canarie

New Funded Initiative: **Intrusion Detection System**

Kevin Parent | Program Manager, Cybersecurity Initiatives
Julian Corduneanu | Director, Cybersecurity

August 5, 2021 | August 18, 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
New Digital Research Infrastructure Organization

NOIRN
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

ᓄᓇᕗᒻᒥ
ᓯᓚᑦᑐᖅᓴᖅᕕᒃ
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

Intrusion Detection System (IDS)

What is the Intrusion Detection System (IDS) initiative?

- *IDS continues the development of a community of institutional security specialists that will strengthen the overall security of higher education by increasing awareness of institutional security issues and better understanding its potential vulnerabilities.*

- IDS is the continuation of the original Joint Security Project (JSP).
- IDS participants will join the 138 institutions that are already part of IDS.

IDS: Expected Outcomes

1. Staff from eligible organizations across Canada work together to implement and improve a data-based security system.

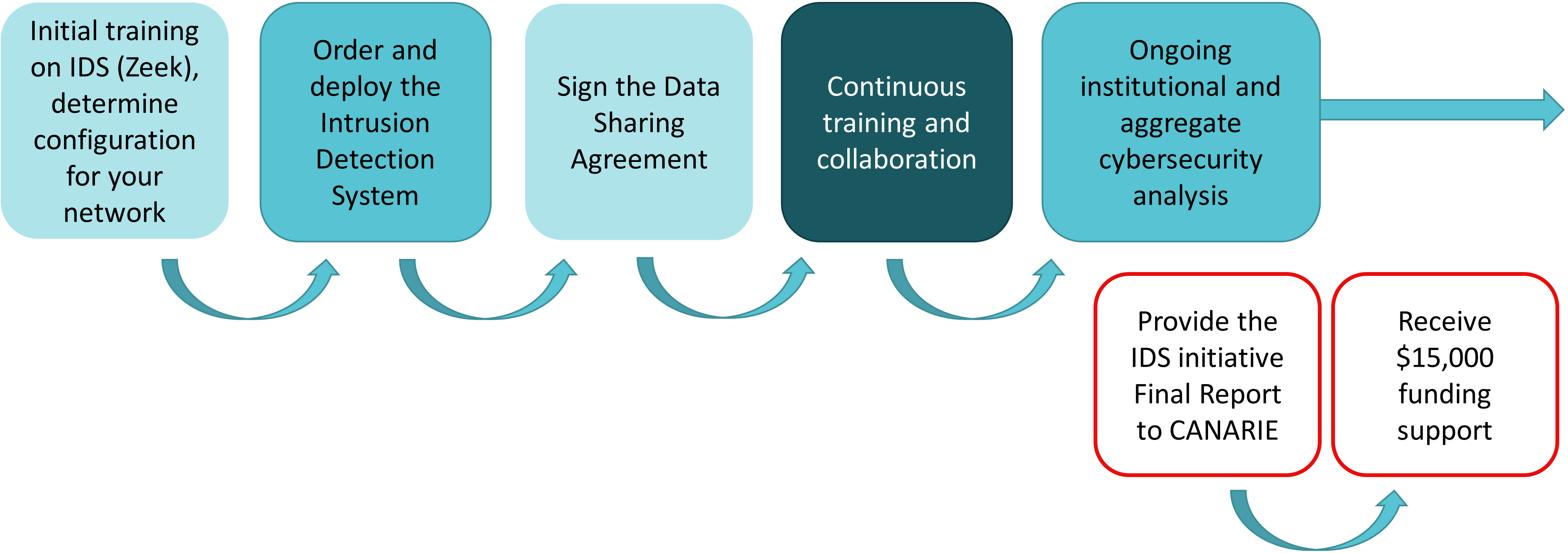
2. Analysis tools monitor network traffic from these organizations to provide current threat and vulnerability information.

IDS: Expected Outcomes

3. The agreed network security monitoring policies and processes, coupled with the resulting threat information, solidify how institutions may work together more closely in future.

4. Position for potential future integration with other security initiatives resulting in more complete, cohesive, and comprehensive network security for all institutions connected to the NREN.

IDS Participation Process Overview



Initial training on IDS (Zeek), determine configuration for your network

Order and deploy the Intrusion Detection System

Sign the Data Sharing Agreement

Continuous training and collaboration

Ongoing institutional and aggregate cybersecurity analysis

Provide the IDS initiative Final Report to CANARIE

Receive $15,000 funding support

IDS Components Provided

- DELL PowerEdge R440 (Recommended OS: CentOSStream, and Zeek Network Traffic Monitoring for IDS anomalies detection)
- Network TAPs with dedicated support shelves (IXIA or GIGAMON)
- SFP/SFP+ (optical/copper)

Technical Implementation & Maintenance Requirements

- 1U server rack space with 120V power outlet
- 1G or 10G optical/copper connectivity from the server via the 2 provided TAPs (passive optical or active copper) to your network, or use mirror ports on your existing networking equipment
- 1G server management connectivity for software updates and user controlled selective data push to the IDS Analytics Platforms

