Cybersecurity Initiatives Program
What It Could Mean for Your Organization

December 16, 2020 | January 12, 2021

Presentation Overview

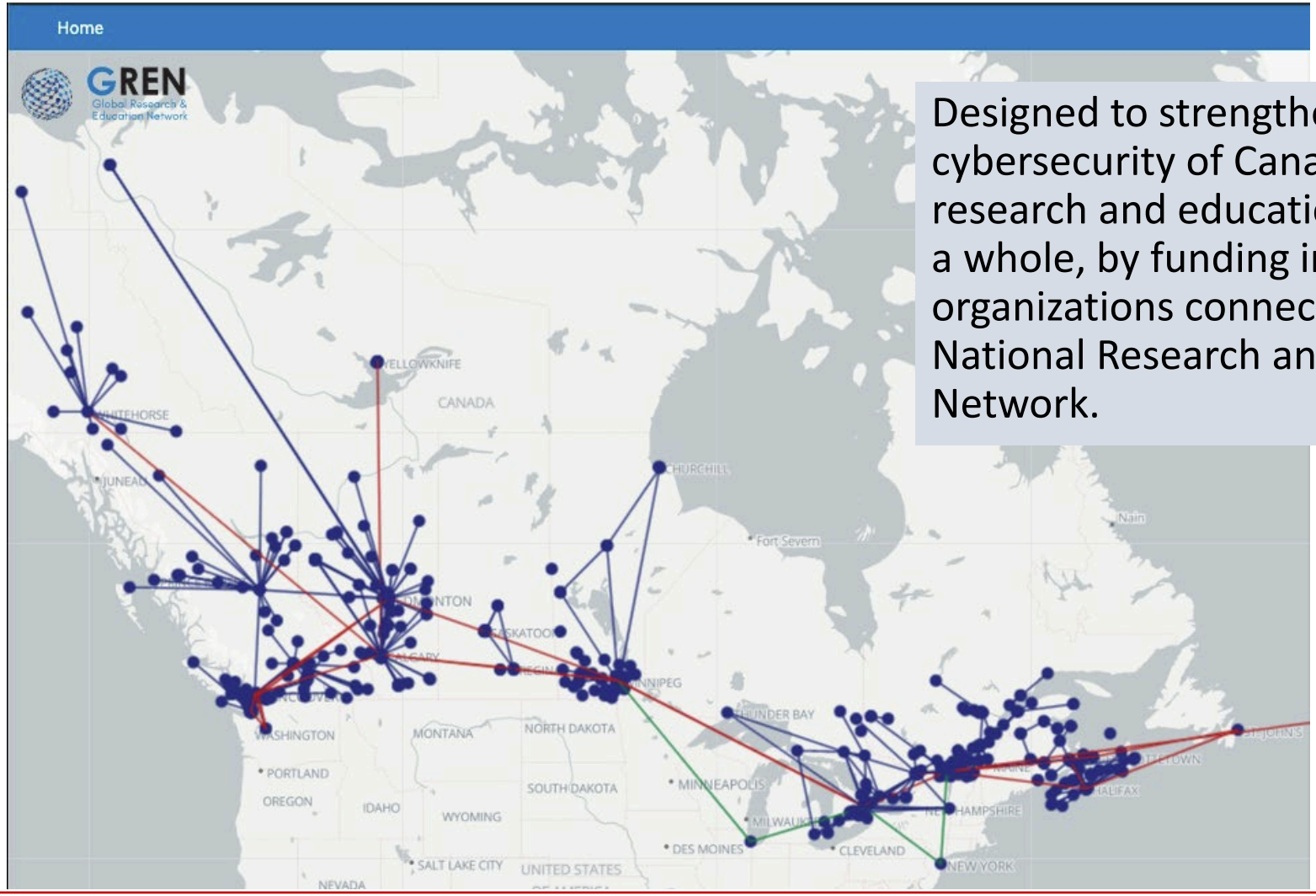
1. Cybersecurity Initiatives Program (CIP) Overview
2. How to Participate
3. The First Three Initiatives
4. Q and A

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.

Introduction to the Cybersecurity Initiatives Program (CIP)



Designed to strengthen the cybersecurity of Canada's research and education sector as a whole, by funding initiatives at organizations connected to the National Research and Education Network.

Terminology

NREN

- National Research and Education Network – the country-wide network implemented by CANARIE and our provincial and territorial partners

NREN Partner

- One of the 13 provincial and territorial partners in the NREN + CANARIE

Initiative Partner

- An organization responsible for delivering a funded initiative under this program (e.g. CIRA or CanSSOC)

Eligible Organization (EO)

- An organization that is eligible to access funded initiatives under the Cybersecurity Initiatives Program

What does the CIP do?

- Funds and delivers initiatives to strengthen EOs' cybersecurity posture
- Initiatives could include:
  - Physical devices to help secure the EOs' internal networks
  - Cloud services to minimize vulnerability of EOs' staff, faculty and students to cybersecurity threats
  - Information about new and emerging threats
  - Training
  - Others

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 direct cost.

