie privée qui touche à la cybersécurité, ainsi que des objectifs additionnels qui soulignent l'importance des gens, des processus et de la technologie nécessaires pour prendre des décisions. Parmi les OEPC figurent certains autres objectifs qui ne se trouvent pas dans la première version des CPG de la CISA, à savoir, les objectifs liés au nuage et à l'IA. Les OEPC fournissent également un contexte canadien en ce qui a trait aux références et aux mesures recommandées pour tenir compte des avis et des conseils du Centre pour la cybersécurité. Plusieurs des objectifs de la CISA qui donnent lieu à des résultats semblables, comme le « leadership en matière de cybersécurité » et le « leadership en matière des TO », sont combinés et simplifiés dans les OEPC canadiens.

Finalement, la version 1.0 des OEPC ne comprend pas la « divulgation des vulnérabilités ».Le Canada ne dispose pas de règles d'exonération, qui sont pourtant courantes aux États-Unis (Safe Harbour, par exemple), et permet aux chercheuses et chercheurs d'effectuer des tests pour déceler des vulnérabilités sans courir le risque d'être poursuivis en justice. Néanmoins, la divulgation des vulnérabilités est une pratique utile. L'inclusion d'un objectif lié à une divulgation des vulnérabilités sera prise en compte dans les versions ultérieures des OEPC.

Le Centre pour la cybersécurité et la CISA continueront à s'échanger de l'information concernant les objectifs de base de la cybersécurité pour les infrastructures essentielles. Ces efforts assurent l'harmonisation des pratiques tant aux États-Unis qu'au Canada, et ils nous permettent de réviser régulièrement les OEPC et d'établir dans l'avenir des objectifs liés à des secteurs particuliers.

Harmonisation avec les publications et les outils du gouvernement du Canada

Les OEPC fournissent aux propriétaires et exploitants d'infrastructures essentielles canadiennes une série d'objectifs de cybersécurité atteignables afin qu'ils accordent la priorité à des investissements en cybersécurité et renforcent leur posture de cybersécurité.

En s'appuyant sur le travail qui a déjà été accompli par des partenaires et par le Centre pour la cybersécurité, les OEPC apportent une valeur ajoutée en couvrant un éventail plus large de mesures que peuvent prendre les exploitants et propriétaires d'IE. Outre les OEPC, le Centre pour la cybersécurité offre des conseils en matière de sécurité des TI et des outils complémentaires pour soutenir les secteurs des infrastructures essentielles. Ce qui comprend :

- Contrôles de cybersécurité de base pour les petites et moyennes organisations[7]
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)[8]
- La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)[9]

Toutes ces ressources proposent des conseils qui sont conformes aux OEPC. Alors que les OEPC regroupent beaucoup des mesures recommandées tirées de ces autres publications et outils, on remarque un chevauchement marqué entre les OEPC et les autres outils. Plus des deux tiers des contrôles de base et les 10 mesures de sécurité des TI se trouvent dans les OEPC. Des recommandations additionnelles et uniques sont également proposées. Tout comme les contrôles de base, les OEPC se veulent des conseils fondamentaux pouvant être appliqués dans les organisations des infrastructures essentielles, alors que les 10 mesures de sécurité des TI s'appliquent à tous les réseaux connectés à Internet. L'ITSG-33 s'adresse au personnel du GC et il aide les ministères à gérer les considérations liées à la sécurité des TI. Toutes les mesures décrites dans ces ressources sont des lignes directrices facultatives, mais des exigences réglementaires additionnelles pourraient s'appliquer en fonction d'un secteur d'IE donné.

7 https://www.cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations
8 https://www.cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-visant-proteger-les-reseaux-internet-et-0
9 https://www.cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie
La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) fait actuellement l'objet d'une mise à jour. Les changements apportés figureront dans les prochaines versions des OEPC, selon les besoins

UTILISATION DES OEPC

La Boîte à outils des objectifs intersectoriels[10] précise les 36 OEPC. Comme il a été noté, chaque objectif est associé à des références, notamment celles mentionnées à la section précédente, qui donnent plus d'information sur la façon de les mettre en œuvre.

