CANADIAN CENTRE FOR
CYBER SECURITY

National Water and Wastewater Conference 2022

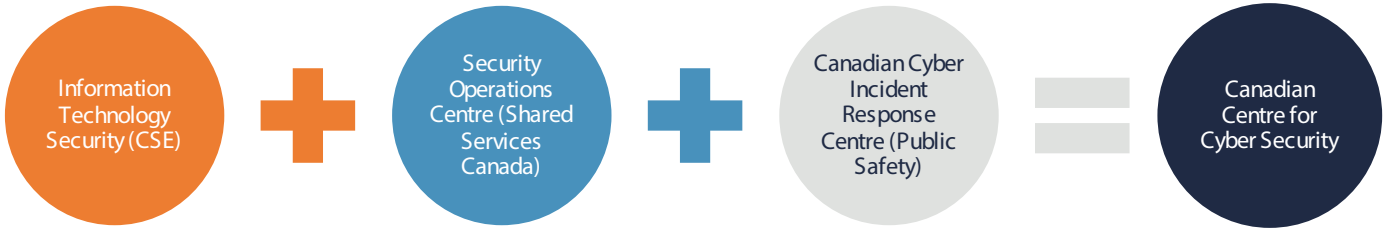
Lindsay MacDonald
Cyber Centre Partnerships

THE CANADIAN CENTER FOR CYBER SECURITY (CYBER CENTER)

- Business line of the Communications Security Establishment, a Federal Agency
- Located in Ottawa, Ontario
- Created in 2018

The Cyber Centre provides expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public.

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ



CYBER CENTRE MANDATE

National Defence Act (NDA)

CSE could provide advice, guidance and services to protect information infrastructures of importance to the GC.

CSE Act

CSE is now authorized to provide more robust cyber defense services by deploying its cyber defence tools to critical non-Government networks designated as being of importance to Canada.

CCCS PARTNER ENGAGEMENT

CANDIAN CITIZENS
Citizens

SMOs
Small Organizations | Medium Organizations

WATER
Generic | Potable Water Provider (Drinking Water) | Sanitation & Wastewater Management

FOOD
Agriculture Supply Chain | Agriculture/Farms & Producers | Food Distribution & Grocery | Food Processing | Food Safety | Generic

SAFETY
Emergency Management& Response | Fire | Generic | Hazardous Materials | Law Enforcement | Paramedic & Ambulatory Services | Security & Intel

MANUFACTURING
Defence Industrial Base | Other Manufacturing | Production of Goods

FEDERAL GOVERNMENT
Crown Corporations & Other Institutions | Departments | Federal Courts | Parliamentary Entities

DEMOCRATIC INSTITUTIONS
Electoral Bodies | Political Parties

INNOVATION
Academic partner | Private organizations | Not-for-profit organizations | Government-based organizations | Groups

ACADEMIA
Universities | Colleges | Polytechnics | Other academic institutions | Service Providers | Associations | Government of Canada Partners

ICT
Telcos & Internet Service Providers | Generic | Managed Service Providers / Managed Security Service Providers | Cloud Service Provider | Hardware / Software vendors | Social Media | Cyber Security Vendors

ENERGY
Electricity | Mining | Nuclear | Oil | Gas

FINANCE
Banks | Credit Unions | Generic | Insurance | Payment Infrastructure | Finance and Leasing | Pension Funds | Investments

GOVERNMENT
Indigenous | Municipal | Provincial | Territorial

TRANSPORT
Air | Marine | Municipal Transit | Rail | Road

HEALTH
Health Associations and COE | Patient Care | Bio/Pharmaceutical Organizations | Academic Research Institutes | Regional Health Authorities | Medical Device Manufacturers | Government of Canada Partners

FEDERAL GOVERNMENT PARTNERS

ROYAL CANADIAN MOUNTED POLICE (RCMP)

The RCMP works to prevent crime, enforce the law, investigate offences, keep Canadians, and their interests, safe and secure, and assist Canadians in emergency situations/incidents. It operates within three main areas of responsibility:

CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)

CSIS is at the forefront of Canada's national security system with a role to investigate activities suspected of constituting threats to the security of Canada and to report on these to the Government of Canada.

PUBLIC SAFETY (PS)

PS Canada ensures coordination across all federal departments and agencies responsible for national security and the safety of Canadians. The mandate is to keep Canadians safe from a range of risks such as natural disasters, crime, and terrorism with a mission to build a safe and resilient Canada.

INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT CANADA (ISED)

ISED works with Canadians in all areas of the economy and in all parts of the country to improve conditions for investment, enhance Canada's innovation performance, increase Canada's share of global trade and build a fair, efficient and competitive marketplace.

*Information provided for each organization comes from their respective web sites.

THE CANADIAN CYBER THREAT LANDSCAPE

EVOLVING THREAT LANDSCAPE

RANSOMWARE

CRITICAL INFRASTRUCTURE

STATE-SPONSORED THREAT ACTORS

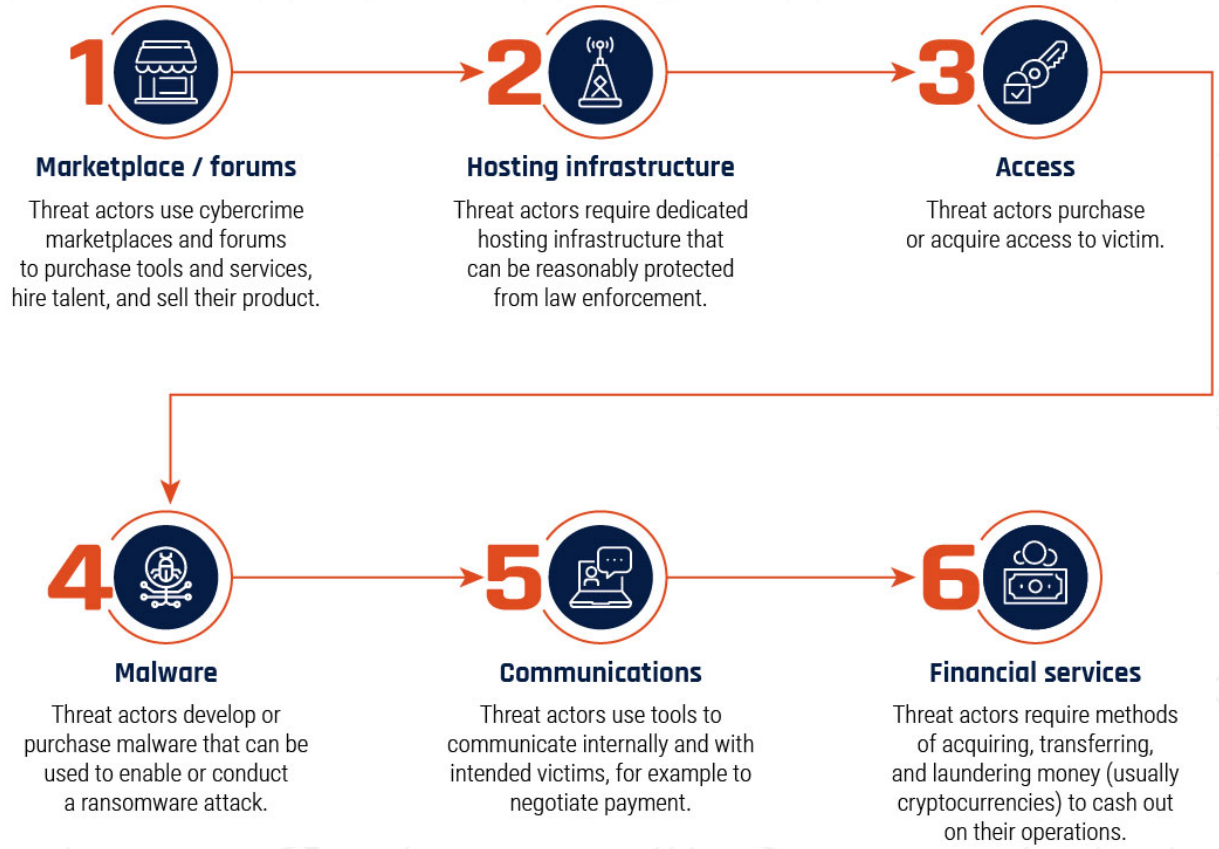
MDM

DISRUPTIVE TECHNOLOGY

RANSOMWARE

Ransomware-as-a-service has significantly lowered the bar to entry for Ransomware

- Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians
- Critical infrastructure organizations are perceived by cybercriminals to be more willing to pay significant ransoms to limit or avoid physical disruption and impacts to their customers



RANSOMWARE

THE RANSOMWARE THREAT IN 2021

- First half of 2021, global ransomware attacks increased by 151% when compared of the first half of 2020 (fueled by Ransomware-as-a-service)
- 2021 was marked by the highest ransoms and the highest payouts
  - In Canada, average cost of a data breach (includes ransomware) was $6.35M CAD
  - Global average cost of recovery from ransomware incident (paying ransom / remediating compromised network) increased from $970 000 CAD in 2020 to $2.3M CAD in 2021
- Cyber Center is aware of 305 ransomware incidents against Canadian victims from Jan 2021 to Jan 2022

Reporting Portal: https://portal-portail.cyber.gc.ca/

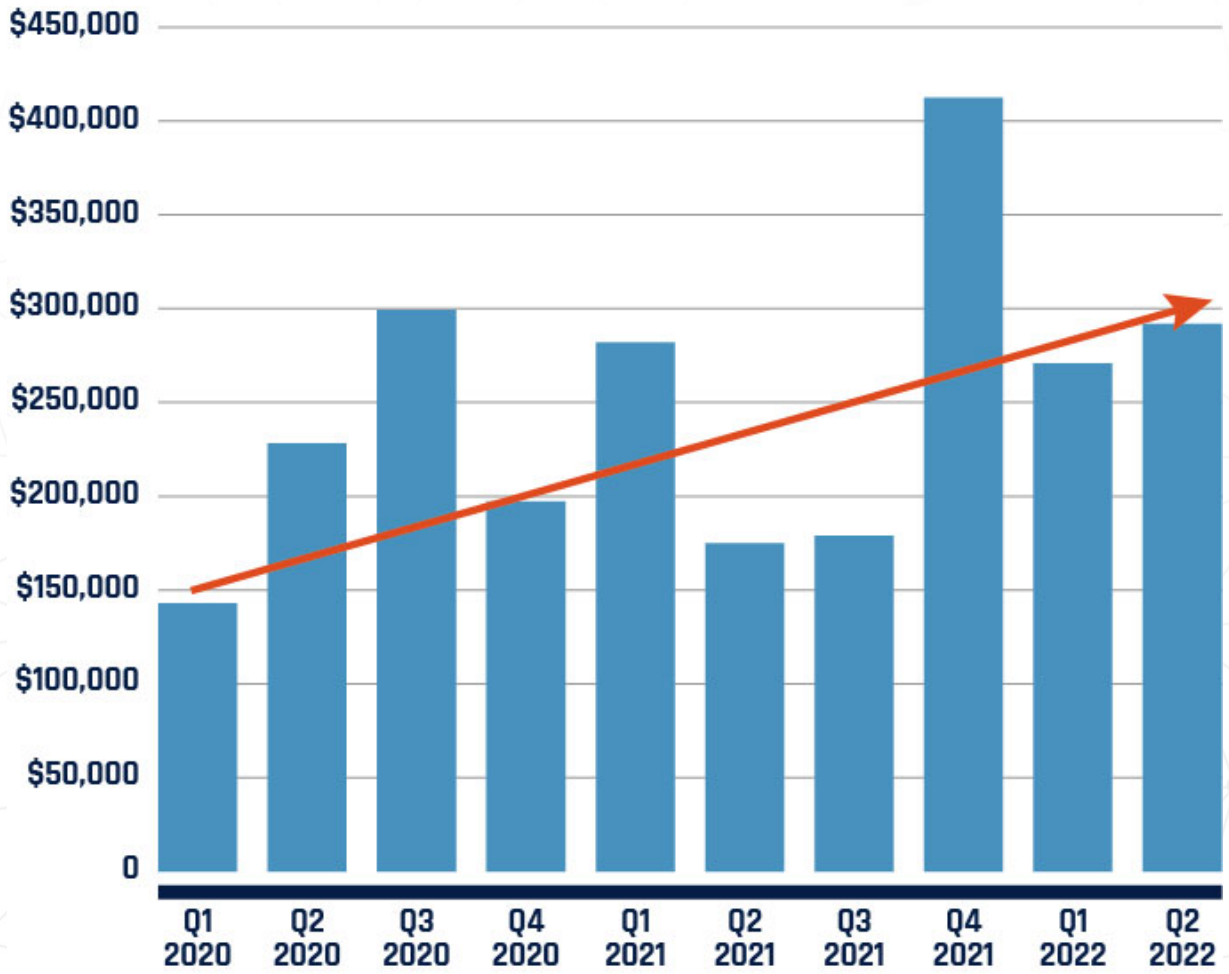
RANSOMWARE

Ransomware is growing in popularity

Ransomware Playbook

- Top Measures to Enhance CyberSecurity for SMO
- Spotting Malicious Email Messages
- Ransomware: How to prevent and recover
- Ransomware: How to recover and get back on track
- Have You Been A Victim of Cyber Crime?

Reporting Portal: https://portal-portail.cyber.gc.ca/



CRITICAL INFRASTRUCTURE

Critical Infrastructure is increasingly at risk from cyber threat activity

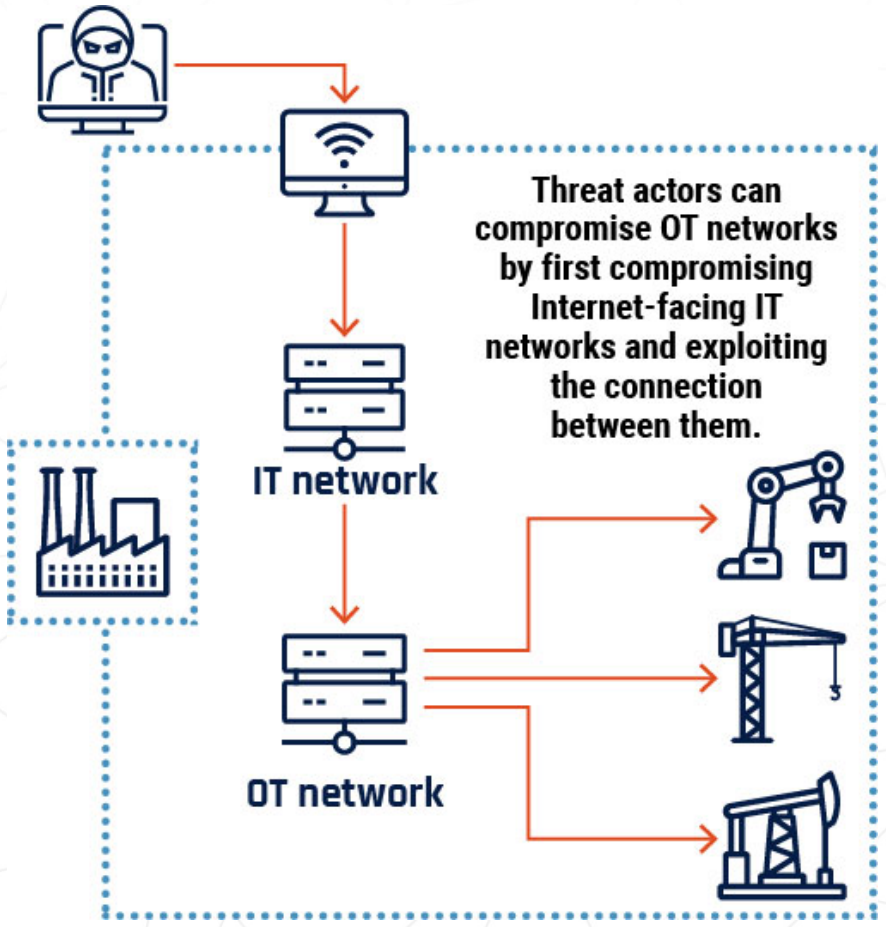
- Cyber criminals exploit critical infrastructure because downtime can be harmful to their industrial processes and the customers they serve
- State-sponsored actors target critical infrastructure to collect information, pre-position in case of hostilities, and as a form of power projection and intimidation
- Increasing exposure of critical infrastructure's operational technology to the internet increases its threat surface