IDS Analysis Tools

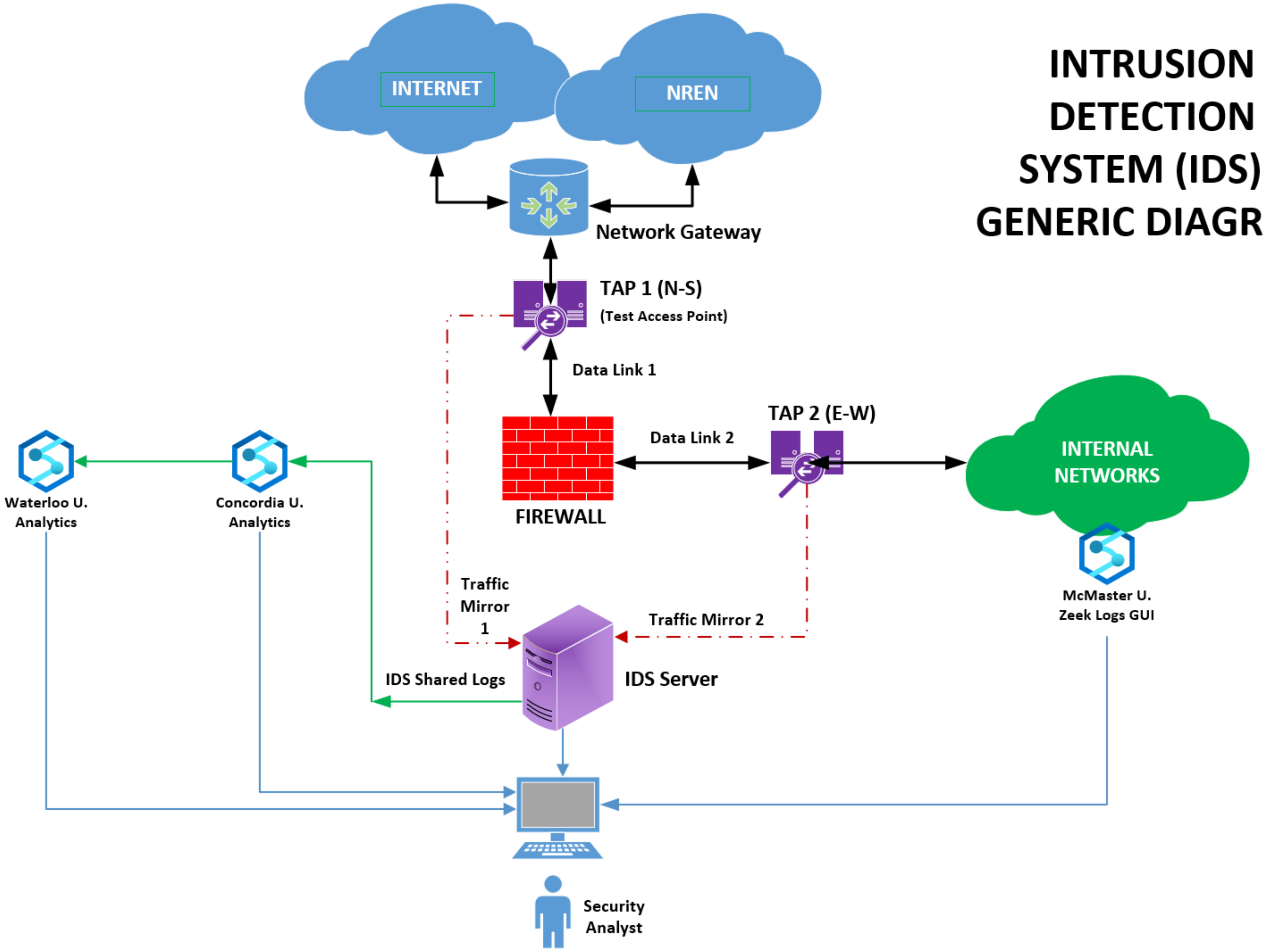
3 researcher-developed cybersecurity analysis tools are available:

1. Concordia University – web portal provides detailed cybersecurity analytics based on the institutional data you are willing to share. Provides the same analysis for all institutions in aggregate, deidentified.

2. University of Waterloo – web portal provides detailed cybersecurity analytics based on the institutional data you are willing to share. Provides the same analysis for all institutions in aggregate, deidentified.

3. McMaster University (now supported by the affiliated FyeLabs) – locally installed tool to examine entire IDS data directly at your institution.

INTRUSION DETECTION SYSTEM (IDS) - GENERIC DIAGRAM



Sign-up Process:

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 IDS and other available initiatives at the same time.

Sign-up Process:
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 IDS Selection Form
2. Once submitted, CANARIE will send you the IDS Participation Agreement
3. Once signed, you'll be invited to technical onboarding sessions to help you decide which IDS equipment you should order for your specific infrastructure
4. Submit your order form
5. Once you receive your equipment, we will follow up with setup and training details.

What happens after you've installed your IDS Server and network tap(s)?

1. Configure what collected data you wish to share externally
2. Sign data sharing agreement
3. Initiate data sharing with Concordia, Waterloo platforms
4. Access cybersecurity analysis portals
5. Participate in ongoing regular coordination meetings with other institutions

A
Q

canarie

canarie.ca | @canarie_inc

cip@canarie.ca