Cybersecurity Initiatives Program: National Alignment for Local Impact

December 15, 2020 | January 11, 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.
Presentation Overview

1. The Problem
2. The Opportunity
3. The Benefits
4. The Details
Urgency of securing research and education (R&E)

Hackers beat university cyber-defences in two hours
By Sean Coughlan
BBC News family and education correspondent

Canadian COVID-19 researchers face a growing threat of cyber-espionage
Foreign hackers are plying into COVID-19 research from around the world, and Canadian universities are not immune.
BY ANDRÉANNE APABLAZA
OCT 15 2020

Australian National University hit by huge data breach
Lisa Martin
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.
Organizations Connected to Canada’s NREN
The Vision: A More Secure Canada
National coordination for local impact

> Cooperatively developed national approach that leverages the collaborative nature of the sector

> Mitigate risks at each layer
  • End user devices
  • Organizational networks
  • NREN infrastructure
  • Sector-wide

> Build on existing initiatives

> Engage the community to govern & evolve
The opportunity:

Participate in a national, collaborative, cybersecurity program that serves Canada’s research and education sector.

Built by the community, for the community.
The collaboration of our partners has been integral to developing the approach and strategy for the program.
What is the Cybersecurity Initiatives Program?

> Government of Canada is funding CANARIE to invest in priority initiatives that will strengthen the whole R&E sector

> Funded initiatives are delivered to eligible organizations through the provincial and territorial partners in Canada’s NREN

  • Defined & prioritized by Canada’s research & education (R&E) community

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
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.
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.
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.

Your involvement is your investment.
Benefits for Canada’s R&E sector

> Strengthened security posture across the whole sector
> Mechanism to measure the program’s impact to support funding of new initiatives
> Expanded national community of security experts specialized in R&E
> National alignment on best practices for securing R&E data
How will this work?

Initiative Partners
Implement initiatives at Eligible Organizations

Research & Education Institutions
Participate in program by deploying funded initiatives & securely sharing data with counterparts

NREN Partners
Promote & administer initiatives to Eligible Organizations

Aligns & coordinates national priorities and funds initiatives

Services Fees (Funding)
Request for Service
Service Delivery
Funded initiatives are intended to integrate with each other to strengthen local cybersecurity and in turn, the overall security of the whole sector.
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 government and public sectors
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 see **1.3M threats blocked/month** or 2 blocks/network user*

* COVID-times data with fewer users and 30% fewer blocks on school networks than normal.
National DNS Firewall Vision

DNS Data
- DNS Data
- AI/ML

Cyber Research

CanSSOC
- Events Data
- Data Analysis
- Shared MISP

DNS Data/Threat Data

DNS Firewall

External Feeds

Ryerson University
McGill University
University of Alberta
University of Toronto
UBC
McMaster University

(founding CanSSOC members shown)
CANSSOC

Better than we can do on our own, always in partnership
Detection & response
Intrusion Detection System (IDS)

> Strengthens overall security by increasing awareness & understanding of institutional security issues and potential vulnerabilities

> Supports the development of a community of organizational security specialists

> Builds upon the success of the first phases of the Joint Security Project (JSP) with 137 participating organizations

> Available to the 70+ R&E organizations that are not yet participating the JSP
IDS/JSP Objectives

- Generate accurate, actionable, and timely threat intelligence
- Assess the security posture of partners and education network
- Perform risk assessment to enable mitigation
- Track threats, trends, threat actors and their infrastructures, patterns, and benchmark our security
IDS/JSP Capabilities – Capacités

- **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
IDS/JSP Capabilities - Capacités

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
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
Is there a deadline?

> 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.

> Funding for the Cybersecurity Initiatives Program continues to March 31, 2024.
More Information

Implementation-focused Webinar:

The Cybersecurity Initiatives Program: What It Could Mean for Your Organization

• December 16, 2020: 12 – 1 p.m. ET
• January 12, 2021: 1 – 2 p.m. ET

canarie.ca/cybersecurity
Governance & Measurement
Cybersecurity Advisory Committee & Standing Committees

**Cybersecurity Advisory Committee**
- Guidance on advancing national cybersecurity collaborations
- Advice on overall CANARIE program strategy, evolution, and intended outcomes

**Trust and Identity Committee**
Guidance on the evolution of sector-wide identity management services, including Canadian Access Federation

**Cybersecurity Technical Committee**
Guidance and recommendations on specific cybersecurity technical aspects that have an impact on CANARIE initiatives

**Cybersecurity Initiatives Deployment Committee**
Feedback and information on institutional operations to support effective program design, execution, and adoption

**Cybersecurity Measurement and Metrics Working Group**
Cybersecurity Program Governance

- CANARIE Board of Directors
- CANARIE Management
- Cybersecurity Advisory Committee
  - Trust and Identity Committee
  - Cybersecurity Technical Committee
  - Cybersecurity Initiatives Deployment Committee
- Cybersecurity Measurement and Metrics Working Group
- Cybersecurity Investment Framework Project
• Funnel of new issues and/or initiatives identified by community for evaluation

• Compliance reporting and next steps

• Ongoing measurement and evaluation

CAC, Standing Committees, CANARIE Board

NREN Partners and Initiative Partners

Eligible Organizations, CANARIE, MM WG

Identify Priorities
Implement Solutions
Report Outcomes
Measure Impacts