Initiative Delivery

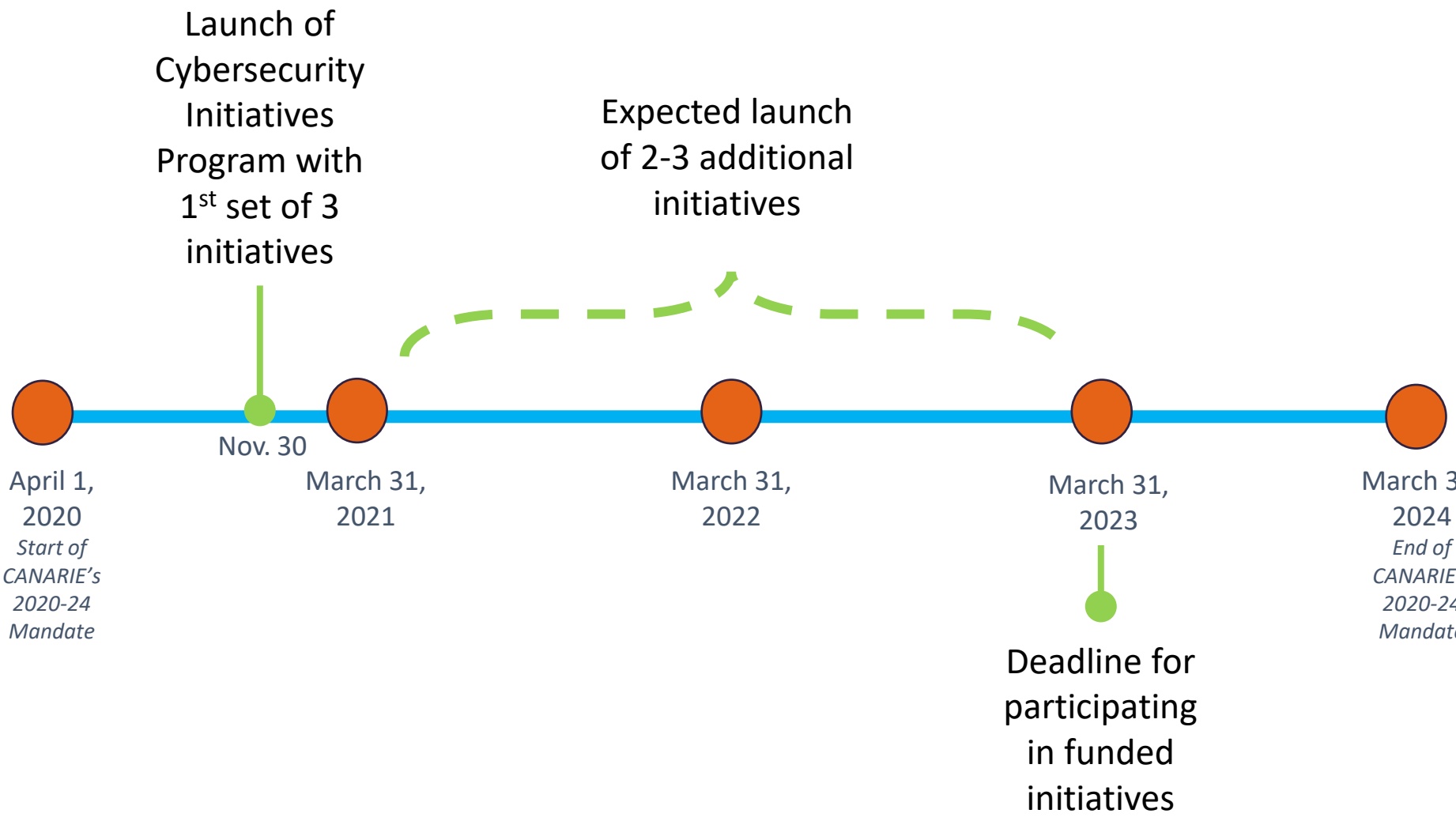
> We work with our NREN Partners to deliver funded initiatives to Eligible Organizations (EOs).

> Your NREN Partner is your primary contact for requesting an initiative.
  - Additional support provided by CANARIE cybersecurity team.

> There is no direct cost to EOs to participate in this program or to access funded initiatives.

> There's no accounting overhead for your organization; Initiative Partners are typically funded directly by CANARIE.

Program Timeline



Who determines the funded initiatives?

Community engagement and input drive all program elements – most importantly, its governance.

Cybersecurity Advisory Committee
Leaders from Canada's universities, colleges, polytechnics, cégeps, not-for-profit and private sector organizations

Role:

- advocates for a coordinated national approach to R&E cybersecurity
- provides guidance on funding initiatives under this program

Selecting Initiatives

> Initiatives are validated against a common set of factors:
  - Efficacy
  - Broad applicability
  - Time to deploy
  - Affordability
  - Sustainability

> Also considered are:
  - National coordination
  - Measuring the impact

First 3 Initiatives

Funding implementation, support, and training across 200+ Eligible Organizations

Funding implementation, support, and training across 200+ Eligible Organizations

Intrusion
Detection
System
(Join the JSP)

Funding implementation, support, & training for all Eligible Organizations not yet enrolled in the Joint Security Project (JSP)

Intended to integrate with each other to strengthen local cybersecurity and in turn the overall security of the whole sector.

How to Participate

Eligibility Criteria

To participate in the CIP, organizations must be:

1. Connected to Canada's National Research and Education Network (NREN); and
2. A member organization of an NREN Partner AND connected to that NREN Partner through an autonomous network; and
3. A post secondary institution, a non-federal research facility, or a Centre of Excellence.

Individual initiatives may have their own eligibility criteria. These will be clearly defined as each initiative is launched.

Participant Obligations

- Typically, provide some staff time to participate in initiative deployment and operation
- Contribute metrics through March 2024 for any initiatives deployed by your organization
- Submit a short report after each initiative is deployed

How to Participate

1. Representatives from provincial & territorial NREN partners will invite Eligible Organizations to participate in the program
   - Please contact your NREN Partner to confirm your eligibility

2. Eligible Organizations:
   - Submit a short participation form to CANARIE
   - Execute a standard Organization Cybersecurity Collaboration Agreement (OCCA)

3. Once the OCCA is executed, your NREN Partner will provide instructions for accessing funded initiatives
   - The OCCA only needs to be executed once

Questions you may have…

Do we have to implement all funded initiatives?

> No. You choose the best initiatives for your organization. Please share reasons for opting out of specific initiatives to help planning of future initiatives.

Are these initiatives intended to replace what we already have in place?

> No. The intention is for all Eligible Organizations connected to the NREN to have a standard baseline of cybersecurity technologies, processes, and skills.

> CIP initiatives are intended to fill gaps that may exist and supplement tools and processes already in place

Questions you may have…

Is there a deadline to participate in the CIP?

