Le programme Initiatives en cybersécurité
Ce qu'il pourrait apporter à votre organisation

16 décembre 2020 | 12 janvier 2021

Aperçu de la présentation

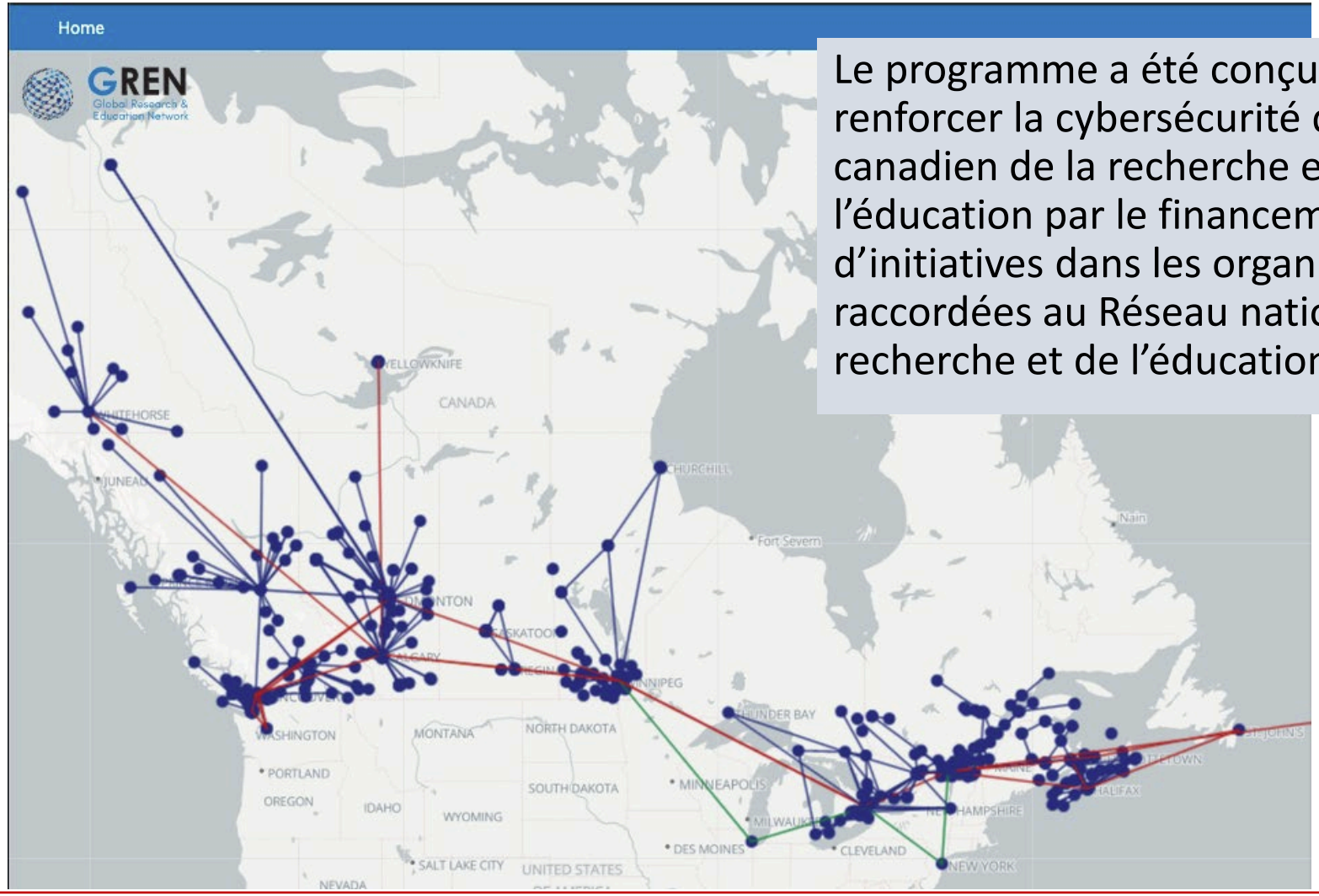
1. Le programme Initiatives en cybersécurité (PIC)
2. Comment participer
3. Les trois premières initiatives
4. Période de questions

Une réalité collective

- Nous sommes tous connectés, que ce soit physiquement ou par la collaboration.
- Chaque organisation, chaque dispositif connecté est susceptible d'être piraté.
- Cette connectivité fait en sorte que la chaîne est aussi solide que son maillon le plus faible.
- La cybersécurité n'est pas qu'un problème IT : c'est une priorité de l'organisation.
- Une approche nationale en cybersécurité n'est réalisable que si le secteur entier s'harmonise et coordonne ses efforts.