CRITICAL INFRASTRUCTURE

THREATS POSED BY IT AND OT CONVERGENCE

- Vulnerabilities in OT systems that were previously not accessible given the air gap traditionally in place can now be actively exploited

- Threat actors can now reach OT systems through increased exposure



CRITICAL INFRASTRUCTURE

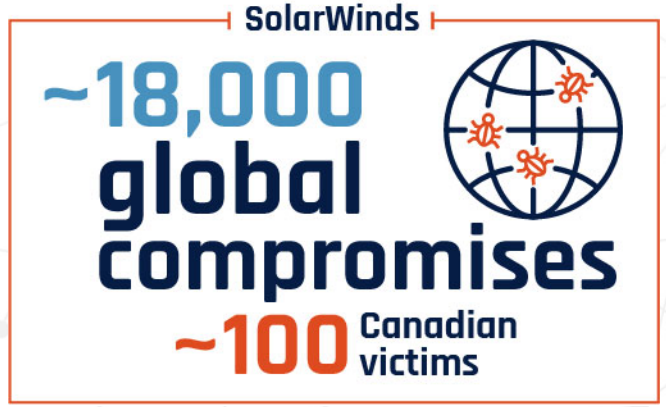
RUSSIAN-BACKED CYBER THREAT ACTIVITY

- Given the Ukraine crisis, Russia will very likely attack the CI of perceived adversaries
- Be prepared to isolate CI components and services from the Internet
- Increase monitoring of your networks
- Enhance security posture (patch systems, enable logging, etc.)

STATE-SPONSORED THREAT ACTORS

State-sponsored threat activity is impacting Canadians

- We assess that the state-sponsored cyber programs of China, Russia. Iran and North Korea pose the greatest strategic cyber threats to Canada
- State-sponsored cyber threat activity against Canada is a constant ongoing threat



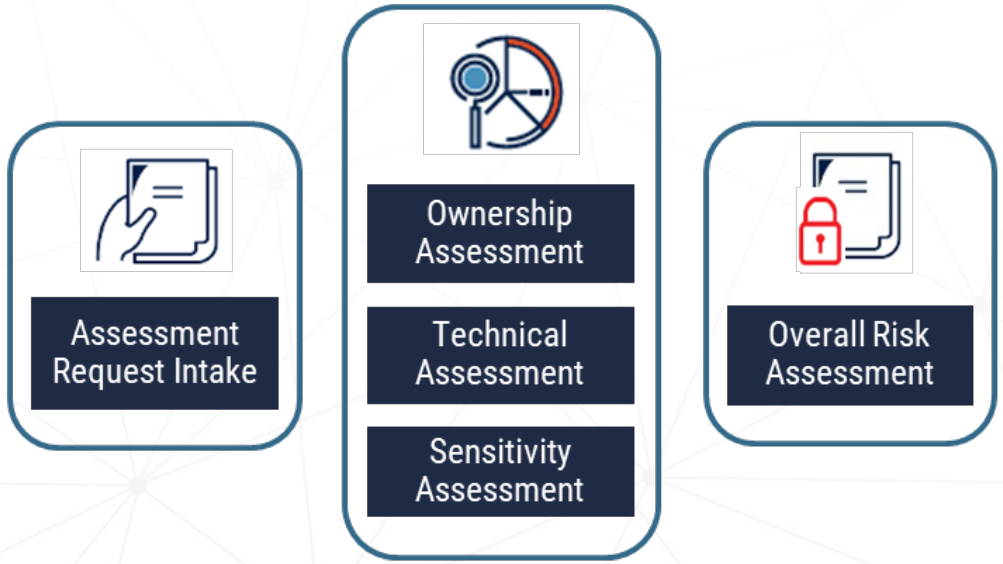
MIS, DIS AND MAL INFORMATION LINK

Cyber threat actors are attempting to influence Canadians, degrading trust in online spaces

- Cyber threat actors' use of misinformation, disinformation and malinformation (MDM) has evolved over the past two years
- Machine-learning enabled technologies are making fake content easier to manufacture and harder to detect.
- Nation states are increasingly willing to use MDM to advance their geopolitical interests.

SUPPLY CHAIN CYBER SECURITY

- Know your supply chain inside and out
- Maintain strong relationships with vendors and suppliers
- Communicate and uphold security requirements
- Foster resiliency and improvement



Ownership

- Underlying controlling interests
- Geolocation of operations
- Business practices

Technical

- Exploitability of products
- Threat actor tactics, techniques, and processes for the product

Sensitivity

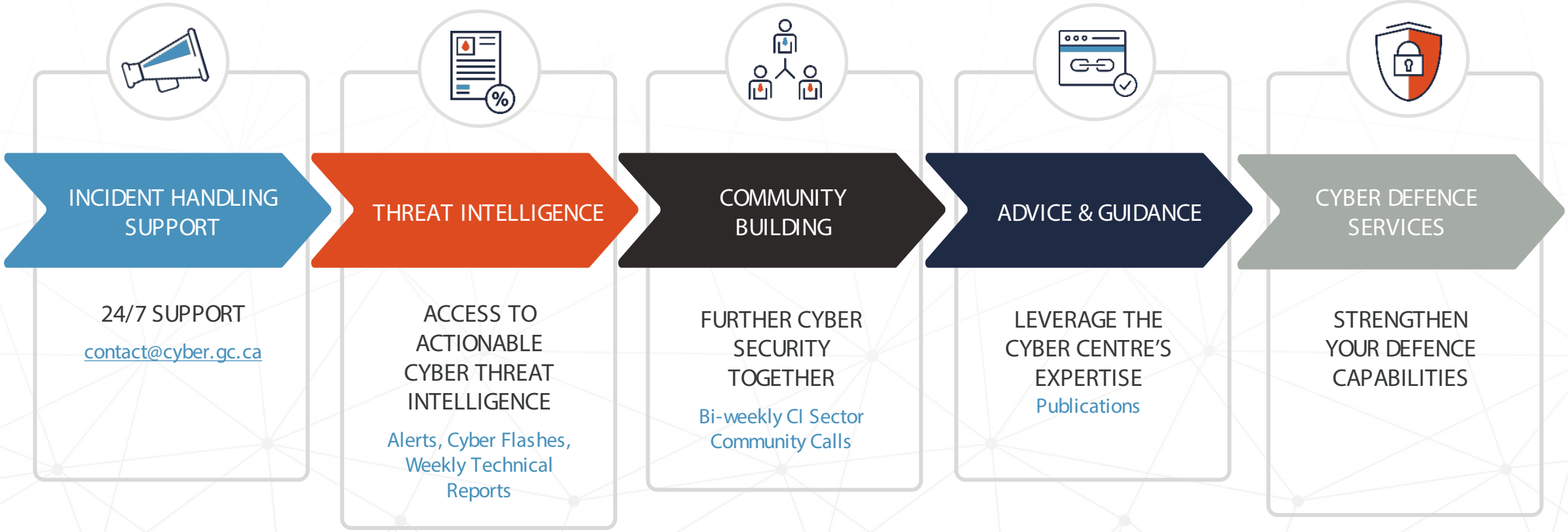
- Sensitivity of data processed by the product or service
- Impact of a product compromise

CONSEQUENCES OF CYBER ATTACKS

- Safety: Malfunctioning IoT/OT devices
- Ethical: Privacy breaches
- Legal: Civil action, lawsuits, regulatory investigations

- Operational: Service interruptions
- Financial: Expenses for investigation, remediation, settlement costs
- Reputational: Loss of public trust due to mis-information
- Loss of IP: Stolen research data or tampering

PRIMARY LINES OF SERVICE



For Free Cyber Center Services: contact@cyber.gc.ca

Incident Handling Support

Support for Cyber Centre Partners

Cyber Incident Reporting

Report cyber incidents to the Cyber Centre

Cyber Centre receives cyber incidents from the community and share back without attribution.