- Participate at any time, but funded initiatives can only be accessed once an OCCA is executed.
- The sooner you participate, the longer your organization will be able to benefit from the funded initiatives.
- Deadline for participation in funded initiatives: March 31, 2023
- Funding for the CIP continues to March 31, 2024

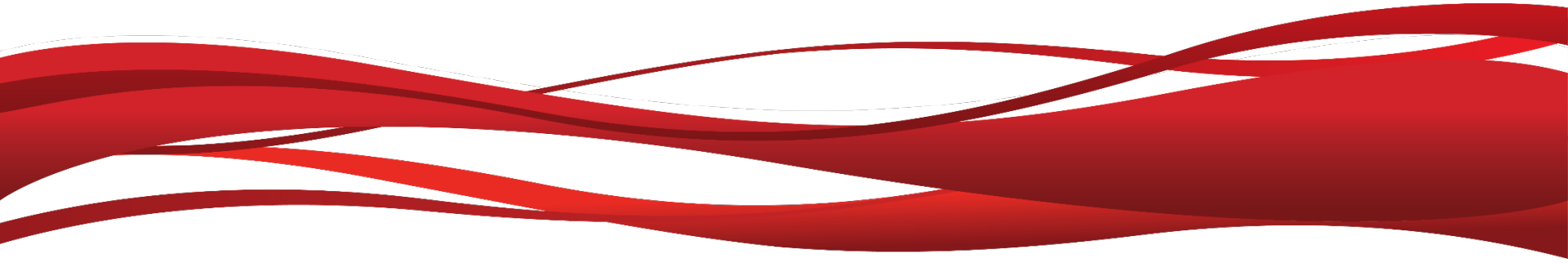
Our organization is already using CIRA DNS Firewall. How can we benefit from the program's funding?

- Funding for the CIRA DNS Firewall begins on January 1, 2021. We urge you to complete the CIP Participation Form that you've received from your NREN Partner as soon as possible. Once we've received this from you, we will send you the agreement (OCCA) that must be executed to benefit from funding.

Introducing the First 3 Initiatives

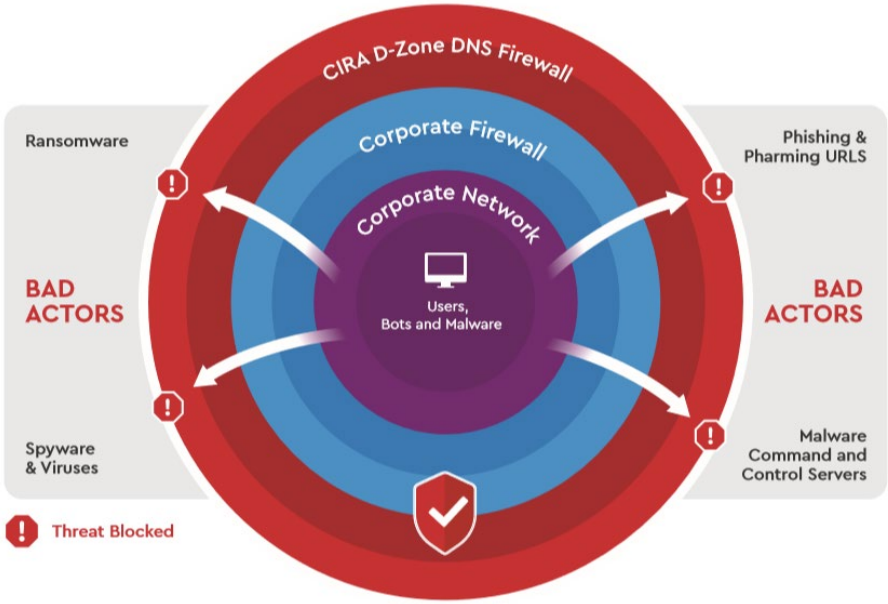
Intrusion
Detection
System
(Join the JSP)

CIRA – Mark Gaudet



CIRA DNS Firewall

- ✓ A layer outside the organization that provides highly effective malware, phishing and botnet protection
- ✓ Already deployed at 57 research and education* organizations in Canada
- ✓ Over 2 million Canadian users across public sectors

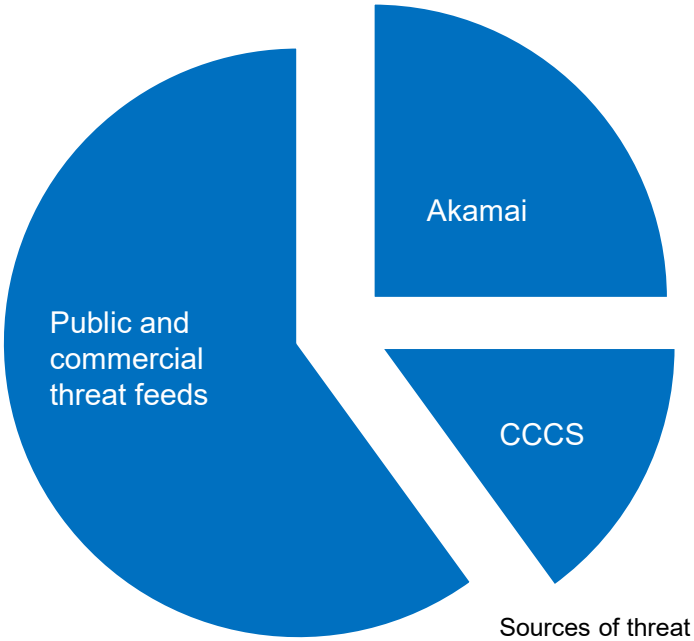


* Excluding K-12

CIRA DNS Firewall is delivering

High performance DNS delivering 5x higher block rate than seen in other public sector peers.

- ✓ Top quality DNS answering 13 billion queries per month with a **median response time of 18 ms** – better than Google 888*.
- ✓ On average more than **100,000 new threats are added** to the block list daily
- ✓ NREN networks saw **1.3M threats blocked last month** or 2 blocks/network user**



