Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Lignes directrices sur le signalement des cyberincidents : Principales exigences liées à l'échange

Série Gestionnaires

TLP:CLEAR

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, 2026

Canada

Avant-propos

La présente est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal, 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 :

- contact@cyber.gc.ca
- 613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 29 janvier 2026.

Historique des révisions

Révision	Modifications	Date
1	Première version	29 janvier 2026

ISBN 978-0-660-79993-3
CAT D96-135/2025F-PDF

Vue d'ensemble

L'organisation et l'échange d'information pendant un cyberincident nécessitent une approche structurée permettant d'assurer la communication efficace des détails pertinents au Centre canadien pour la cybersécurité (Centre pour la cybersécurité). La présente publication vise à clarifier les types d'information que le Centre pour la cybersécurité considère comme « exploitables ».

Table des matières

Liste des tableaux

Liste des annexes

1 Introduction

Pour les entités participantes, cette publication est destinée à être transmise à l'interne à l'équipe de direction aux fins de consultation et de préapprobation, ce qui comprend les parties prenantes des équipes juridiques et opérationnelles. Vous devriez également partager cette publication avec les fournisseurs de services de sécurité gérés et assurer le soutien interorganisationnel en ce qui a trait à l'approche et à la préapprobation des types d'information à communiquer.

Avant qu'un incident se produise, votre organisation devrait décider si elle peut et compte communiquer ces types d'information pour :

- mieux orienter les prochaines étapes,
- faciliter les activités de reconstruction ou de rétablissement du réseau,
- accroître la résilience de l'écosystème global de la cybersécurité. Pour obtenir plus de détails, veuillez consulter l'Annexe A : Avant les cyberincidents.

En outre, l'échange d'information sert de ressource centralisée visant à recueillir des données sur les cybermenaces et les vulnérabilités. Nous recommandons à votre organisation de diffuser l'information entre les membres de votre secteur. L'objectif est de se concerter pour sécuriser les infrastructures essentielles (IE) et assurer une protection contre les cybermenaces. Les aspects recommandés de l'échange d'information intracommunautaire sont décrits à l'Annexe B : Recommandations concernant l'échange d'information.

2 Échange d'information durant un cyberincident

Durant un incident de cybersécurité, l'entité participante pourrait communiquer au Centre pour la cybersécurité des artéfacts qui serviraient à appuyer l'enquête sur l'incident et à mieux comprendre la nature de la compromission. Cela comprend de l'information contextuelle et des artéfacts techniques.

2.1 Information contextuelle

Cette catégorie comprend des preuves permettant de mettre en contexte l'incident pour ainsi aider votre organisation à mieux comprendre les circonstances et les implications de la compromission. L'information contextuelle inclut généralement des anomalies dans les activités des utilisatrices et utilisateurs, des communications (par exemple, un courriel) et du contenu. Cette information aide à produire un rapport détaillé, à éclairer l'attribution et à valider le comportement malveillant.

Cela peut comprendre l'information suivante :

- un résumé de l'activité et de l'incident observés;
- toute information fournissant des précisions sur la nature de la menace (si elle est connue), par exemple
    - le maliciel ou le déni de service
    - l'auteur impliqué
    - la motivation
    - le vecteur et l'incidence de la menace
- la méthode employée par l'attaquante ou attaquant pour obtenir l'accès, comme l'hameçonnage, l'exploitation de vulnérabilités ou d'autres méthodes;
- la chronologie des événements avant, pendant et après l'incident;
- la portée de l'incident, y compris les types de systèmes touchés et les données qui ont été compromises, notamment
    - les opérations touchées
    - les perturbations qui ont résulté de cette compromission, notamment en ce qui touche les logiciels tiers
- les détails observés sur le trafic du réseau (si disponible);
- la liste des mesures d'atténuation prises, le cas échéant, par les responsables du traitement des incidents;
- l'état actuel de l'incident;
- la liste des indicateurs de compromission (IC) recueillis durant l'enquête;
- les prochaines étapes;
- les coordonnées.

2.2 Artéfacts techniques

Cette catégorie comprend toutes les données liées aux aspects techniques de l'incident.

Le Tableau 1 : Artéfacts de données et d'information exploitables requis décrit les types d'artéfacts de données et d'information exploitables que le Centre pour la cybersécurité demande aux entités participantes de fournir en cas d'incident de cybersécurité. De plus, le tableau met en évidence le processus analytique auquel fait appel le Centre pour la cybersécurité pour analyser les artéfacts et les résultats escomptés de l'analyse.

Il est important de noter les aspects suivants :

- Les adresses IP et les domaines fournis comme indicateurs de compromission sont présumés ne pas appartenir à l'organisation, et les artéfacts communiqués au Centre pour la cybersécurité ne comportent pas d'information relative aux citoyennes et citoyens du Canada ou aux personnes se trouvant au Canada.
- En aucun cas le Centre pour la cybersécurité n'acheminera à des entités externes des données brutes ou nominatives.
    - Le Centre pour la cybersécurité est lié par les dispositions de la *Loi sur le Centre de la sécurité des télécommunications* [1] et la *Loi sur la protection des renseignements personnels* [2] qui régissent ses activités. Le CST peut également conclure des accords de non-divulgation (AND) avec des partenaires en matière d'infrastructures essentielles pour protéger les renseignements confidentiels lors des activités d'échange d'information.