Les OEPC qui se trouvent dans la Boîte à outils des objectifs intersectoriels sont accessibles dans un format clair et structuré afin d'aider votre organisation à comprendre non seulement les objectifs, mais aussi les aspects connexes suivants :

- **RÉSULTAT**
  Le résultat escompté sur le plan de la sécurité que chaque OEPC cherche à atteindre.
- **MESURE RECOMMANDÉE**
  Exemple des mesures que peut prendre une organisation pour tenter d'atteindre l'objectif et le résultat. Ces mesures seront mises à jour à mesure que de nouvelles menaces et défenses sont identifiées.
- **TTP/RISQUES GÉRÉS**
  Un énoncé sur le risque ou, le cas échéant, une référence pertinente aux TTP du cadre MITRE ATT&CK. Lorsqu'une organisation met en œuvre la mesure recommandée, elle peut réduire le risque que des TTP soient exploitées efficacement.
- **RÉFÉRENCE NIST CSF 2.0**
  La sous-catégorie NIST CSF 2.0 qui se rapporte le plus directement à la pratique de sécurité pour chaque objectif.
- **RÉFÉRENCE SUR LES CONSEILS CONNEXES**
  Les conseils du Centre canadien pour la cybersécurité associés à l'objectif et au résultat connexes, pour l'obtention d'information et de ressources supplémentaires.

Les praticiennes et praticiens de la cybersécurité devraient consulter la boîte à outils et mettre en œuvre les mesures recommandées appropriées.

10 https://www.cyber.gc.ca/fr/objectifs-relatifs-letat-preparation-matiere-cybersecurite/boite-outils-objectifs-relatifs-letat-preparation-matiere-cybersecurite-intersectoriels


002
003
004

VISÉE DU PROGRAMME DES OBJECTIFS RELATIFS À L'ÉTAT DE PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ

Les OEPC ne sont que le début des efforts du Centre pour la cybersécurité visant à soutenir l'état de préparation en matière de cybersécurité au sein des infrastructures essentielles. Ces objectifs sont la base du programme des objectifs relatifs à l'état de préparation en matière de cybersécurité et ils seront essentiels au renforcement de la posture de cybersécurité des IE canadiennes.

Dans le cadre du programme, le Centre pour la cybersécurité continuera de prodiguer des conseils destinés aux propriétaires et exploitants d'infrastructures essentielles pour leur permettre d'acquérir des connaissances pour mieux protéger leurs TI et TO contre des cyberincidents.

À l'avenir, le Centre pour la cybersécurité mettra à jour ces OEPC, au besoin, pour s'assurer qu'ils demeurent pertinents et applicables face à des menaces qui évoluent et au contexte législatif en pleine mutation. Les objectifs relatifs à l'état de préparation en matière de cybersécurité intersectoriels seront une ressource de base pour beaucoup propriétaires et exploitants d'infrastructures essentielles au Canada.

Objectifs liés à des secteurs particuliers

Le Centre pour la cybersécurité passera des objectifs relatifs à l'état de préparation en matière de cybersécurité intersectoriels aux objectifs liés à des secteurs particuliers. Grâce à une analyse des technologies et aussi à la cybermaturité propre à chaque secteur, nous serons en mesure de proposer des recommandations adaptées pour le secteur en question. Comme le montre la figure 2, les objectifs liés à des secteurs particuliers tiendront compte de la base intersectorielle. Par exemple, les objectifs liés à des secteurs particuliers qui touchent le secteur de l'énergie offriront une vue personnalisée des objectifs de base qui permet de reconnaître les capacités des exploitants de l'industrie énergétique et du contexte des menaces unique auxquels ils font face. En tenant compte de plusieurs facteurs, le Centre pour la cybersécurité se concentre sur l'élaboration d'objectifs liés à des secteurs particuliers, soit les secteurs de l'énergie, des finances, des télécommunications et des transports.