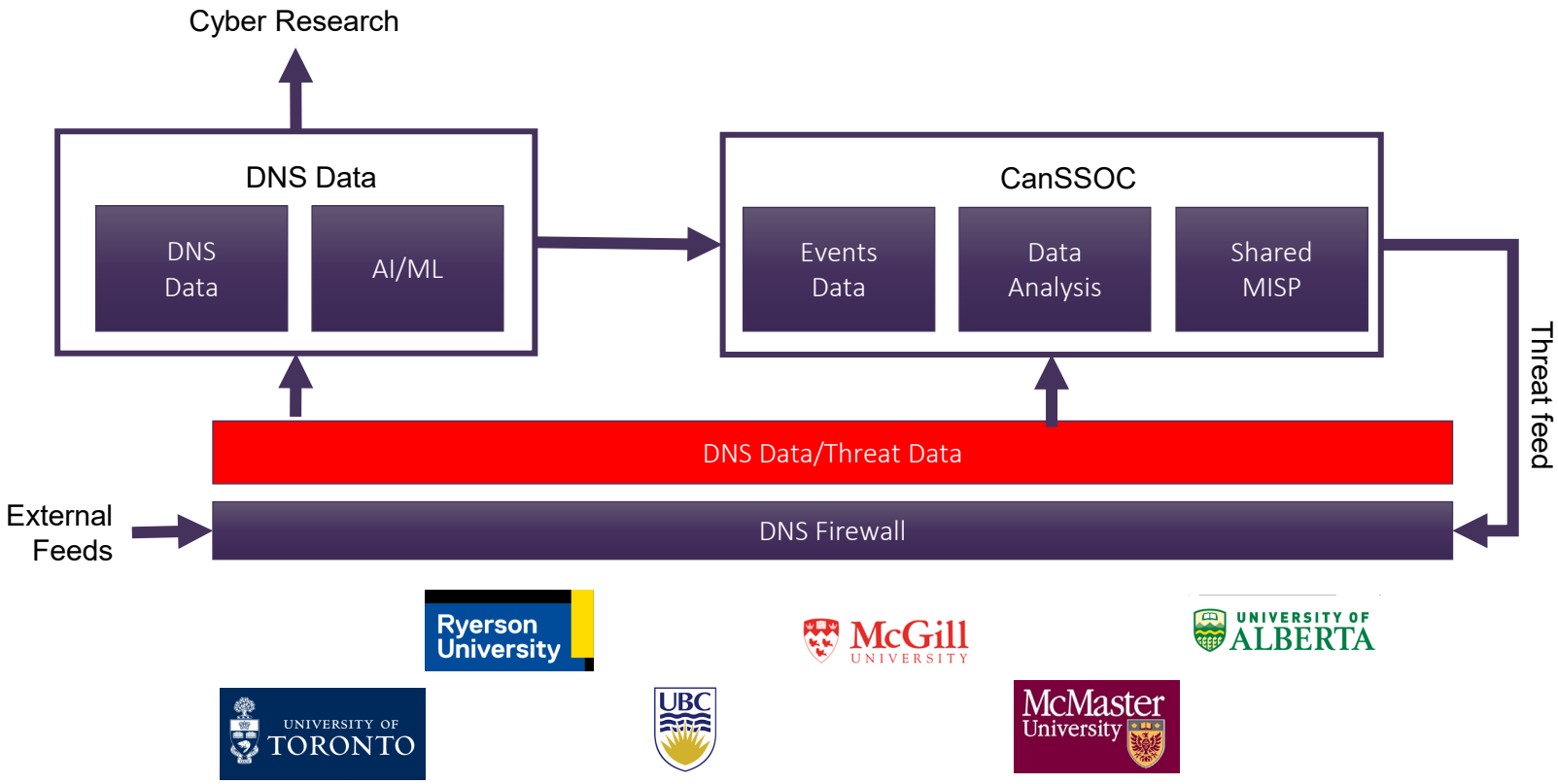
Sources of threat blocking

* Tests performed using RIPE Atlas from Canadian servers

**COVID-times data. For comparison, pre-COVID was just under 3 blocks/user in higher-ed, 5 in K-12, and 1.6 in municipalities.

cira

National DNS Firewall Vision



(founding CanSSOC members shown)

cira

CIRA DNS Firewall

Architecture Highlights

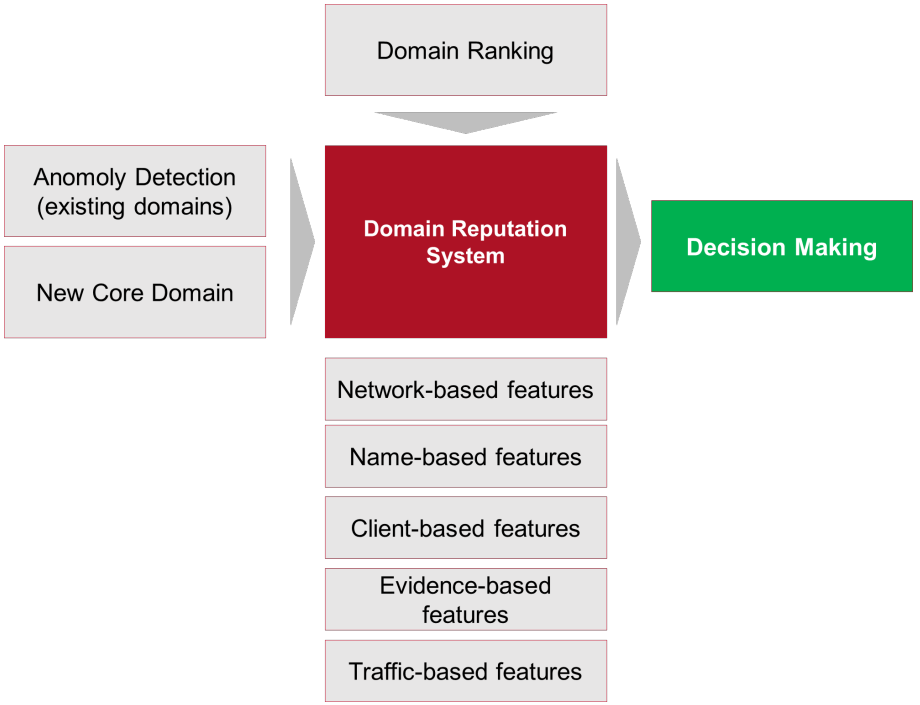
- ✓ Two anycast clouds
- ✓ Server redundancy at nodes
- ✓ Network redundancy
- ✓ Peered to Canadian IXPs
- ✓ 18 ms median DNS response time seen in NREN customers
- ✓ 13 billion queries answered per month across the service