Table 1: Artéfacts de données et d'information exploitables requis

Artéfacts techniques	Processus d'analyse interne	Résultats escomptés
Adresses IP suspectes ou malveillantes	• Comparer les adresses IP malveillantes à la base de connaissances du Centre pour la cybersécurité pour les valider et fournir des renseignements connexes, y compris, sans s'y limiter, les indicateurs classifiés	• Confirmer le caractère malveillant • Communiquer l'information à l'entité participante et à la collectivité des infrastructures essentielles pour la prise de mesures • Communiquer les indicateurs supplémentaires le cas échéant
Domaines suspects ou malveillants	• Comparer les domaines malveillants à la base de connaissances du Centre pour la cybersécurité, y compris, sans s'y limiter, les indicateurs classifiés, pour les valider et établir l'infrastructure de commande et contrôle (C2) • Analyser le comportement (tendance en matière de redirection, requêtes système d'adressage par domaines [DNS pour *Domain Nam System*] pour obtenir des renseignements sur les types de maliciels distribués dans le cadre de campagnes d'hameçonnage et l'étendue géographique de la menace	• Confirmer le caractère malveillant • Communiquer l'information à l'entité participante et à la collectivité des infrastructures essentielles pour la prise de mesures • Communiquer les indicateurs supplémentaires le cas échéant
Codes de hachage de fichiers suspects ou malveillants	• Comparer les codes de hachage de fichiers malveillants à la base de connaissances du Centre pour la cybersécurité, y compris, sans	• Confirmer le caractère malveillant

Artéfacts techniques	Processus d'analyse interne	Résultats escomptés
	s'y limiter, les indicateurs classifiés, pour les valider et déterminer la source, le comportement et les risques connexes • Comparer les codes de hachage des fichiers à ceux de maliciels connus aux fins de détection et d'identification	• Communiquer l'information à l'entité participante et à la collectivité des infrastructures essentielles pour la prise de mesures • Communiquer les indicateurs supplémentaires le cas échéant
Adresses URL suspectes ou malveillantes	• Comparer les adresses URL malveillantes à la base de connaissances du Centre pour la cybersécurité, y compris, sans s'y limiter, les indicateurs classifiés, pour les valider et comprendre les méthodes d'hébergement et de distribution des maliciels	• Confirmer le caractère malveillant • Communiquer l'information à l'entité participante et à la collectivité des infrastructures essentielles pour la prise de mesures • Communiquer les indicateurs supplémentaires le cas échéant
Documents et fichiers suspects ou malveillants (échantillons de maliciel)	• Exécuter des méthodes de détection heuristiques pour évaluer le degré de malveillance • Les comparer pour révéler les tactiques, les techniques et les procédures (TTP), comme les types de maliciels utilisés, leurs fonctionnalités et les moyens employés pour éviter la détection	• Confirmer le caractère malveillant • Révéler les tendances, tactiques, techniques et comportements • Communiquer le code de hachage des documents et fichiers malveillants • Communiquer avec l'entité participante et la collectivité des infrastructures essentielles pour la prise de mesures afin de mettre à jour les signatures des antivirus et renforcer les stratégies de sécurité
Journaux de sécurité (journaux d'événements, journaux de systèmes, journaux d'accès, journaux de systèmes de détection d'intrusion [SDI] et de systèmes de prévention d'intrusion [SPI], journaux réseau et de coupe-feu, journaux de détection et intervention sur les terminaux [EDR pour *Endpoint Detection and Response*], journaux DNS et de réseau virtuel privé, journaux de base de données et de serveurs de courrier, etc.)	• Analyser et appliquer des cas d'utilisation ou des analyses qui complètent les outils commerciaux et détectent les signes d'activités suspectes ou malveillantes	• Révéler les tendances, tactiques, techniques et comportements • Révéler les artéfacts malveillants (adresses IP, domaines, codes de hachage, adresses URL, etc.) • Communiquer l'information à l'entité participante et à la collectivité des infrastructures essentielles pour la prise de mesures
Artéfacts de criminalistique numérique : images disque,	• Exécuter une analyse criminalistique pour trouver des preuves de compromission et reconstruire la chronologie des événements,	• Révéler les tendances, tactiques, techniques et comportements

Artéfacts techniques	Processus d'analyse interne	Résultats escomptés
images mémoire, entrées de registre, lecteurs système, etc.	pour déterminer l'étendue de l'accès et de l'exfiltration, les méthodes employées pour obtenir l'accès et l'identité de l'auteur de menace	• Révéler les artéfacts malveillants (adresses IP, domaines, codes de hachage, adresses URL, etc.) • Communiquer l'information à l'entité participante et à la collectivité des infrastructures essentielles pour la prise de mesures

Annex A Avant les cyberincidents

Avant toute confirmation qu'un cyberincident s'est produit, l'organisation participante est invitée à communiquer l'information présentée dans les sous-sections suivantes de cette annexe au Centre pour la cybersécurité. Cette information peut permettre

- de déterminer les lacunes
- de calibrer l'efficacité de la détection
- d'augmenter le rapport signal sur bruit
- de réduire les faux positifs pour minimiser la désensibilisation aux alertes

Votre organisation devrait également communiquer toute autre information pouvant servir à retracer une série d'événements.