- 24/7 monitoring
- Provide Advice and Guidance on resolving the cyber incident issue.
- Emails to be UNCLASSIFIED (NO PB or CLASSIFIED data)

- Portal: https://portal-portail.cyber.gc.ca/
- Email: contact@cyber.gc.ca

Requirements

✓ Accept the Terms of Use or sign a Non-Disclosure Agreement

Cyber Incident Reporting

The Canadian Centre for Cyber Security works to help build Canada's cyber resilience and security through our advice, guidance, expertise and partnerships.

Malware sample submission

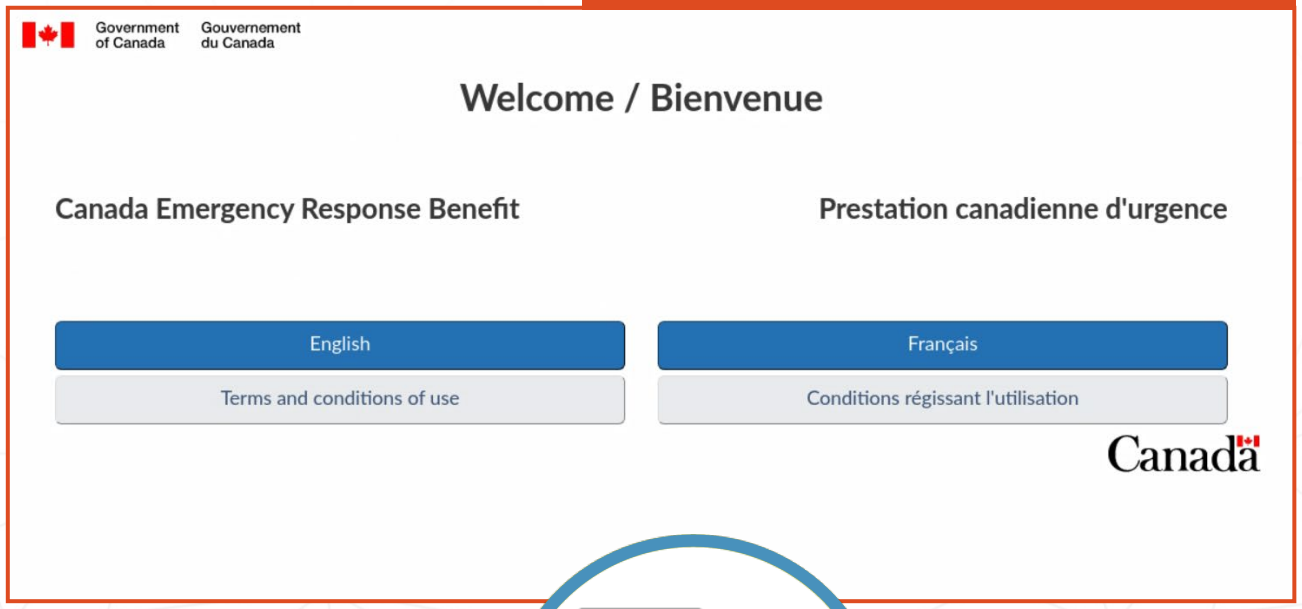
Submit a file suspected of malware or other malicious content for analysis.

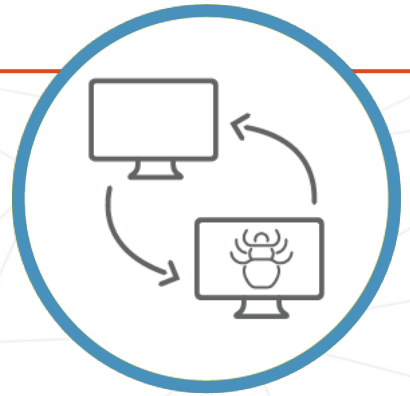
Takedown Service

- Increase in phishing websites with a COVID-19 lure such as Canada Emergency Response Benefit Phishing URL or Government of Canada (i.e. CRA) lure

- The Cyber Centre will takedown these fake websites to protect Canadians from phishing

http://visionchb.com/ref/covid-19

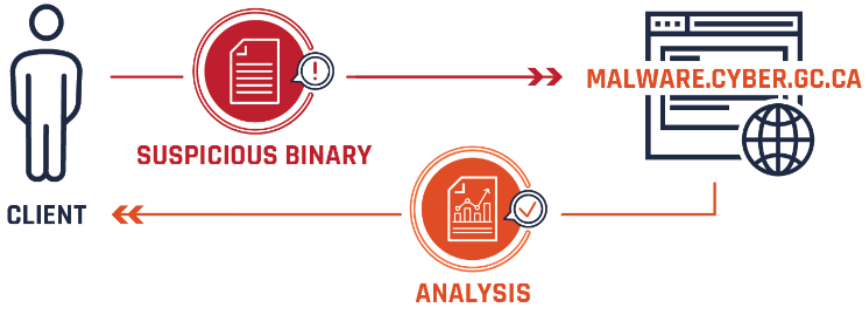




Malware.cyber.gc.ca

Cyber Centre-operated platform to perform deep file analysis, extract indicators of compromise (IP, domain, virus name) and provide a verdict

- Leverages Cyber Centre detection capabilities to analyze new threats
  - Access to 20+ Cyber Centre services, 1000s of signatures, and cyber knowledge bases
  - Can analyze Office documents, PDF, zip files, Windows binaries, and many other file types
  - Updated constantly



Powered by ASSEMBLYLINE

User Access

API

Requirements

- ✓ Fill out Organization Profile and Essential Services form
- ✓ Register in portal
- ✓ Confirm Terms of Use on portal

Threat Intelligence

Actionable Cyber Threat Intelligence

Alerts

Pro-active Notifications on New Cyber Threats

Distributing information, bringing attention and providing detection and mitigation advice on active cyber threats and campaigns that are expected to target Canadian assets and pose an elevated risk to the Government of Canada and its organizations.

Email Alerts

For Government of Canada and Critical Infrastructure partners

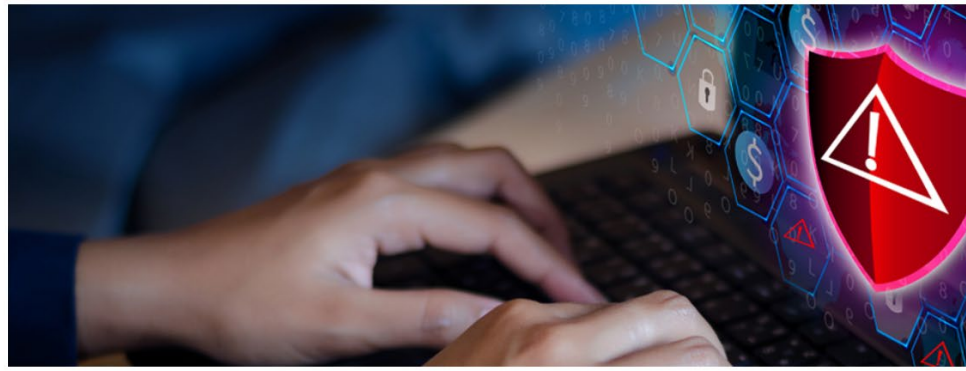
Cyber Centre Website

https://www.cyber.gc.ca/en/alerts-advisories

Requirements

✓ Fill out Organization Profile and Essential Services form

ALERTS | **Disruptive activity against Ukrainian - Update 1**



Number: AL22-002
Date: 24 February 2022
Updated: 25 February 2022

Audience

This Alert is intended for IT professionals and managers of notified organizations.

Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provic mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional of this Alert to recipients as requested.

