Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR
CYBER SECURITY

Cyber incident reporting guidelines: Key information sharing requirements

Management

TLP:CLEAR

Canada

Foreword

This is an UNCLASSIFIED publication issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre). For more information, please email or phone our Contact Centre:

- contact@cyber.gc.ca
- (613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on January 29, 2026.

Revision history

Revision	Amendments	Date
1	First release	January 29, 2026

D96-135/2025E-PDF
ISBN 978-0-660-79992-6

Overview

Organizing and sharing information during a cyber incident involves a structured approach that ensures the effective communication of relevant details to the Canadian Centre for Cyber Security (Cyber Centre). The purpose of this publication is to clarify the types of information the Cyber Centre considers “actionable.”

Table of contents

List of tables

List of annexes

1 Introduction

For participating entities, this publication should be shared and circulated internally for consultation and pre-approval from your executive team, including legal and operational teams. You should also share this publication with managed security service providers and ensure cross-organizational support for the approach and pre-approval of the type of information to be shared.

In advance of a cyber incident, your organization should decide whether you can and will share these types of information to:

- best inform next steps
- assist in network rebuild and recovery
- benefit the resilience of the broader cyber ecosystem. For more details, please read Annex A: Pre-cyber incidents.

In addition, information sharing serves as a centralized resource for gathering data on cyber threats and vulnerabilities. We recommend that your organization disseminate information amongst the members of your sector. The goal is to enable collaborative efforts to secure critical infrastructure (CI) and protect against cyber threats. The recommended aspects of intra-community information sharing are described in Annex B: Recommended information sharing.

2 Information sharing during a cyber incident

During a cyber security incident, the participating entity could disclose artifacts to the Cyber Centre that would be used to investigate and provide clarity and enrichment to the nature of the compromise. This includes contextual information and technical artifacts.

2.1 Contextual information

This category includes evidence that provides context to the incident, which assists your organization in understanding the circumstances and implications of the compromise. Contextual information typically consists of user activity anomalies, communications (for example, email) and content. This information helps to provide comprehensive reporting, inform on attribution, and validate the malicious behavior.

This might include the following information:

- summary of the observed activity or incident
- information that would provide clarity regarding the form of threat (if known), such as the
    - malware or denial of service
    - actor involved
    - motivation
    - vector and impact
- how the attacker gained access (whether through phishing, exploiting vulnerabilities or other means)
- timeline of events leading up to, during and after the incident
- scope of the incident, including the type of systems affected and the data that was compromised, including
    - what operations are impacted
    - what disruptions have resulted from this compromise, including to third-party software
- observed network traffic details (if available)
- list of mitigations taken, if any, by the incident handlers
- current status of the incident
- list of indicators of compromise (IOCs) gathered during the investigation
- next steps to be taken
- contact information

2.2 Technical artifacts

This category includes all data related to the technical aspects of the incident.

Table 1: Required actionable information and data artifacts details the specific types of actionable information and data artifacts that the Cyber Centre requires from your organization in the event of a cyber security incident. Additionally, the table highlights the analytical process the Cyber Centre takes to analyze the artifacts and the expected outcomes that stem from the analysis.

It is important to note that:

- Internet Protocol (IP) addresses and domains supplied as IOCs are presumed not to be owned by the organization, and that the artifacts shared with the Cyber Centre do not contain any information pertaining to Canadian individuals or persons located in Canada.
- At no time will the Cyber Centre share raw or identifying victim data with any external entity
    - The Cyber Centre is bound by provisions in the *Communications Security Establishment Act* [1] and the *Privacy Act* [2] that govern our activities. CSE may also establish non-disclosure agreements (NDA) with critical infrastructure partners to protect confidential information during information sharing activities.

Table 1: Required actionable information and data artifacts

Technical artifacts	Internal analytics process	Expected outcomes
Suspicious/malicious IPs	• Cross-reference malicious IP with the Cyber Centre's knowledge base to validate and provide insights, including but not limited to classified indicators	• Confirm maliciousness • Share with participating entity and the CI community for action • Share any additional indicators when applicable
Suspicious/malicious domains	• Cross-reference malicious domains with the Cyber Centre's knowledge base including but not limited to classified indicators to validate and identify command and control (C2) infrastructure • Analyze the behaviour (redirection pattern, domain name system (DNS) queries) to gain insights into the types of malware being distributed through the phishing campaigns and the geographical spread of the threat	• Confirm maliciousness • Share with participating entity and the CI community for action • Share any additional indicators when applicable
Suspicious/malicious file hashes	• Cross-reference malicious file hashes with the Cyber Centre's knowledge base including but not limited to classified indicators to validate and gather the source, behaviour and associated risks • Compare the hashes of files with those of known malware for detection and identification	• Confirm maliciousness • Share with participating entity and the CI community for action • Share any additional indicators when applicable
Suspicious/malicious URLs	• Cross-reference malicious URLs with the Cyber Centre's knowledge base including but not limited to Classified indicators to validate and understand the methods used to host and distribute malware	• Confirm maliciousness • Share with participating entity and the CI community for action • Share any additional indicators when applicable