A.1.1 Règles d'alerte

Des ensembles de critères et de configurations qui sont dans le système de surveillance de la sécurité d'une organisation, comme un système de gestion des informations et des événements de sécurité (GIES) ou un SDI, utilisé pour déclencher des alertes lors d'incidents de sécurité potentiels. Cet ensemble comprend les déclencheurs, leurs seuils, filtres et règles de corrélation telles que

- l'atteinte du nombre maximal de tentatives d'ouverture de session
- des irrégularités géographiques
- du trafic sortant inhabituel
- des changements dans l'intégrité des fichiers

L'organisation pourrait opter pour la mise en œuvre d'un système de détection et intervention sur les terminaux (EDR pour *Endpoint Detection and Response*) ou de détection et d'intervention avancées (XDR pour *Extended Detection and Response*) afin d'aider à la détection et à l'intervention dans le cadre d'une activité anormale du système.

A.1.2 Journaux de sécurité

Enregistrements numériques d'activités et d'événements liés à la sécurité des TI qui se produisent notamment sur :

- des dispositifs réseau (par exemple, coupe-feu, routeurs et commutateurs)
- des serveurs et des postes de travail, des appliances de sécurité (par exemple, SDI, SPI et logiciels antivirus)
- des applications (par exemple, journaux de bases de données et de serveurs Web)

Annex B Recommandations concernant l'échange d'information

Cette annexe comprend les pratiques exemplaires recommandées en matière d'échange d'information. En échangeant divers types d'information, les membres de la collectivité du secteur des infrastructures essentielles peuvent améliorer considérablement leur posture de cybersécurité collective, réduire le risque de cyberattaques et réagir plus efficacement aux incidents.

B.1.1 Rapports de renseignement sur les menaces

Les rapports de renseignement sur les menaces offrent des analyses détaillées de menaces précises, y compris les TTP employées par les adversaires dans le cyberespace. Ces rapports peuvent donner un aperçu

- de la nature de la menace
- des systèmes touchés
- des stratégies d'atténuation
- des mesures de protection recommandées

B.1.2 Indicateurs de compromission

Les indicateurs de compromission sont des artéfacts ou des éléments d'information précis utilisés pour détecter les cybermenaces, comme

- les adresses IP malveillantes
- les localisateurs de ressources uniformes (adresses URL)
- les codes de hachage de fichiers
- les signatures de courriels

La communication des indicateurs de compromission aide les membres à repérer les menaces et à y intervenir rapidement.

B.1.3 Pratiques exemplaires et recommandations en matière de sécurité

Information sur les pratiques, politiques et mesures de sécurité efficaces que les organisations peuvent mettre en œuvre pour se protéger contre les cybermenaces. Elle comprend les lignes directrices pour la configuration, les contrôles de sécurité et les stratégies de prévention.

B.1.4 Information sur les vulnérabilités et les correctifs

Communication de détails sur les nouvelles vulnérabilités découvertes, les répercussions possibles et les correctifs ou mesures de contournement offerts. Ces détails aident les organisations à corriger les vulnérabilités rapidement avant que les auteurs de menace puissent les exploiter.

B.1.5 Signalement des incidents

Sommaires des incidents de sécurité subis par les membres, y compris la nature des incidents, leur détection, les mesures prises et les leçons retenues. La communication des rapports d'incident peut aider les autres membres à mieux se préparer et intervenir à des incidents similaires.

B.1.6 Mécanismes de communication anonyme

Il est possible que des membres préfèrent communiquer de l'information sensible de façon anonyme pour protéger leur confidentialité ou pour des raisons juridiques. L'organisation devrait envisager l'adoption de mécanismes de communication anonyme permettant ainsi d'assurer la diffusion d'information précieuse sans exposer la source.

B.1.7 Plateformes d'échanges automatisés de renseignement sur les menaces

Il est recommandé d'utiliser des plateformes comme STIX (pour *Structured Threat Information eXpression*) et TAXII (pour *Trusted Automated Exchange of Indicator Information*) pour l'échange automatisé de renseignement sur les menaces. Ces plateformes facilitent la diffusion en temps réel de données sur les menaces dans un format standardisé et permettent ainsi de détecter et d'atténuer les menaces plus rapidement.

B.1.8 Collaboration en matière de recherche et d'analyse

Efforts conjoints visant à analyser des cybermenaces ou des tendances précises, mettant à profit l'expertise et les ressources collectives des membres du secteur de l'énergie. Cette approche de collaboration peut mener à une compréhension approfondie des menaces complexes et à des contre-mesures plus efficaces.