cira

Defence in depth

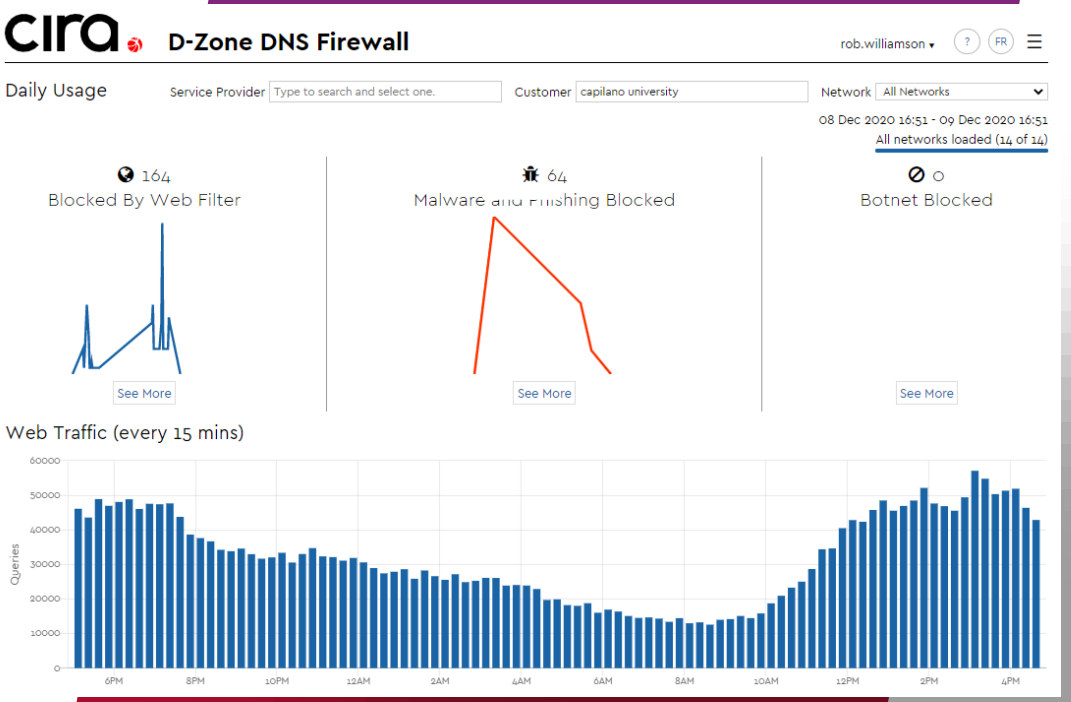
Greater than 40% of threat detection is exclusive to the CIRA DNS Firewall platform. 60% are from public and commercial feeds.

- 1 million QPS are analyzed on a global network of DNS servers
- Time from first query to the block list is < 14 mins
- On average more than 100,000 net new threats are added to the list daily



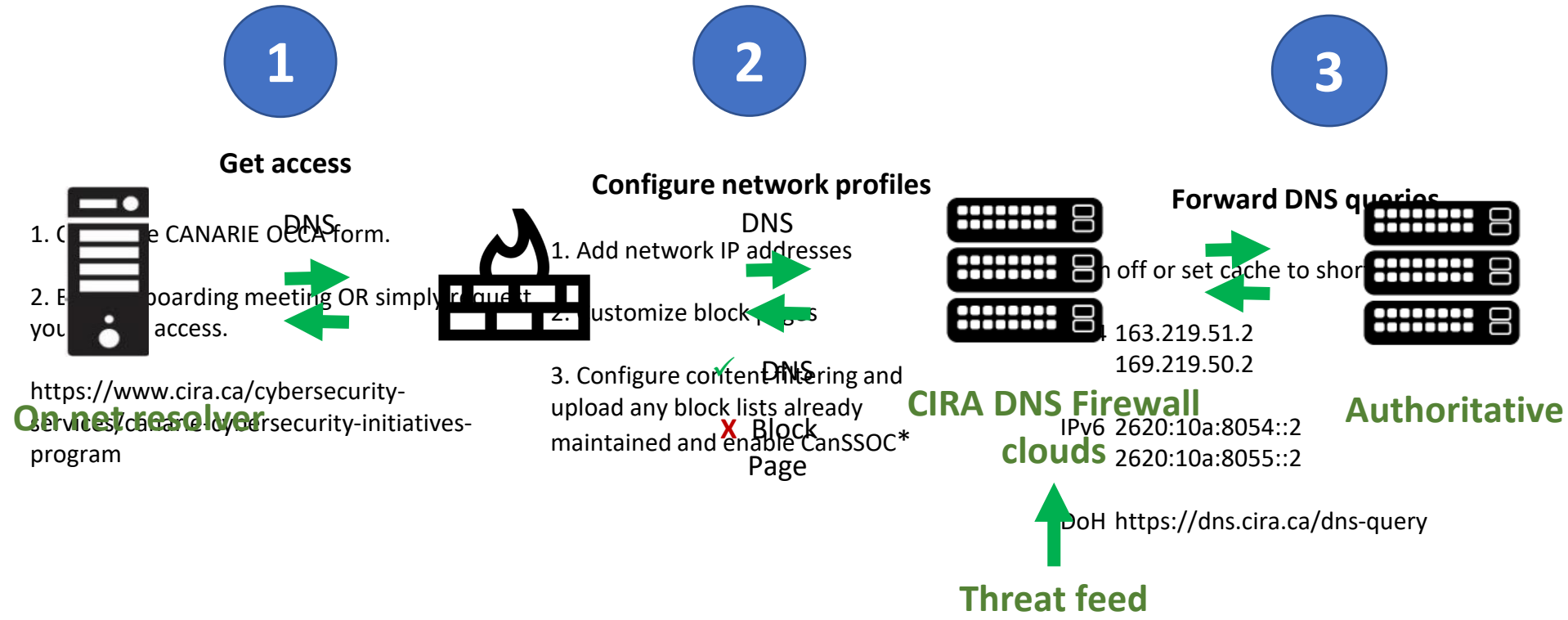
Features

- ✓ Manage multiple networks from a single portal
- ✓ Over 60 custom content filter categories plus whitelist and blacklist management
- ✓ Customizable block pages for content and malware threats
- ✓ Full API for further integration of reporting

