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.
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.
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

<table>
<thead>
<tr>
<th>Function</th>
<th>DNS Firewall</th>
<th>Threat Feed</th>
<th>IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocks end users from accessing malicious websites</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provides intelligence to devices to block traffic</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alerts security analysts of suspicious behaviour</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Dynamically updates systems with new threats</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
CanSSOC Threat Feed: A New, Funded Initiative for Canada’s Research & Education Sector
Better than we can do on our own, always in partnership

PART OF THE SHARED FABRIC
SPECIALIZING IN DETECTION & RESPONSE
THREAT FEED PERSONNEL REQUIREMENTS

Limited cybersecurity resources

1-3 hours from firewall administrator - One time only

Greater cybersecurity resources

Save Security Analyst time to focus on detection and response
WHAT IS THREAT FEED?

Threat Intelligence Sources
- CCCS
- Commercial
- Partner Institutions
- OSINT

Institution
- Threat Intel Platform
- SIEM
- Intrusion Detection System
- NextGen Firewall
- DNS Firewall
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

Ingestion → Negative Curation → Automatic Positive Curation → Manual Positive Curation → Feed Generation
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