Une fois sécurisé, le secteur sera plus solide que la somme de ses parties.

Le programme Initiatives en cybersécurité (PIC)



Le programme a été conçu pour renforcer la cybersécurité du secteur canadien de la recherche et de l'éducation par le financement d'initiatives dans les organisations raccordées au Réseau national de la recherche et de l'éducation.

Terminologie

RNRE

- Réseau national de la recherche et de l'éducation – réseau pancanadien mis en place par CANARIE et ses partenaires provinciaux et territoriaux

Partenaire du RNRE

- Un des treize partenaires provinciaux et territoriaux du RNRE, plus CANARIE, le partenaire fédéral

Partenaire de l'initiative

- Organisation chargée de mettre à exécution une initiative subventionnée dans le cadre du programme (par ex., ACEI ou CanSSOC)

Organisation admissible (OA)

- Organisation pouvant bénéficier des initiatives financées dans le cadre du programme Initiatives en cybersécurité

Que fait le PIC?

> Il finance et met à exécution des initiatives qui renforceront la cybersécurité dans les OA.

> Exemples

- Dispositifs sécurisant le réseau interne de l'OA
- Services en nuage mettant les employés de l'OA, les enseignants et les étudiants à l'abri des cybermenaces
- Diffusion d'informations sur les nouvelles menaces
- Formation
- Autres

Avantages pour l'organisation

> Élargir l'infrastructure de cybersécurité
> Jauger l'impact des initiatives en cybersécurité au sein de votre organisation
> Collaborer avec un bassin national de spécialistes en sécurité du secteur R-E
> Renforcer les compétences et l'expertise de l'équipe de sécurité de l'organisation : le programme comprend un volet formation et soutien technique

Sécuriser l'organisation davantage

Gratuitement

Exécution de l'initiative

> Nous collaborons avec nos partenaires du RNRE pour mettre les initiatives en œuvre dans les organisations admissibles (OA).