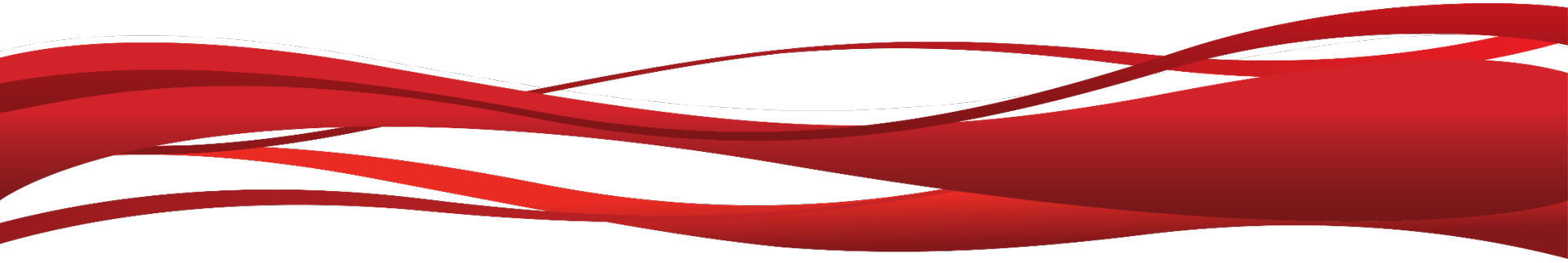


cira

Configuration



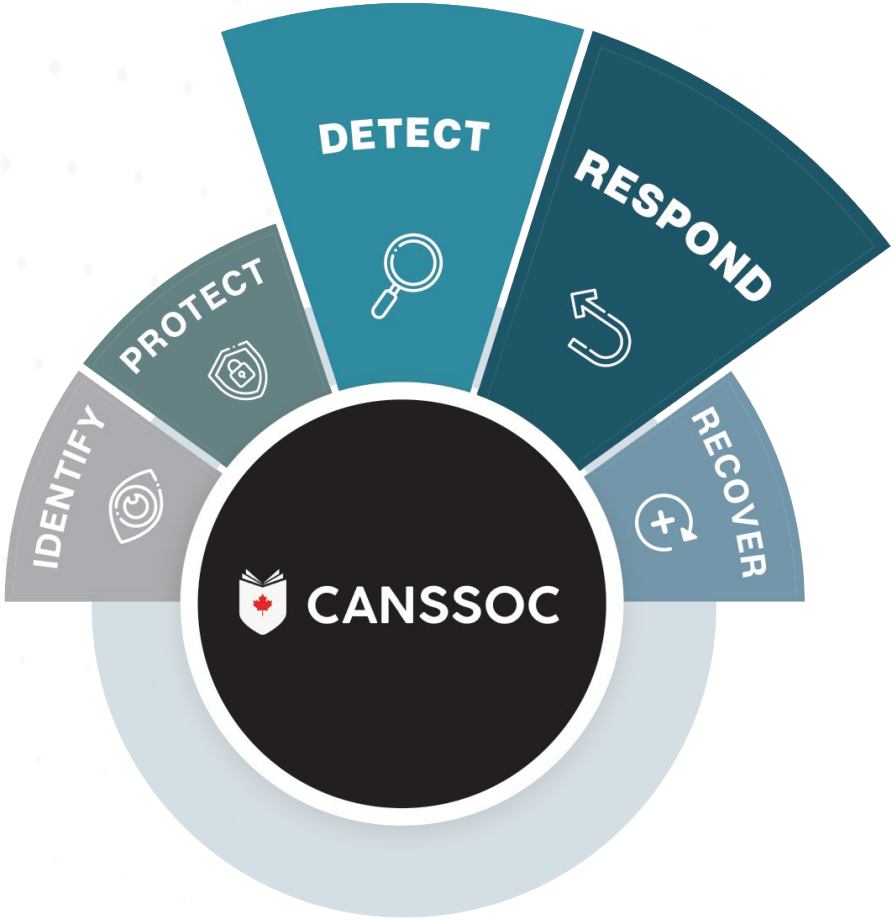
CanSSOC – Jill Kowalchuk



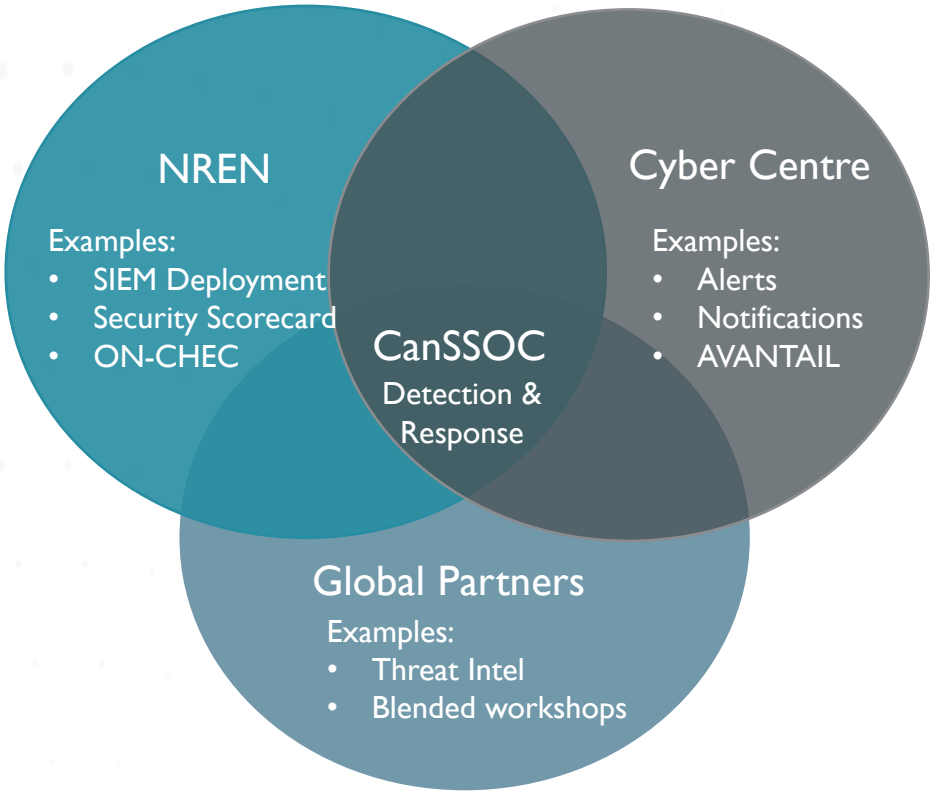
CANSSOC

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

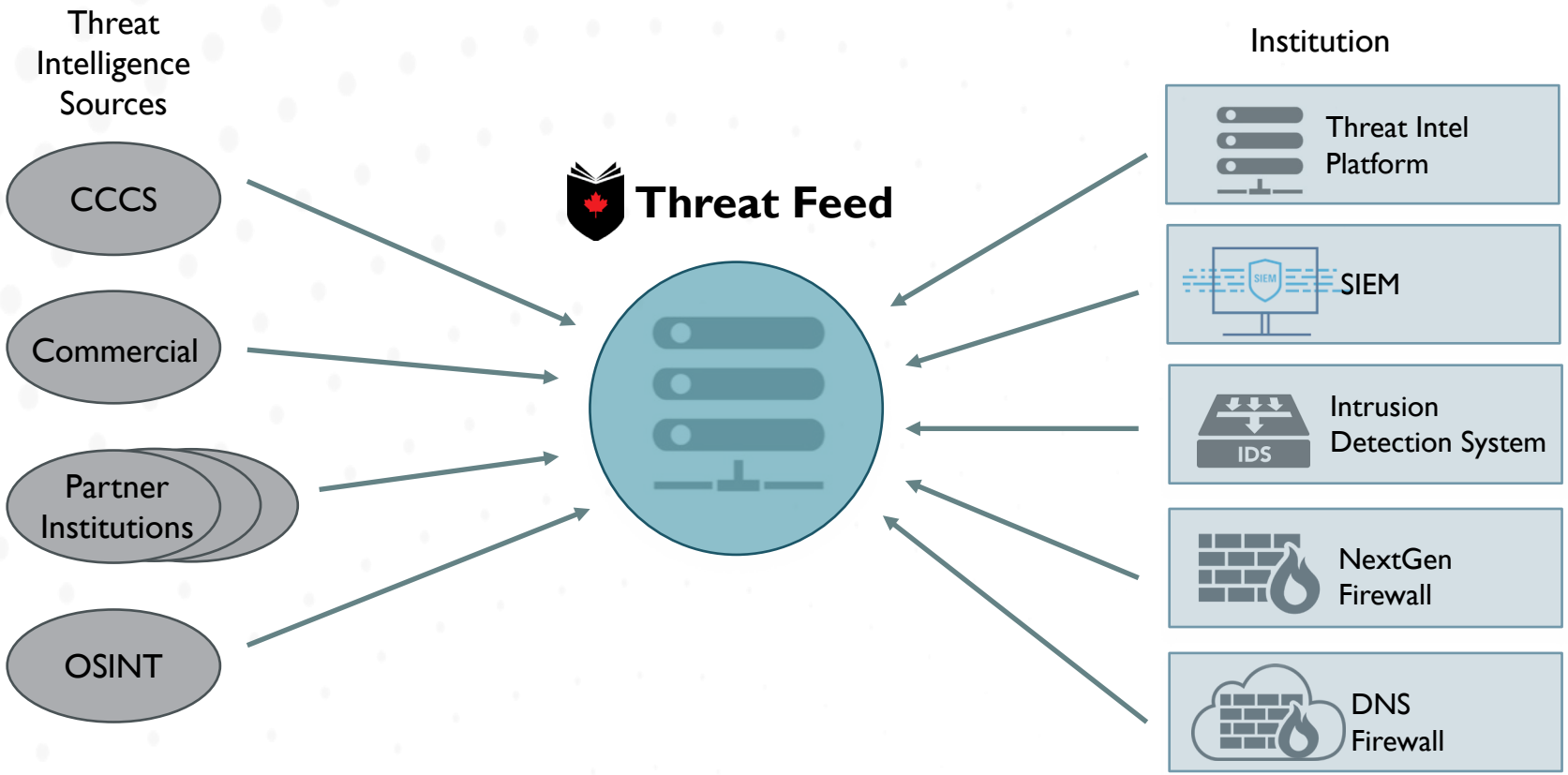
DETECTION & RESPONSE



