Intelligent Defence:
Partnering to Detect and Respond to Cyber Attacks

Kevin Parent | Program Manager, Cybersecurity Initiatives | CANARIE
Jill Kowalchuk | Executive Director | CanSSOC
Martin Vezina | Security Solution Architect / Product Lead, Threat Feed | CanSSOC

May 18, 2021 | May 28, 2021

Webinar Recording Policy

This webinar will be recorded and archived, including all audio. The video will be archived on the CANARIE YouTube channel and may be promoted through CANARIE communication channels.

Any text questions or comments, if responded to, will remain anonymous and not be part of the recording.

The recorded video will include your voice, if audio participation is enabled.

Politique concernant l'enregistrement des webinaires

Ce webinaire sera enregistré et archivé, y compris tout le matériel audio. La vidéo sera conservée sur le canal YouTube de CANARIE et pourra être promue au moyen des filières de communication de CANARIE.

Si on y répond, les questions écrites et orales demeureront anonymes et ne feront pas partie de l'enregistrement.

Toutefois, si la fonction « participation audio » a été activée, le fichier vidéo inclura votre voix.

Our shared reality

- We are all connected – both physically and by our collaborations.
- Every connected device and organization is susceptible to cyber threats.
- Given our interconnectedness, we're only as strong as our weakest link.
- Cybersecurity is not simply an IT problem – it's an organizational priority.
- A national approach to cybersecurity is only possible when the whole sector aligns and coordinates their efforts.

When it comes to securing the whole sector, we are stronger than the sum of our parts.

The Vision: A More Secure Canada

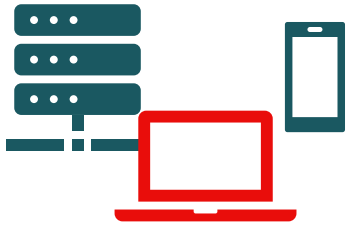
The Cybersecurity Initiatives Program (CIP)

A national, collaborative, cybersecurity program that serves Canada's research and education sector.

Built by the community, for the community.

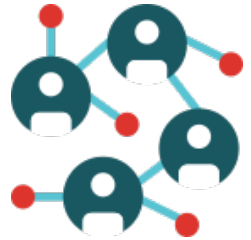
National Coordination for Local Impact

Leverages the collaborative nature of the sector



Mitigates risk at each layer

Builds on existing initiatives



Engages the community to evolve

Our partners' collaboration has been integral to developing the approach and strategy for the CIP.

CANSSOC

CAUBO ACPAU

cira

COLLÈGES & INSTITUTS CANADA | COLLEGES & INSTITUTES CANADA

compute canada | calcul canada

CUCCIO
Communication / Collaboration / Innovation

Fédération des cégeps

NDRIO | NOIRN
New Digital Research Infrastructure Organization | Nouvelle organisation d'infrastructure de recherche numérique

POLYTECHNICSCANADA

Universities Canada. Universités Canada.

ACORN-NL

ACORN NOVA SCOTIA

COLLÈGE AURORA COLLEGE

BCNET

cybera

ECN
NB PEI Educational Computer Network

MRnet
Manitoba Research Network

NUNAVUT ARCTIC COLLEGE

ORION

risq

SRNET

Yukon University

Benefits for eligible organizations:

- Augment your cybersecurity infrastructure
- Measure the impact of cybersecurity initiatives at your organization
- Collaborate with a national community of security experts in R&E
- Increase your team's security capacity and expertise; training & support is integrated into the program
- Strengthen the overall security posture of your organization.

At no cost. Your participation is your investment.

First 3 Funded Initiatives

Implementation, support, and training across 210 eligible organizations.

cira

D-ZONE DNS FIREWALL

CANSSOC Threat Feed

Intrusion Detection System

Funded initiatives are intended to integrate with each other to strengthen local cybersecurity and in turn, the overall security of the whole sector.