Overview

On 23 February 2022 the Canadian Centre for Cyber Security (Cyber Centre) became aware of a new disruptive malware, nan Ukrainian organizations [1].

This Alert is being released to raise awareness and share open-source indicators associated with this activity.

Cyber Flash

Urgent Notifications on Active Security Issues

Actionable information sent to describe an immediate or an active security issue that is believed to be targeting the Government of Canada or Systems of Importance to the Government of Canada. The Cyber Flash notifications are TLP:Amber.

Email

Emitted as quickly as possible

Requirements

- ✓ Fill out Organization Profile and Essential Services form

```
*********
TLP:AMBER

This TLP:AMBER report may not be shared beyond the recipient
organization without the express permission of the Canadian Centre for
Cyber Security.

For additional information about the Traffic Light Protocol please
review the following https://www.first.org/tlp/
*********

TITLE
-----
Lorem ipsum dolor sit amet

AUDIENCE
--------
This Cyber Flash is intended for IT professionals and managers within
the federal government and industry.

PURPOSE
-------
Cyber Flashes are time-sensitive and describe an immediate or active
security issue. Examples of situations that warrant a Cyber Flash
include: public release of an exploit which is related to a previous
advisory or alert, rapidly spreading malicious code, an imminent threat
against GC, critical infrastructure and other related industry
networks, multiple denial of service activity, etc.

SUMMARY
-------
```

Publications for Situational Awareness

In addition to the more tactical Cyber Flashes, the Cyber Centre publishes relevant information to keep our CI partners (and Canadians in general) informed. Examples include:

- How to Identify Disinformation, Misinformation and Malinformation
- Cyber Threat Bulletin to take mitigations against known Russian-backed cyber threat activity
- Cyber Threat Bulletin on the cyber threat to Canada's electricity sector
- National Cyber Threat Assessment
  (2022 edition coming this fall)

National Cyber Threat Notification Service (NCTNS)

Cyber Threats Seen on Your IP Space

Sent to you when a sign of compromise or a vulnerable service is seen on your IP space to notice cyber threats faster and better protect your organization.

√ Vetted data to ensure quality and a low percentage of false positive

Email Notifications

API

Requirements

- ✓ Fill out Organization Profile and Essential Services form
- ✓ Provide contact information for the person who will be receiving and using the notifications within the forms
- ✓ Share the IP range specific to your organization within the forms

Scorecards

Actionable Cyber-Event Information

Report on potential infections, vulnerable services notifications, situational awareness data, and a peer-based comparison to other organizations within your sector.

PDF reports emailed monthly
(raw CSV data available on request)

Requirements

- ✓ Fill out Organization Profile and Essential Services form
- ✓ Provide contact information for the person who will be receiving and using the Scorecards
- ✓ Share the IP range specific to your organization

AVENTAIL

Real-time IOC sharing

Sharing relevant and verified information on Indicators of Compromises (IoCs) at machine speed

Requirements

- ✓ Sign a Non-Disclosure Agreement and Letter of Assistance
- ✓ Provide contact information for the person setting up the feed
- ✓ Share the IP address(es) of the system(s) to connect

AVENTAIL-web COMING SOON

Access the reports via online portal

The same information available via our automated feeds can now also be viewed over the web:

- IOCs can be exported as CSVs to feed directly to firewalls which can only ingest flat files
- Organizations can see which IOCs they have ingested via TAXII/MISP
- Graph visualizer shows enrichment for IOCs where available
- Self-serve options include signing up for email reports, updating IP address range, etc.

Requirements

- ✓ Sign a Non-Disclosure Agreement and Letter of Assistance
- ✓ Provide an “admin” user to manage the organization’s info
- ✓ Users will require valid MyCyber portal logins

Community Building

Furthering Cyber Security Together

Community Calls

To Share Sector Relevant Cyber Expertise

Bi-weekly on Wednesday

- Community of Trust
- Situational Awareness
- Regular cadence (monthly, bi-weekly)

contact@cyber.gc.ca

Walk-the-Talk Information Series

Short, Actionable Calls for Partners

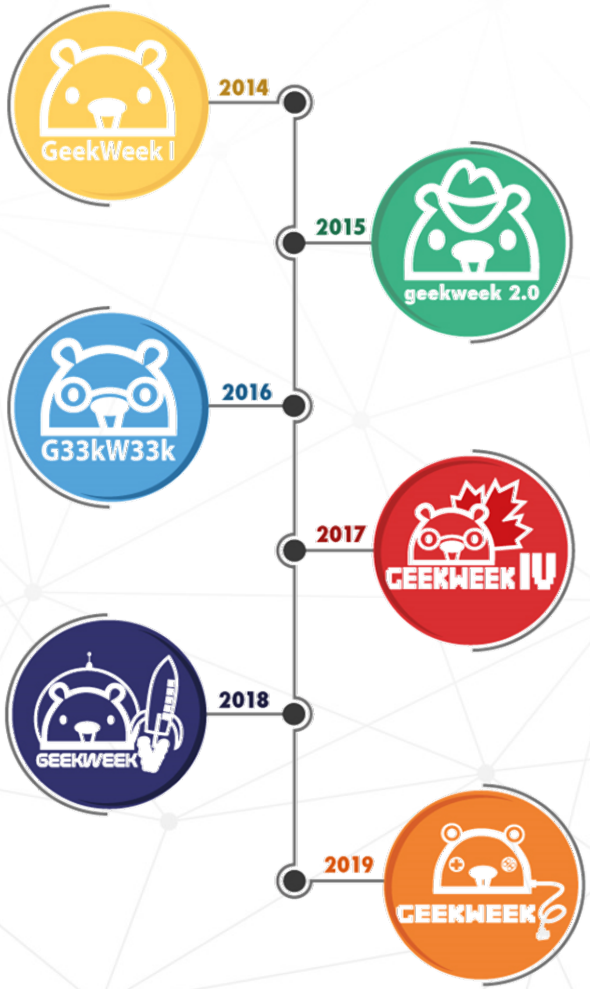
- Roughly bi-weekly cadence
- Short (~45 min) calls on one topic which provide actionable steps or information
- Variety of topics, e.g.
  - Considerations when using an MSP/MSSP
  - Top 10 security controls for small-medium businesses
  - How to do a Supply Chain Risk assessment

GeekWeek

Gathering the Whole Cyber Community

An annual cyber security workshop during which professionals work collaboratively to address cyber security problems through innovative solutions.

- This event is by invitation only. We invite individuals from cyber-related sectors, including private sector security firms and critical infrastructure organizations.
- Participants from cyber-related sectors, including critical infrastructure organizations (e.g., all levels of Government, Finance, Health, Academia) and private sector security firms, work in teams to develop practical, hands-on solutions. We match participants based on their preferred project or topic of interest.