DETECTION & RESPONSE - OPERATIONAL COORDINATION

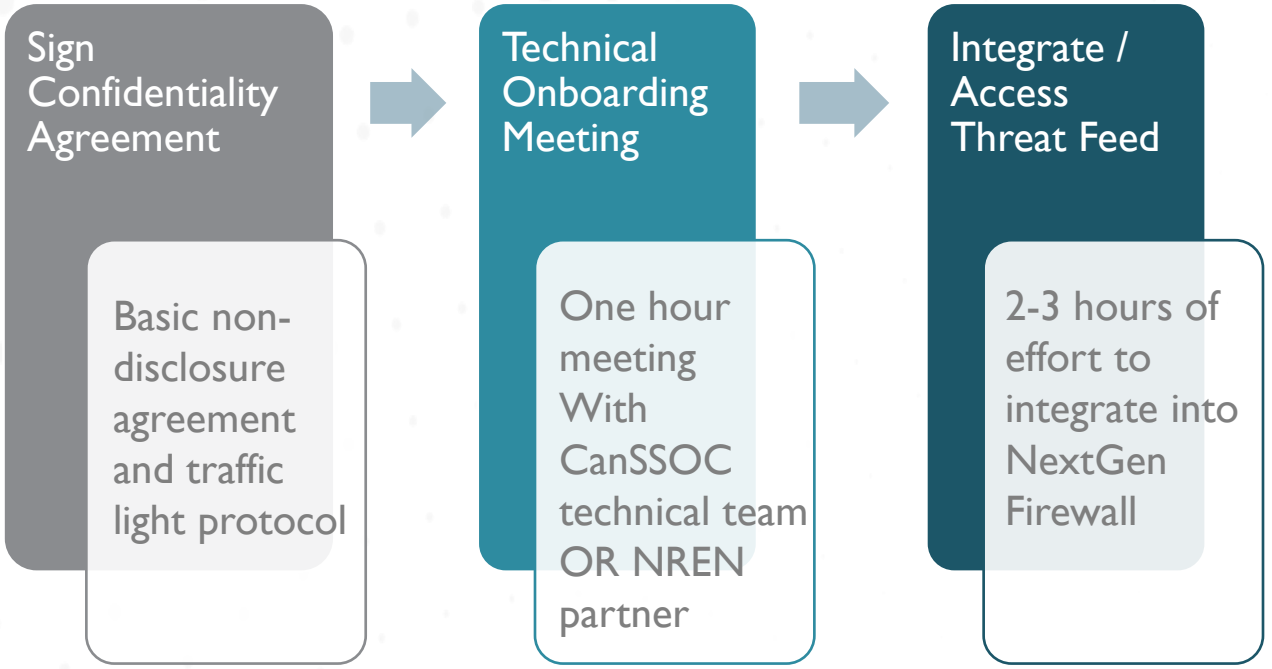


CANSSOC


Threat Intelligence Sources
CCCS
Commercial
Partner Institutions
OSINT
Threat Feed
Institution
Threat Intel Platform
SIEM
Intrusion Detection System
IDS
NextGen Firewall
DNS Firewall