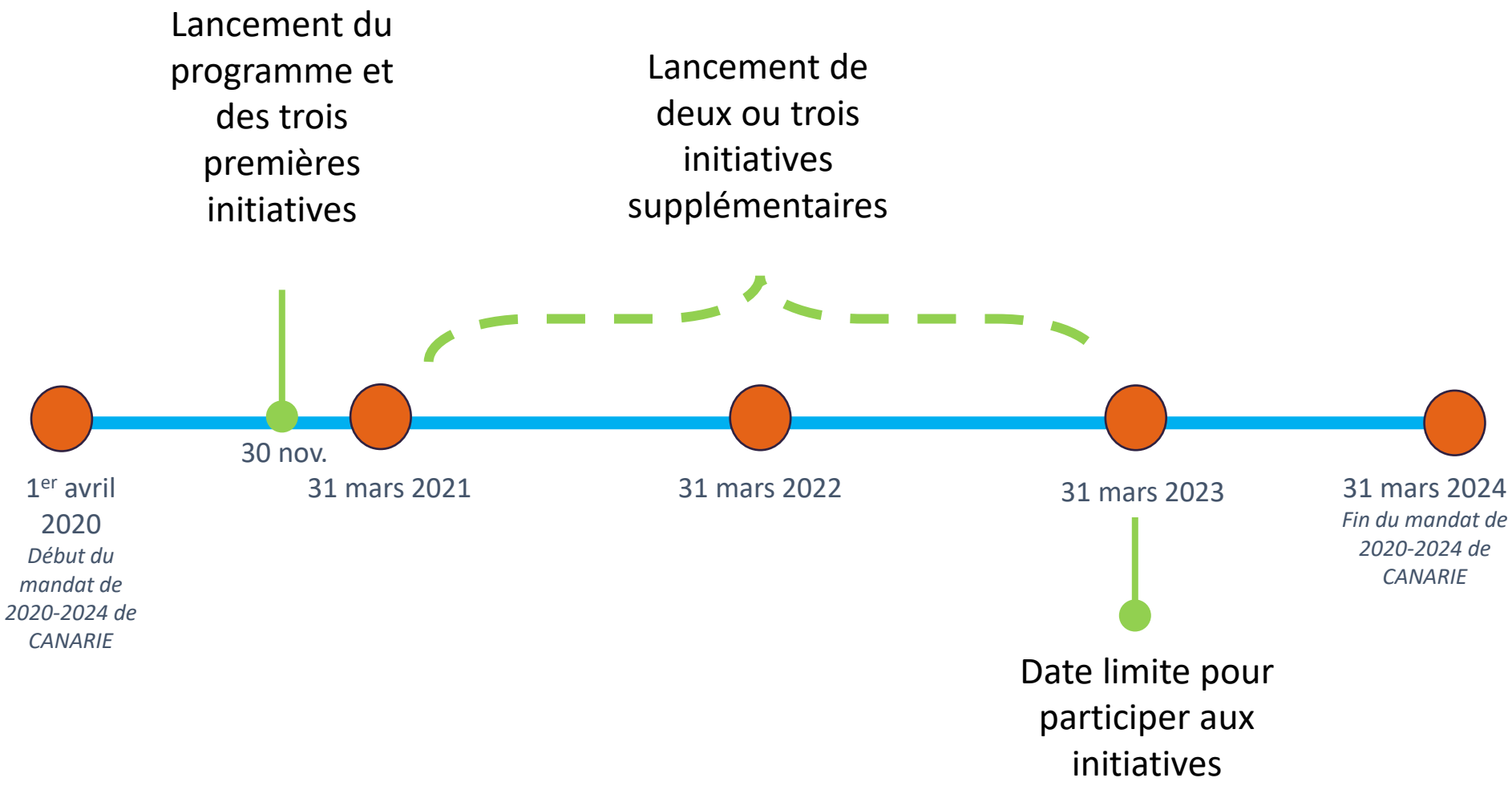
> Le partenaire du RNRE est le contact principal pour participer à l'initiative.

- Soutien supplémentaire fourni par l'équipe de cybersécurité de CANARIE

> La participation au programme ou l'accès aux initiatives subventionnées ne suscite aucun coût direct pour l'OA.

> Pas de frais généraux pour l'organisation; le plus souvent, le partenaire de l'initiative est financé directement par CANARIE.

Déroulement du programme



Qui choisit les initiatives qui seront financées?

La mobilisation et la participation de la communauté commandent tous les éléments du programme, mais surtout, sa gouvernance.

Commission consultative en cybersésurité

Elle se compose de chefs de file des universités, collèges, écoles polytechniques, cégeps, organismes sans but lucratif et organisations privées du Canada.

Rôle

- Prôner une approche nationale coordonnée à la cybersésurité dans le secteur R-E
- Orienter les initiatives financées dans le cadre du programme

Choix d'une initiative

- L'initiative est validée d'après un jeu de facteurs commun.
  - Efficacité
  - Possibilité d'une vaste application
  - Temps requis pour le déploiement
  - Coût abordable
  - Durabilité
- Autres paramètres pris en compte
  - Coordination nationale
  - Quantification des retombées

Les trois premières initiatives

cira

D-ZONE DNS FIREWALL

Financement de la mise en œuvre, du soutien et de la formation dans plus de 200 organisations admissibles

CANSSOC Threat Feed

Financement de la mise en œuvre, du soutien et de la formation dans plus de 200 entreprises admissibles

Intrusion Detection System *(Join the JSP)*

Financement de la mise en œuvre, du soutien et de la formation dans les organisations admissibles non inscrites au Projet conjoint en sécurité (PCS)

Les initiatives subventionnées sont conçues pour s'intégrer et renforcer la cybersécurité localement, ce qui rendra l'ensemble du secteur plus sûr.