Requirements

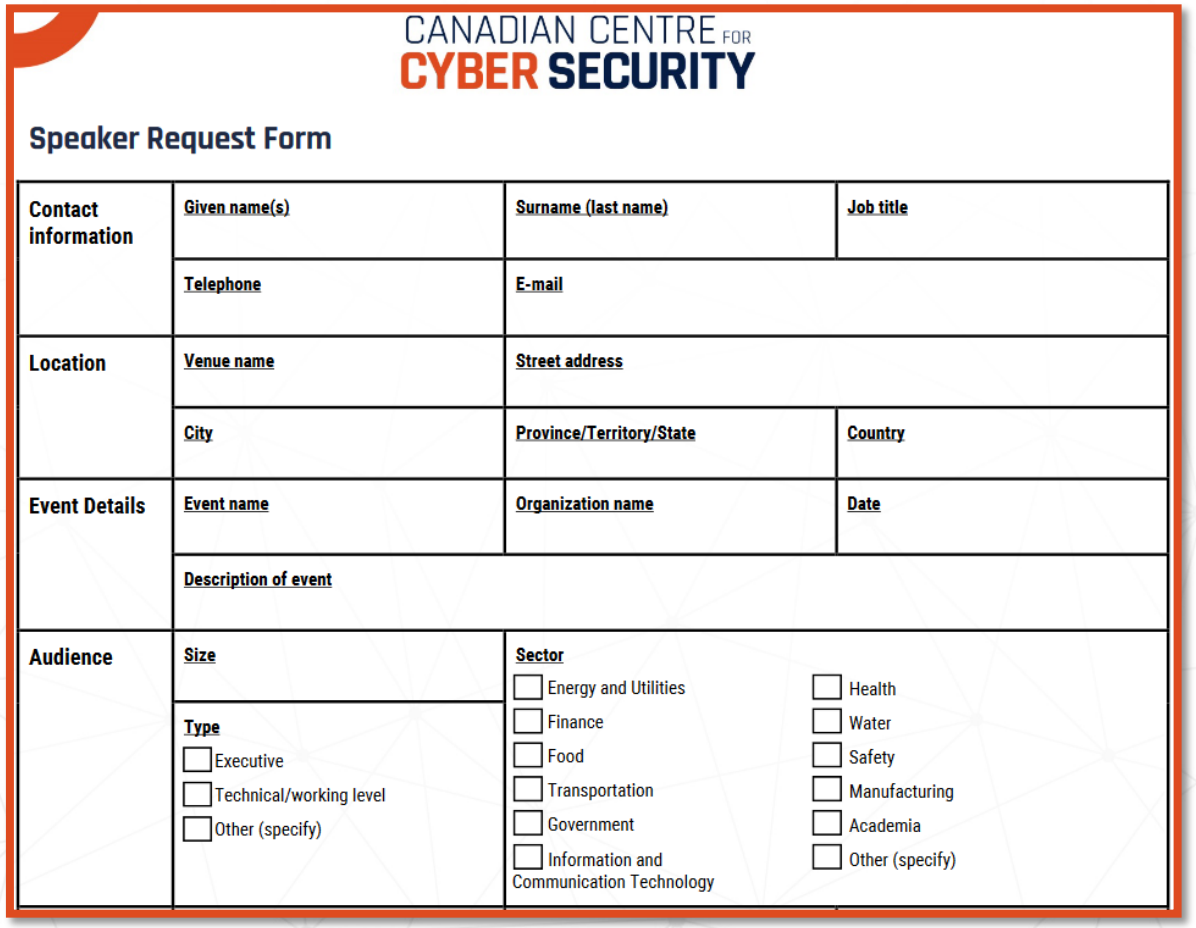
- ✓ Submit your application to the GeekWeek team.
- ✓ Sign a non-disclosure agreement.
- ✓ Attend at least four (4) days of the event and cover all associated travel costs.
- ✓ Bring your own laptop and any other tools needed.

Cyber Centre Speakers for Events

The Cyber Centre makes executives and staff available for speaking engagements

These include activities such as:

- Keynote speeches
- Panel appearances
- Addresses to company boards
- Cyber security awareness briefings for general staff
- Technical talks



CANADIAN CENTRE FOR CYBER SECURITY

Speaker Request Form

Contact information	**Given name(s)**	**Surname (last name)**	**Job title**
	Telephone	**E-mail**	
Location	**Venue name**	**Street address**	
	City	**Province/Territory/State**	**Country**
Event Details	**Event name**	**Organization name**	**Date**
	Description of event		
Audience	**Size**	**Sector** ☐ Energy and Utilities ☐ Finance ☐ Food ☐ Transportation ☐ Government ☐ Information and Communication Technology ☐ Health ☐ Water ☐ Safety ☐ Manufacturing ☐ Academia ☐ Other (specify)	
	Type ☐ Executive ☐ Technical/working level ☐ Other (specify)		

Advice & Guidance

Leverage the Cyber Centre's Expertise

Publications

- Visit cyber.gc.ca and check out all our recent publications

- Security considerations for industrial control systems (ITSAP.00.050)
- Security considerations for critical infrastructure (ITSAP.10.100)
- Protecting your organization against denial of service attacks (ITSAP.80.100)
- Protect your organization from malware (ITSAP.00.057)
- Managing and controlling administrative privileges (ITSM.10.094)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Baseline security requirements for network security zoning (version 2.0) (ITSP.80.022)
- Preventative security tools (ITSAP.00.058)

Canadian Cyber Security Tool (CCST)

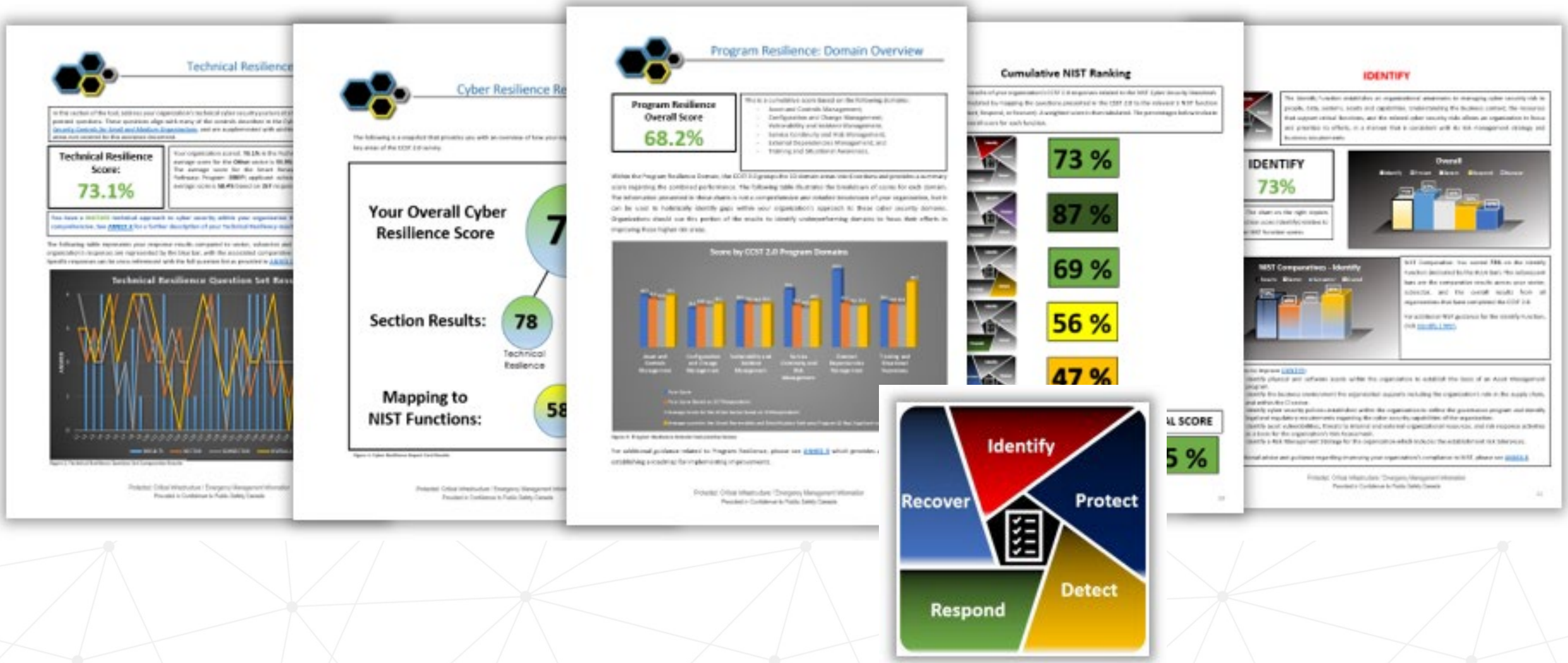
Virtual Self-Assessment Tool

An easy-to-use questionnaire for organizations to assess their operational resilience and cyber security posture

- Developed in collaboration with Public Safety
- Questions assessing:
  - ✓ Organizational information
  - ✓ Cyber incidents
  - ✓ Incident reporting
  - ✓ Technical resilience
  - ✓ Program resilience
- Approximately 1-2 hours to complete
- Participants will receive a report with advice and guidance related to each cybersecurity theme and an entity specific score based on comparative results with other organisations

CCST v1.0	CCST v2.0
38 questions	140 questions
Released Jan 2021	Released Oct 2022
High level assessment	Medium level assessment
Program and technical resilience scores	Includes additional scores for each NIST pillar

Program, Technical Resilience and NIST Results



Cyber Security Plan Template

For Canadian Cyber Security Tool (CCST) Users

- Template to help critical infrastructure organizations develop their cyber security plans based on their CCST self-assessment results.