Cadre relatif à l'état de cyberpréparation

Sous forme d'ensemble, les objectifs intersectoriels et ceux liés à des secteurs particuliers feront partie intégrante du CRF pour renforcer la cybersécurité des IE au Canada. Le cadre CRF englobera tous les objectifs sous forme d'ensemble exhaustif et cohérent de conseils pour soutenir les exigences en matière de cybersécurité. La figure 2 décrit le CRF comme étant un cadre extérieur. Ce document général englobe les objectifs intersectoriels et ceux liés à des secteurs particuliers, avec des conseils appropriés à l'intention des propriétaires et des exploitants des systèmes pour en faire la mise en œuvre.

Figure 2: Cadre relatif à l'état de préparation en matière de cybersécurité pour les infrastructures essentielles canadiennes

PROCHAINES ÉTAPES

Les OEPC constituent une étape essentielle tandis que le Centre pour la cybersécurité continue de s'employer à renforcer la cybersécurité au sein des IE. Le Centre pour la cybersécurité, qui travaille en étroite collaboration avec l'industrie, continuera d'élaborer des objectifs liés à des secteurs particuliers pour certains secteurs d'infrastructures essentielles afin de fournir des conseils adaptés axés sur les besoins uniques de chaque secteur. Les objectifs seront adaptés à mesure qu'évoluent les menaces à l'endroit des infrastructures essentielles du Canada. En outre, le Centre pour la cybersécurité devra s'assurer que ces objectifs demeurent pertinents et applicables. Une rétroaction de la part de l'ensemble des partenaires contribuera à améliorer les OEPC.

Les OEPC et les objectifs liés à des secteurs particuliers, qui s'inscrivent dans le cadre du CRF, aideront les organisations des infrastructures essentielles à continuer de renforcer leur posture de cybersécurité. Le Centre pour la cybersécurité continuera ses travaux d'orientation pour soutenir la mise en œuvre des OEPC dans les IE. L'état de préparation se veut un effort collectif et une priorité partagée. Les OEPC constituent un point de départ pour conduire les IE canadiennes vers une posture de cybersécurité plus résiliente.

Contenu complémentaire

Liste d'abréviations, d'acronymes et de sigles

AMF Authentification multifacteur

CISA Cybersecurity Infrastructure Security Agency

CPG Objectifs de rendement en matière de cybersécurité intersectoriels (Cross-Sector Cybersecurity Performance Goals)

CSF Cadre de cybersécurité (Cybersecurity Framework)

GC Gouvernement du Canada

IA Intelligence artificielle

IE Infrastructures essentielles

NIST National Institute of Standards and Technology

OEPC Objectifs relatifs à l'état de préparation en matière de cybersécurité

SAW Poste de travail administratif sécurisé (Secure Administrator Workstation)

SCI Système de contrôle industriel

TI Technologies de l'information

TO Technologie opérationnelle

TTP Tactiques, techniques et procédures

Glossaire

Authentification multifacteur
Mécanisme pouvant ajouter une couche supplémentaire de sécurité aux appareils et aux comptes. L'authentification multifacteur (AMF) 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'AMF.

Chiffrement
Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.

Compromission
Divulgation intentionnelle ou non intentionnelle d'information mettant en péril sa confidentialité, son intégrité ou sa disponibilité.

Cyberattaque
Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à infiltrer un système informatique, un réseau ou un dispositif.

Cyberincident
Toute tentative non autorisée, réussie ou non, d'avoir accès à une ressource informatique ou à un réseau, de le modifier, de le détruire, de le supprimer ou de le rendre inutilisable.

Cybermenace
Situation où une auteure ou un auteur de menace, utilisant Internet, profite d'une vulnérabilité connue dans un produit dans le but d'exploiter un réseau et les informations sur ce réseau.

Cybersécurité
Protection de l'information numérique et de l'intégrité de l'infrastructure qui héberge et transmet cette information. Concrètement, la cybersécurité comprend l'ensemble des technologies, des processus, des pratiques et des mesures d'intervention et d'atténuation conçu pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés pour ainsi assurer la confidentialité, l'intégrité et la disponibilité.

Détection
Surveillance et analyse des événements d'un système en vue de relever les tentatives d'accès non autorisées aux ressources du système.

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).

Infrastructures essentielles
Ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services essentiels à la santé, à la sécurité ou au bien-être économique des Canadiennes et Canadiens ainsi qu'au fonctionnement efficace du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontières du pays. La perturbation des infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public.