Technical artifacts	Internal analytics process	Expected outcomes
Suspicious/malicious documents and files (malware samples)	• Run detection heuristics to evaluate the level of maliciousness • Cross reference to reveal tactic, techniques, and procedures (TTPs), such as the type of malware used, its motives, or its functionality and how it evades detection	• Confirm maliciousness • Reveal patterns, tactics, techniques and behaviours • Share hash value of malicious documents and files • Share with participating entity and the CI community for action, to update antivirus signatures, and to refine security policies
Security logs (event logs, system logs, access logs, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) logs, network and firewall logs, endpoint detection and response (EDR) logs, DNS and virtual private network logs, database logs and mail server logs, etc.)	• Analyze and apply use case and analytics that complement the commercial tooling and detect evidence of suspicious/malicious activities	• Reveal patterns, tactics, techniques, and behaviours. • Reveal malicious artifacts (IPs, domains, hashes, URLs, etc.) • Share with participating entity and the CI community for action
Forensic artifacts: Disk images, memory dumps, registry entries, system drives, etc.	• Conduct forensic analysis to find evidence of compromise and reconstruct the timeline of events, to determine the extent of the access and exfiltration, the methods used to gain access and identity of the threat actor	• Reveal patterns, tactics, techniques, and behaviours • Reveal malicious artifacts (IPs, domains, hashes, URLs, etc.) • Share with participating entity and the CI community for action

Annex A Pre-cyber incident

Before any confirmation that a cyber incident has occurred, the participant organization is encouraged to share the information presented in the following sub-sections of this annex with the Cyber Centre. This information can:

- identify gaps
- calibrate the efficiency of the detection
- increase the signal-to-noise ratio
- lower false positives to avoid alert fatigue

Your organization should also share any other information that can be used to retrace a series of events.

A.1.1 Alert rules

Configuration and criteria are set within the organization's security monitoring system, such as a security information and event management (SIEM) system or an IDS, used to trigger alerts for potential security incidents. This includes the triggers, their thresholds, filters and correlation rules, such as:

- excessive login failures
- geographical irregularities
- unusual outbound traffic
- changes in file integrity.

Consider implementing endpoint detection and response (EDR) or extended detection and response (XDR) system to assist in detecting and responding to anomalous system activity.

A.1.2 Security logs

Digital records that capture activities and events related to IT security, such as:

- network devices (for example, firewalls, routers, and switches)
- servers and workstations, security appliances (for example, IDS, IPS, and antivirus software)
- applications (for example, database and web server logs).

Annex B Recommended information sharing

This annex includes the recommended information sharing best practices. By sharing various types of information, critical infrastructure community members can significantly enhance their collective cyber security posture, reduce the risk of cyber attacks, and respond more effectively to incidents.

B.1.1 Threat intelligence reports

Threat intelligence reports offer detailed analyses of specific threats, including the TTPs used by cyber adversaries. These reports can provide insights into the

- nature of the threat
- affected systems
- mitigation strategies
- recommended protective measures

B.1.2 Indicators of compromise

IoCs are specific artifacts or pieces of information used to detect cyber threats, such as:

- malicious IP addresses
- uniform resource locators (URL's)
- file hashes
- email signatures

Sharing IoCs helps members to quickly identify and respond to potential threats.

B.1.3 Best practices and security recommendations

Information on effective security measures, policies, and practices that organizations can implement to protect themselves from cyber threats. This includes configuration guidelines, security controls, and preventive strategies.

B.1.4 Vulnerability information and patches

Sharing details about newly discovered vulnerabilities, potential impacts, and available patches or workarounds. This helps organizations to address vulnerabilities promptly before they can be exploited by threat actors.

B.1.5 Incident reports

Summaries of security incidents experienced by members, including the nature of the incident, how it was detected, the actions taken, and lessons learned. Sharing incident reports can help others to better prepare for and respond to similar incidents.

B.1.6 Anonymous sharing mechanisms

Some members may prefer to share sensitive information anonymously to protect their privacy or for legal reasons. Consider providing mechanisms for anonymous sharing, ensuring that valuable information can still be disseminated without exposing the source.

B.1.7 Automated threat intelligence sharing platforms

Utilizing platforms like structured threat information expression (STIX) and trusted automated exchange of indicator information (TAXII) for the automated exchange of threat intelligence. These platforms facilitate real-time sharing of threat data in a standardized format, enabling faster detection and mitigation of threats.

B.1.8 Collaborative analysis and research

Joint efforts to analyze specific cyber threats or trends, leveraging the collective expertise and resources of the energy sector members. This collaborative approach can lead to a deeper understanding of complex threats and more effective countermeasures.