Breakdown of Initiatives

Describe each initiative in more detail. You can use the example table provided below.

[Initiative]

Estimated internal effort (High/Medium/Low)	Choose an item.	**Initiative description** [Describe the initiative here. Which gaps will it address? Are there any dependencies?] **Objectives** • [Objective 1] • [Objective 2] • [Objective 3] • [Etc.] **Scope** [Describe what is in scope for this initiative.] **Risk/assumptions** [List any risks and assumptions.]
Operating cost (High/Medium/Low)	Choose an item.	
Risk impact (High/Medium/Low)	Choose an item.	
Managed service	[Yes/No]	
Duration	[timeframe]	
Approximate start date	[Quarter#, Year #]	
[List the business goals and the Level 1 baseline controls that will be met and the gaps (identified in your assessment results) that will be addressed.]		

HOW CAN I PROTECT MY ORGANIZATION?

Regularly back up your data and store off-line. LINK

Use strong and unique passwords, implement MFA. LINK

Update and patch systems. LINK

Have an Incident Response Plan (and test it!) LINK

Use security tools. LINK

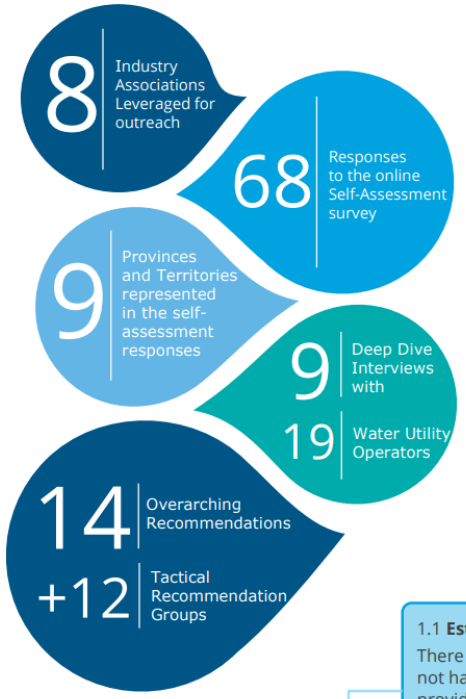
Cyber Center's Baseline Cyber Security Controls for SMO
ISED's CyberSecure Canada eLearning
National Standard CAN/CIOC 104:2021
Cyber Centre's Top 10 To Protect Internet Connected Networks

Cyber Security Study of the

Canadian Water Sector

Deloitte. | CANADIAN CENTRE FOR CYBER SECURITY

The Canadian water sector is one of the 10 national Critical Infrastructure sectors that directly contribute to the safety, well-being and prosperity of Canadian citizens. In recent years, OT and IT environments have become more converged to enable efficiencies and automation, which has exposed the water sector to a myriad of new cyber threats. The Cyber Centre has engaged Deloitte to deepen its understanding of 4 critical infrastructure sectors including the Canadian Water sector, and maximize its support to these sectors.



Sector Maturity

2.33 Overall Maturity

Strategy Capabilities: **2.2** Secure Capabilities: **2.5**
Vigilant Capabilities: **2.0** Resilient Capabilities: **2.4**

Small Operator Average: **2.31**
Large Operator Average: **2.29**

*The self-assessment for this study used the **Deloitte Cyber Strategy Framework**, which leverages inputs from industry-standard frameworks including NIST, ISO and SANS and is organized into **34 sub-capabilities** in **12 capability groups** across **4 core pillars**; Strategy, Secure, Vigilant and Resilient*

Least Mature Capabilities:

- Threat Intelligence
- Vulnerability Identification

Most Mature Capabilities:

- People and Workplace
- Infrastructure Security
- Identity & Access Management

Key Observations

Key findings and observations were gleaned from the self-assessment and further explored with water utility operators in deep-dive interviews. These informed 14 recommendations that the cyber centre could leverage to support the Canadian Water Sector

Ransomware is top-of-mind

By a wide margin, organizations listed ransomware most frequently as a severe threat that "kept them up at night". This is not just driven through sensationalism, as the ability to monetize malware is a real and prevalent threat that water sector should be concerned about.

IT and OT lack coordination

Municipalities often have distinct structures responsible for cyber security in their OT environment and their Corporate IT environment.

OT environments rely on imperfect air-gapping, and operators lack resources specific to OT to improve maturity

Suspected self-assessed overconfidence

Some questionnaire respondents likely scored their organization higher than warranted. Contributing factors include a level of unfamiliarity with IT/cyber frameworks and a perception that they can be satisfied with basic safeguards because they don't perceive themselves as a target.

Recommendations

Shaded items are High-Impact Recommendations

1. **Leverage Leadership Opportunities**
2. **Create Tailored Instructional Resources**
3. **Provide Specific Threat Intelligence**
4. **Support Incident Response Capabilities**

1.1 **Establish a community network and 'Centre of Excellence'**
There is little communication amongst utility providers, and they do not have a clear champion for cyber security. The Cyber Centre could provide significant value by organizing regular communications, events, and a platform for secure ad-hoc chat.
FTE: 1 Time: ①① Initial Cost: $$ Ongoing Cost: $

2.1 **Step by step guides and 'top action' guides**
OT environment-specific guides to establish best practices across the industry. Respondents expressed interest in guides outlining top actions that an organization could take to improve their cyber security posture, and documentation for implementing 'low-hanging fruit'.
FTE: <1 Time: ①① Initial Cost: $$ Ongoing Cost: $

3.1 **Develop Targeted Threat Reports**
FTE: 1+ Time: ①① Initial Cost: $$ Ongoing Cost: $

4.1 **Help organizations develop IR plans and procedures**
FTE: 1 Time: ① Initial Cost: $$ Ongoing Cost: $

1.2 **Publish briefings for executives and municipal leaders**
FTE: <1 Time: ① Initial Cost: $ Ongoing Cost: $

2.2 **Self-Assessment Tools**
FTE: 1 Time: ①① Initial Cost: $$ Ongoing Cost: $

3.2 **Host briefing sessions on threat intelligence interpretation**
FTE: <1 Time: ① Initial Cost: $ Ongoing Cost: $

4.2 **Help Organizations develop IR playbooks for specific threats**
FTE: 1 Time: ① Initial Cost: $ Ongoing Cost: $

4.3 **Test IR plans and procedures**
Water utility systems do not have sufficient redundancy to be safely take offline for testing. Hosting tabletop exercises, penetration testing, etc. would enable operators to test their incident response plans in a safe, controlled environment.
FTE: 1+ Time: ①① Initial Cost: $ Ongoing Cost: $$

1.3 **Host a steady series of online and in-person conferences**
FTE: <1 / 1+ Time: ①① Initial Cost: $$ Ongoing Cost: $

3.3 **Assist risk analysis & remediation strategies**
Aid in cost/benefit analyses on potential actions suggested in threat intelligence reports based on the risk appetite of the organization.
FTE: 1 Time: ① Initial Cost: $ Ongoing Cost: $

3.4 **Alert system for Zero Day vulnerabilities**
FTE: <1 Time: ①① Initial Cost: $$ Ongoing Cost: $

4.4 **Design a simulation environment**
Design a virtual water treatment OT environment for full-scale incident response exercises.
FTE: 1+ Time: ①①① Initial Cost: $$ Ongoing Cost: $$