Intelligence artificielle
Un sous-champ de l'informatique qui développe des programmes informatiques intelligents capables de donner l'impression d'une intelligence humaine (p. ex. résoudre des problèmes, tirer des leçons, comprendre une langue, interpréter des scènes visuelles).

Logiciels antivirus
Logiciels qui protègent contre les virus, les chevaux de Troie, les vers et les espiogiciels. Les logiciels antivirus ont recours à un analyseur pour détecter les programmes qui pourraient être malveillants. Les analyseurs peuvent détecter les virus connus, des virus inconnus auparavant et des fichiers suspects.

Maliciels
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.

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.

Rançongiciels
Type de maliciel qui empêche une utilisatrice ou un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'il ait payé une rançon.

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 en vue de compromettre les biens ou les activités d'une organisation.

Références

1 Centre canadien pour la cybersécurité, Évaluation des menaces de base : Cybercriminalité (https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite), 28 août 2023.

2 Affaires mondiales Canada. Déclaration sur les cyberactivités malveillantes de la Russie qui touchent l'Europe et l'Ukraine, (https://www.canada.ca/fr/affaires-mondiales/nouvelles/2022/05/declaration-sur-les-cyberactivites-malveillantes-de-la-russie-qui-touchent-leurope-et-lukraine.html) 10 mai 2022.

3 Centre de la sécurité des télécommunications, Since Russia's brazen and unjustifiable invasion of Ukraine, CSE continues to observe numerous Russia-backed #disinformation campaigns online, (https://x.com/cse_cst/status/1514246874890395654?s=20) X (Twitter), 13 avril 2022.

4 Cybersecurity and Infrastructure Security Agency, People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection, (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a) 24 mai 2023..

5 Cybersecurity and Infrastructure Security Agency, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a) 7 février 2024.

6 Lionel Sujay Vailshery. Industrial IoT – market size worldwide 2020-2030, Statista, (https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/#statisticContainer) 13 février 2024.

7 Dee-ann Durbin. Meat company JBS Foods confirms it paid U.S.$11M ransom in cyberattack, Global News, (https://globalnews.ca/news/7936930/jbs-foods-ransomware-attack-paid/) 9 juin 2021.

8 Christina Wilkie. Colonial Pipeline paid $5 million ransomware one day after cyberattack, CEO tells Senate, CNBC, (https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html) 9 juin 2021.

9 Gouvernement de Terre-Neuve-et-Labrador. Cyberattack on the Newfoundland and Labrador Heath Care System, (https://www.gov.nl.ca/hcs/files/OVERVIEW-NL-Health-Cyber-Incident-March-2023.pdf) mars 2023.

10 Rob Antle. N.L. says Hive ransomware group was behind 2021 cyberattack on health systems, (https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyberattack-hive-ransomware-group-1.6778579) CBC News. 14 mars 2023.

11 L'hôpital pour enfants malades (SickKids), SickKids lifts Code Grey with 80 per cent of priority systems restored, (https://www.sickkids.ca/en/news/archive/2023/sickkids-lifts-code-grey-with-80-per-cent-of-priority-systems-restored/) 5 janvier 2023.

12 Jonathan Greig. Canadian banking tech giant Moneris says it prevented ransomware attack, (https://therecord.media/moneris-canada-ransomware-attack-prevented) The Record from Recorded Future News. 13 novembre 2023.

13 Sécurité publique Canada. Stratégie de cybersécurité du Canada Renforcer le Canada et accroître sa prospérité, (https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-fra.pdf) 2010.

14 Sécurité publique Canada. Stratégie nationale de cybersécurité Vision du Canada pour la sécurité et la prospérité dans l'ère numérique, (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-fr.pdf) 2018.