Complementary Functions to Strengthen Your Organization

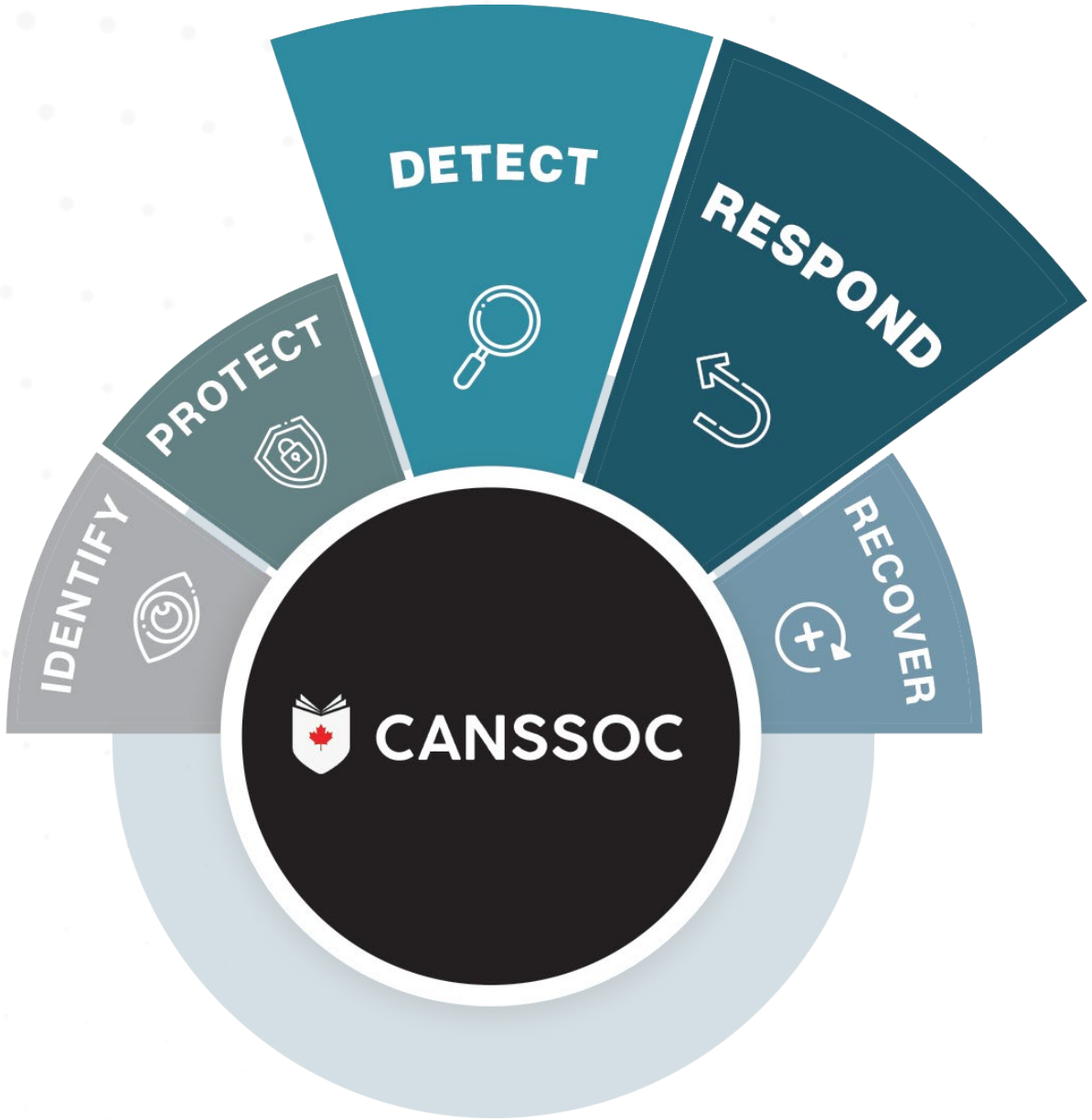
	DNS Firewall	Threat Feed	IDS
Blocks end users from accessing malicious websites	X		
Provides intelligence to devices to block traffic		X	
Alerts security analysts of suspicious behaviour			X
Dynamically updates systems with new threats	X	X	X

CanSSOC Threat Feed: A New, Funded Initiative for Canada's Research & Education Sector