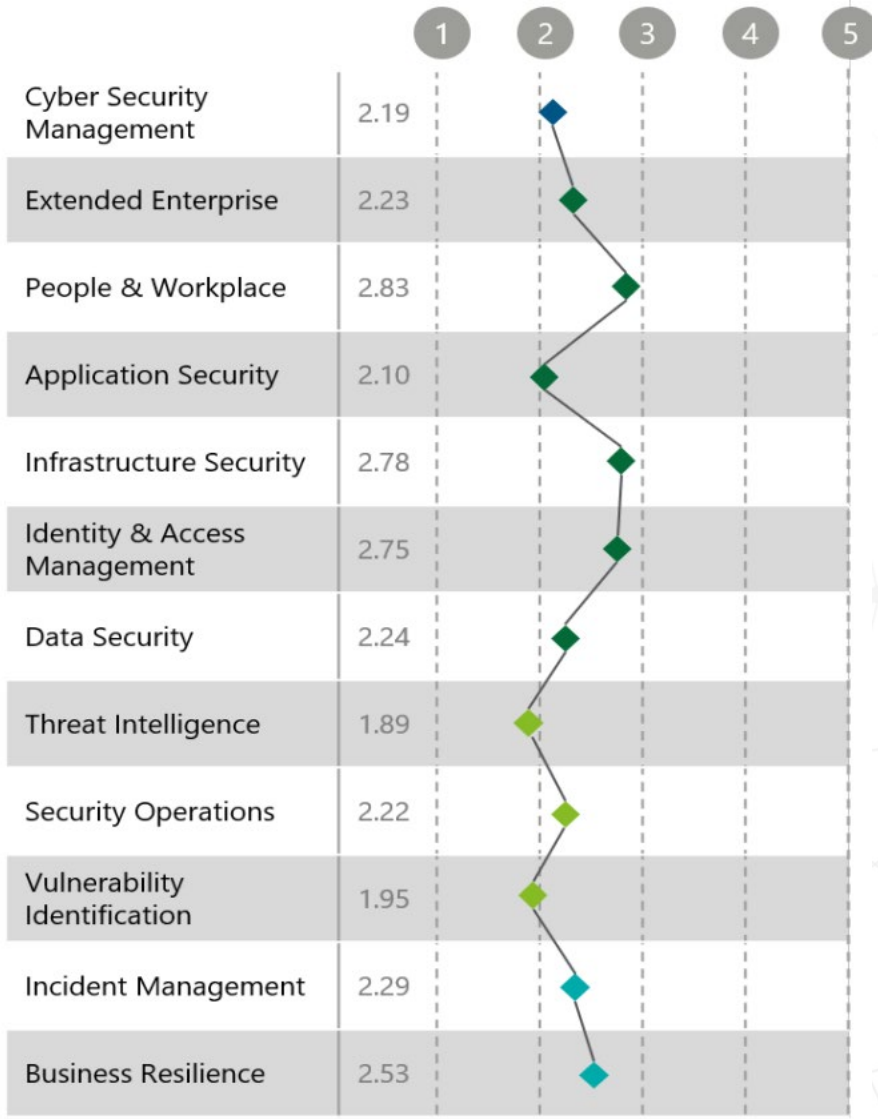
4.5 **Build capacity to directly assist incident response efforts.**
Provide 'Hands on Keyboards support to utility providers during cyber incidents.
FTE: 1+ Time: ①① Initial Cost: $$ Ongoing Cost: $$

<1: Less than 1 FTE **①: Less than 3 months** **$: Under $300K**
1: 1 FTE **①①: 3 months to 1 year** **$$: $300k – $1.5M**
1+: 2+ FTEs **①①①: Greater than 1 year** **$$$: $Over 1.5M**

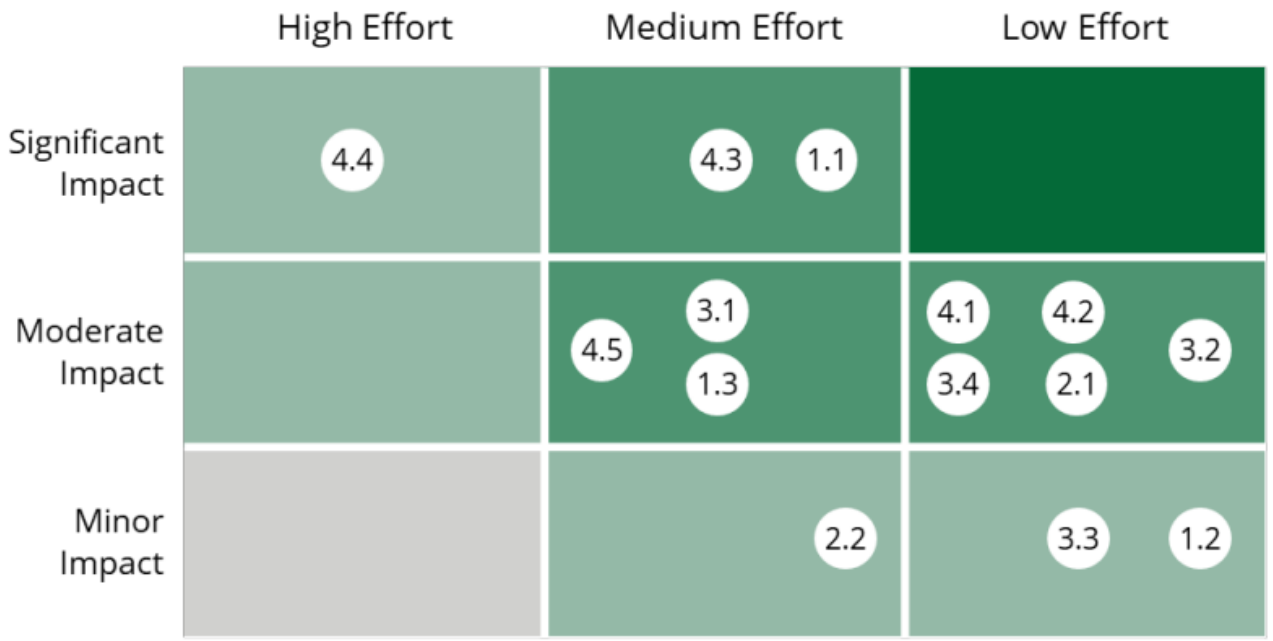
Cybersecurity Study of the Canadian Water Sector

Top Threats and Requested Supports

Most Concerning Threats		Most Requested Support	
Score	Threat	Score	Support
138	Ransomware	87	Cyber Threat Intelligence
77	Data Loss	74	Employee Awareness Training
64	Malware and Spyware	69	Cyber self-assessment tools
58	Phishing Attacks	56	Step-by-step cyber guides
57	Security Convergence (OT/IT/IoT)	51	Technology & cyber tool guides



Cybersecurity Study of the Canadian Water Sector



1: Leverage Leadership Opportunities	**2:** Create Tailored Instructional Resources	**3:** Provide specific Threat Intelligence	**4:** Support Incident Response Capabilities
1.1: Establish a community network and 'centre of excellence' 1.2: Publish briefings for executives and municipal leaders 1.3: Host and participate in steady series of online and in person conferences	2.1: Step-by-step guides and 'top action' guides 2.2: Self-assessment tools	3.1: Develop targeted threat reports 3.2 Host briefing sessions on threat intel interpretation 3.3 Assist with risk analysis and remediation strategies 3.4 Establish alert system for zero day vulnerabilities	4.1: Help organizations develop IR plans and procedures 4.2: Help organizations develop IR playbooks for specific threats 4.3: Test IR plans and procedures 4.4: Design a simulation environment 4.5: Build capacity to direct assist incident response efforts.

CONNECT WITH US

 contact@cyber.gc.ca

 www.cyber.gc.ca

 @cybercentre_ca

Cyber Centre Publications :
https://cyber.gc.ca/en/publications

Cyber Center Alert & Advisories:
https://cyber.gc.ca/en/alerts-advisories

To report fraud:
Canadian Anti-Fraud Centre
1-888-495-8501
www.antifraudcentre-centreantifraude.ca

To report a cybercrime:
Local police or
Royal Canadian Mounted Police
www.rcmp-grc.gc.ca

To report a cyber incident
Canadian Center for Cyber Security

 cyberincident@cyber.gc.ca