Annex A : Différences entre les OEPC et les CPG

Nouveau pilier et nouveaux objectifs

- **Pilier gouvernance**
  - **Type** : Pilier
  - **Justification** : Un nouveau pilier appelé « gouvernance » a été ajouté aux cinq piliers existants pour refléter les nouveaux conseils du NIST CSF 2.0. Le pilier gouvernance permet aux organisations de mettre l'emphase sur l'importance de la gouvernance en matière de cybersécurité. Le nouveau pilier amène les organisations à se concentrer sur les processus, les gens et la technologie nécessaires pour réussir la mise en œuvre de pratiques de cybersécurité.
- **Leadership en matière de respect de la vie privée**
  - **Type** : Objectif **Pilier** : Gouvernance
  - **Justification** : Sous le nouveau pilier « gouvernance », les OEPC ont ajouté un objectif de leadership en matière de respect de la vie privée que les organisations doivent atteindre. Des atteintes à la protection de renseignements personnels sont de plus en plus courantes au sein des secteurs des infrastructures essentielles aux prises avec un cyberincident. En déployant les équipes et les procédures appropriées, il est possible d'empêcher et d'atténuer ces atteintes. De plus, des contrôles en lien à l'atteinte à la vie privée touchant la cybersécurité ont été ajoutés au NIST CSF 2.0.
- **Sélection d'un fournisseur de services infonuagiques (FSI) de confiance**
  - **Type** : Objectif **Pilier** : Identification
  - **Justification** : Un FSI de confiance possédant des compétences sur le plan technique est essentiel pour permettre aux organisations d'adopter en toute confiance des technologies de services infonuagiques.
- **Poste de travail administratif sécurisé (SAW pour Secure Administrator Workstation)**
  - **Type** : Objectif **Pilier** : Protection
  - **Justification** : Un SAW est un poste de travail sécurisé dédié aux tâches sensibles qu'exécutent les administratrices et administrateurs. Il permet de séparer les tâches et les comptes sensibles pour empêcher une utilisation à des fins non administratives et ainsi protéger le réseau d'une organisation contre les risques liés à la cybersécurité, comme les risques associés à des maliciels, de l'hameçonnage et des attaques de type « Pass-the-Hash ».

Objectifs changés

- **Leadership en matière de cybersécurité organisationnel et des TO**
  - **Type** : Objectif **Pilier** : Gouvernance
  - **Justification** : Combine leadership pour la cybersécurité et rôle-titre des TO.
- **Processus et politiques de signalement des incidents liés à la chaîne d'approvisionnement**
  - **Type** : Objectif **Pilier** : Gouvernance
  - **Justification** : Ajoute des processus et des politiques lorsqu'il est question de l'objectif de signalement des incidents liés à la chaîne d'approvisionnement. Met de l'avant le programme de gestion des risques liés à la chaîne d'approvisionnement de l'organisation pour exiger que les fournisseurs signalent aux clientes et clients tout incident.
- **Répertoire des biens et topologie de réseau**
  - **Type** : Objectif **Pilier** : Identification
  - **Justification** : Le répertoire des biens comprend maintenant un composant infonuagique pour assurer, le cas échéant, qu'une organisation documente tous les biens en lien à l'écosystème infonuagique.
- **Formation relative à la formation en matière de cybersécurité de base et des TO**
  - **Type** : Objectif **Pilier** : Protection
  - **Justification** : Combine la formation en cybersécurité et la formation liée aux TO dans un seul objectif et intègre les concepts de protection de la vie privée et les atteintes à la vie privée dans le cadre de la formation pour mieux sensibiliser aux incidents concernant l'atteinte à la vie privée.
- **Stockage des journaux sécurisé et central**
  - **Type** : Objectif **Pilier** : Protection
  - **Justification** : Les organisations doivent veiller à ce que le stockage des journaux se fasse dans un espace de stockage sécurisé et centralisé.

Objectifs retirés

- **Divulgation des vulnérabilités**
  - **Type** : Objectif **Pilier** : Réponse
  - **Justification** : Le Canada ne dispose pas de règles d'exonération, qui sont pourtant courantes aux États-Unis (Safe Harbour, par exemple), et permet aux chercheuses et chercheurs d'effectuer des tests pour déceler des vulnérabilités sans courir le risque d'être poursuivis en justice. L'inclusion d'un objectif lié à une divulgation des vulnérabilités sera prise en compte dans les versions ultérieures des OEPC.

Notes