CANSSOC

THREAT FEED ONBOARDING



CANSSOC

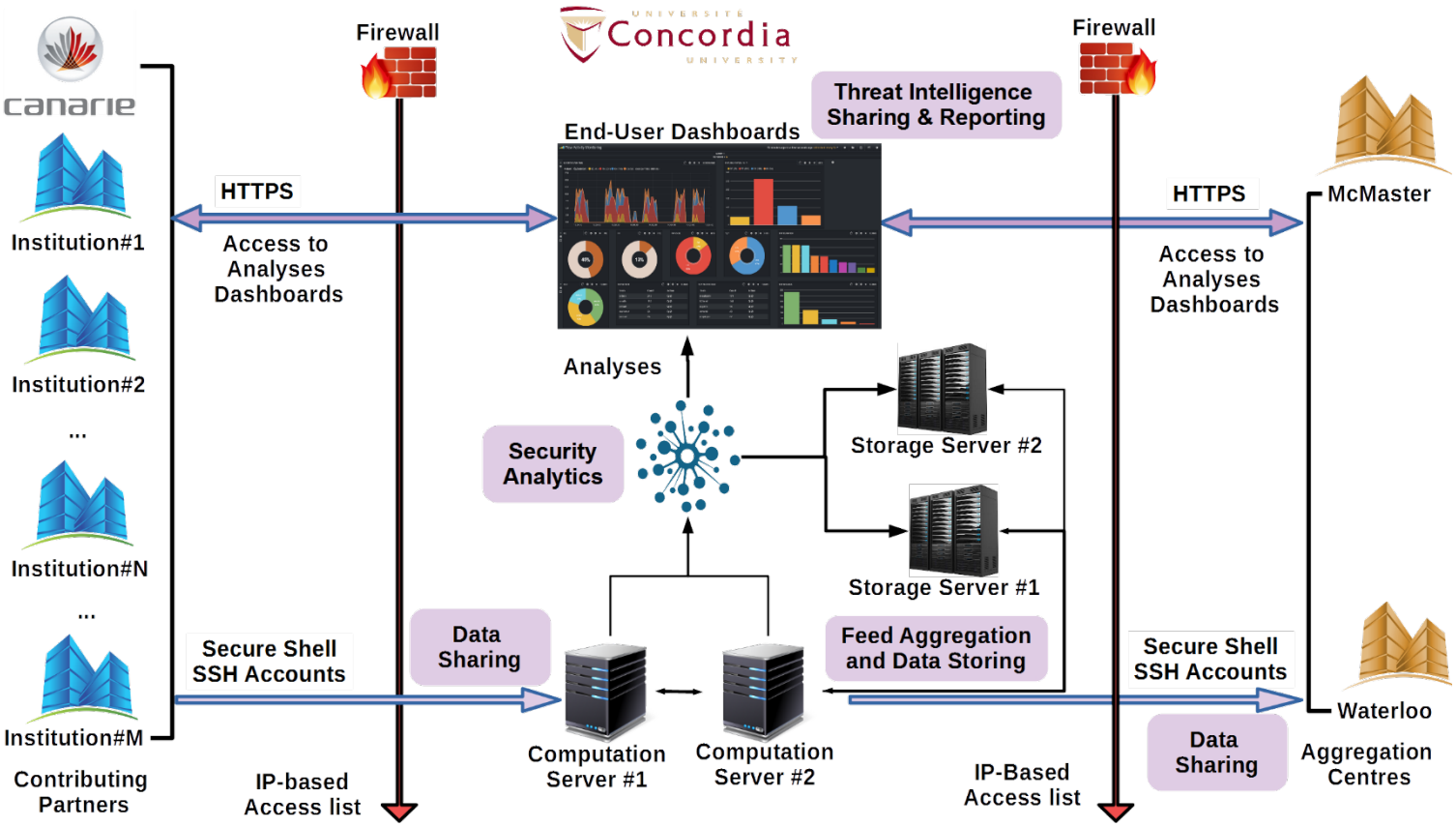
IDS – Dr. Mourad Debbabi, Concordia University

IDS – Initiative Details

- Eligible Organizations (not currently participating in JSP) will receive:
  - Server and Zeek software install
  - 2 network taps
  - Training
  - $15k of funding available for your IT staff to install, configure, and maintain the IDS hardware and software
  - Technical support (Slack channel + document portal) delivered by your NREN Partner and CANARIE
- (Current) JSP participants will continue to have analysis platform access and benefit from improvements and can enroll in the online training sessions

IDS/JSP Objectives

IDS/JSP Architecture



IDS/JSP Capabilities

Malicious Fingerprinting

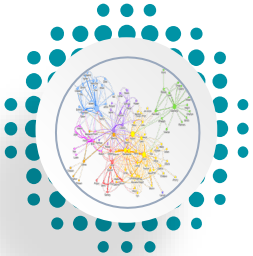
AI/ML to fingerprint malicious network behaviour

IA pour élaborer une empreinte digitale du comportement malveillant dans le réseau

Anomaly Detection

AI/ML to detect abnormal network behaviour

IA pour la détection du comportement anormal dans le réseau



Campaign Detection

Identification & tracking of attack campaigns

Identification et traçage des menaces orchestrées

pDNS Analysis

Detecting suspicious IPs or domain names

Détection des adresses IP ou des noms de domaines suspects

Threat Intel Sharing & Reporting

Generating relevant, timely and actionable intelligence

Génération des renseignements pertinentes, opportuns, et exploitable sur les menaces détectées

UNIVERSITÉ Concordia UNIVERSITY

IDS/JSP Capabilities

Vulnerability Analysis

Analysis of open and vulnerable services

Analyse des services ouverts et vulnérables

Notice Analysis

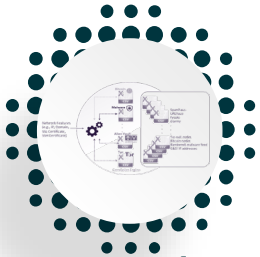
Analysis of Zeek notice logs

Analyses des logs d'alertes Zeek

Network Flow Analysis

Analysis of network flow traffic

Analyse des flux réseaux



Local Analysis

Analysis of institutional network infrastructure

Analyse de l'infrastructure du réseau institutionnelle

Risk Assessment

Quantifying the security posture

Mesurer la posture de sécurité