PART OF THE **SHARED FABRIC**

Better than we can do on our own, always in partnership

SPECIALIZING IN
DETECTION & RESPONSE

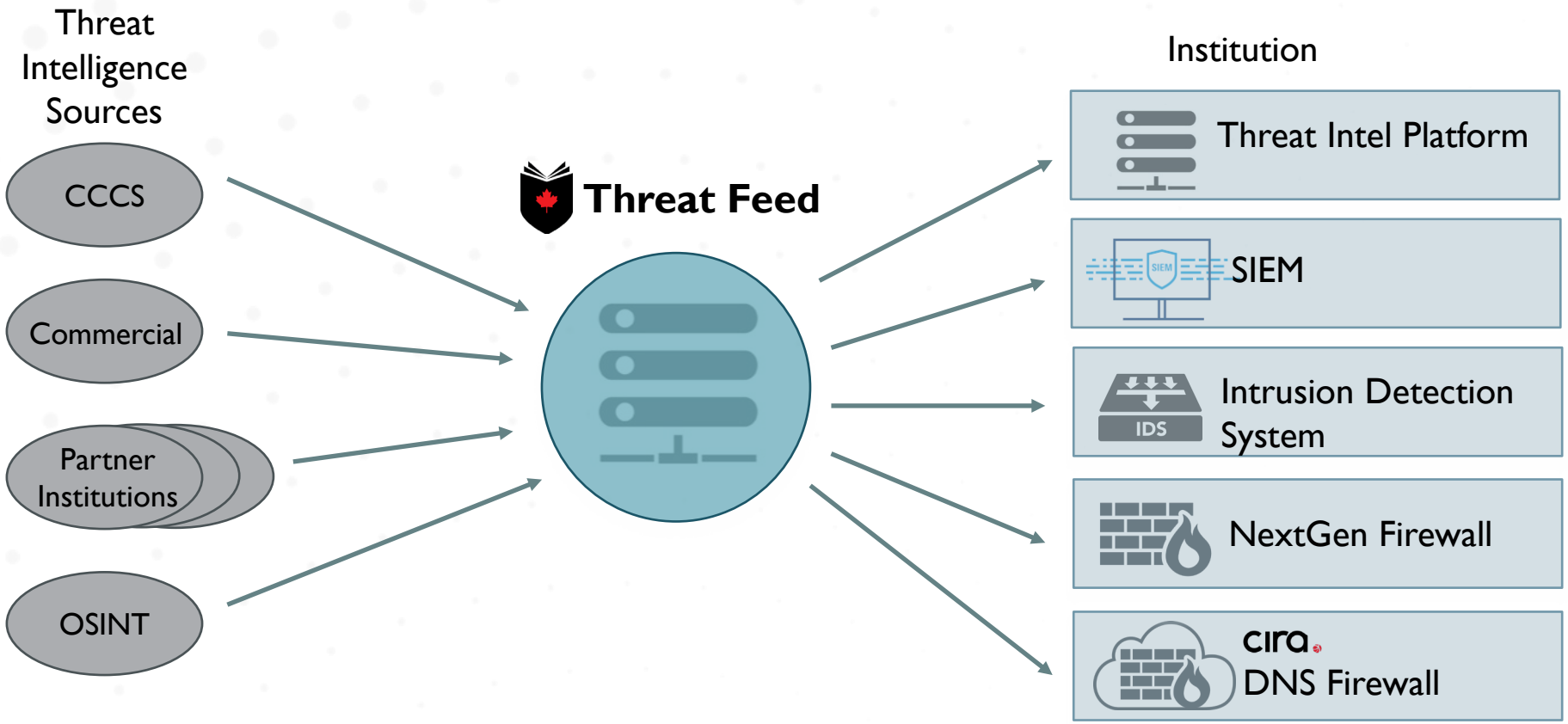


THREAT FEED PERSONNEL REQUIREMENTS

1-3 hours from firewall administrator - One time only

Save Security Analyst time to focus on detection and response

WHAT IS THREAT FEED?



CANSSOC

WHY CANSSOC THREAT FEED?

- Reduce time spent by local analysts on curating threat intel
- Consolidates multiple feeds into one consistent curated feed
- CanSSOC Analysts update with Open-Source Threat Intelligence (OSINT)
- Institutional specific threat intelligence (automated and manual)

THREAT INTELLIGENCE PLATFORM VS FEEDS

Threat Intelligence platform (MISP)

- Repository of all indicators and attributes
- Centralized location to investigate information about indicators
- Established open-source solution with a growing community
- Extensible platform, no vendor tie-in

Threat Intelligence feeds (MineMeld)

- Feeds that can be automatically ingested into protection devices
- Open-source solution – To be replaced– fall 2021

THREAT INTELLIGENCE PIPELINE

CANSSOC

NEXT GENERATION FIREWALL INTEGRATION

- Most Next Generation Firewalls can consume threat intelligence feeds
- Simple to configure (1-3 hours of administrator time)
- Set it and forget it -
- Benefit: ~30% reduction in malicious connections with little effort

SUPPORT

- Collaboration between NREN Partner Analysts & CanSSOC Analysts
- Primary mechanism is Slack
  - #institution-canssoc – sign up any staff members; primarily used for support and reporting issues
  - #threatfeed – any staff members; updates to the service
  - #threatintel – InfoSec staff only; agree to TLP; sensitive sharing of info
  - #threatfeed_documentation – any staff; documentation

ONBOARDING

1. Sign confidentiality agreement (CANARIE)
2. Book onboarding meeting
3. CanSSOC creates accounts: MISP & MineMeld
4. One hour onboarding session: CanSSOC or your NREN Partner
5. Integrate into firewall or other end point protection or detection devices

ACTIONABLE INTELLIGENCE

- Trusted partner for disclosure: report@canssoc.ca
- Threat Feed is the foundation for detection & response
- Provides a simple, sector sourced, mechanism for sharing information

How to sign up:
If your organization has already enrolled in the CIP…

1. Your provincial or territorial partner in the NREN will send you a link to the Threat Feed Selection Form
2. After you submit the form, CANARIE will send you the CanSSOC Confidentiality Agreement
3. Execute (sign) the agreement
4. Your NREN Partner will contact you to coordinate your technical onboarding session

How to sign up:
If your organization has not yet enrolled in the CIP…

1. Contact your NREN Partner to confirm your organization's eligibility
2. If you're eligible, your NREN Partner will send you a link to the CIP Participation Form; you can select the Threat Feed at the same time
3. After you submit the form, CANARIE will send you the agreement to enrol in the CIP (OCCA) and the CanSSOC Confidentiality Agreement
4. Execute (sign) the CANARIE OCCA
5. Execute the CanSSOC Confidentiality Agreement
6. Your NREN Partner will contact you to coordinate your technical onboarding session


A
Q

canarie

canarie.ca | @canarie_inc

cip@canarie.ca