Comment participer

Critères d'admissibilité

Pour participer au PIC, l'organisation doit respecter les critères que voici.

1. Elle doit être connectée au Réseau national de la recherche et de l'éducation (RNRE) du Canada.
2. Elle doit adhérer à un des partenaires du RNRE ET y être connectée au moyen d'un réseau autonome.
3. Elle doit être une institution d'enseignement supérieur, une installation de recherche non fédérale ou un centre d'excellence.

Certaines initiatives pourraient avoir des critères d'admissibilité bien à elles. Ces critères seront clairement établis au lancement de l'initiative.

Obligations du participant

- Habituellement, prévoir du temps pour que le personnel concourent au déploiement et à l'exécution de l'initiative

- Fournir des données sur l'initiative qui a été déployée par l'organisation jusqu'en mars 2024

- Remettre un court rapport après le déploiement de l'initiative

Comment participer

1. Des représentants des partenaires provinciaux et territoriaux du RNRE inviteront les organisations admissibles à participer au programme.
   - Veuillez prendre contact avec le partenaire du RNRE de votre province ou territoire pour vérifier votre admissibilité.

2. Organisation admissible
   - Elle soumet un court formulaire d'inscription à CANARIE.
   - Elle signe l'Entente de collaboration en cybersécurité avec une organisation (ECCO).

3. Après ratification de l'ECCO, votre partenaire du RNRE vous indiquera comment accéder à l'initiative subventionnée.
   - L'ECCO ne doit être exécuté qu'une seule fois.

Questions que vous pourriez vous poser…

Doit-on mettre en œuvre toutes les initiatives subventionnées?

> Non. Vous choisissez celles qui conviennent le mieux à l'organisation. Néanmoins, on vous demandera la raison pour laquelle vous ne voulez pas y participer afin de faciliter la planification des initiatives futures.

Les initiatives ont-elles pour but de remplacer les initiatives existantes?

> Non. L'idée est de faire en sorte que toutes les organisations admissibles connectées au RNRE disposent des mêmes technologies, des procédés et des compétences de base en cybersécurité.

> Les initiatives du PIC visent à combler les lacunes qui pourraient exister et à procurer les outils et les processus complémentaires à ceux en place.

Questions que vous pourriez vous poser…

Y a-t-il une date limite pour participer au programme?

> L'organisation admissible peut participer en tout temps, mais elle n'aura accès aux initiatives subventionnées qu'après avoir signé l'ECCO.

> Plus tôt l'organisation participera, plus longtemps elle profitera des initiatives subventionnées.

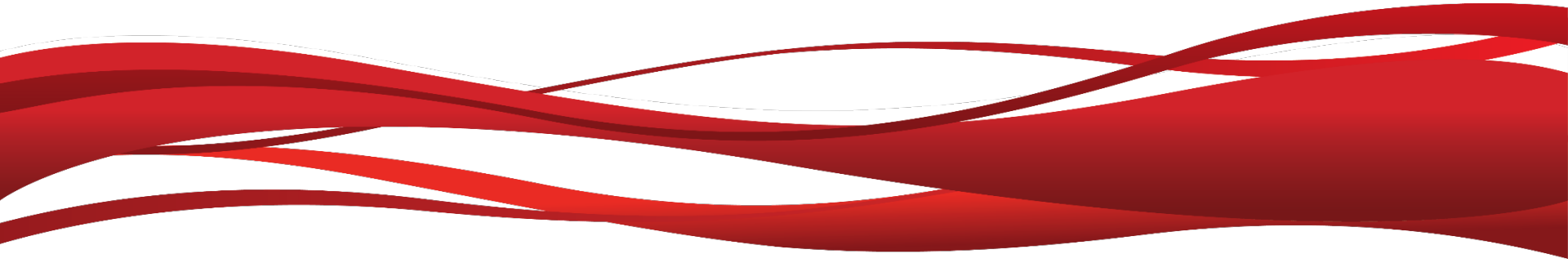
> Date limite de participation aux initiatives subventionnées : 31 mars 2023

> Le financement du PIC se poursuivra jusqu'au 31 mars 2024.

Voici les trois premières initiatives

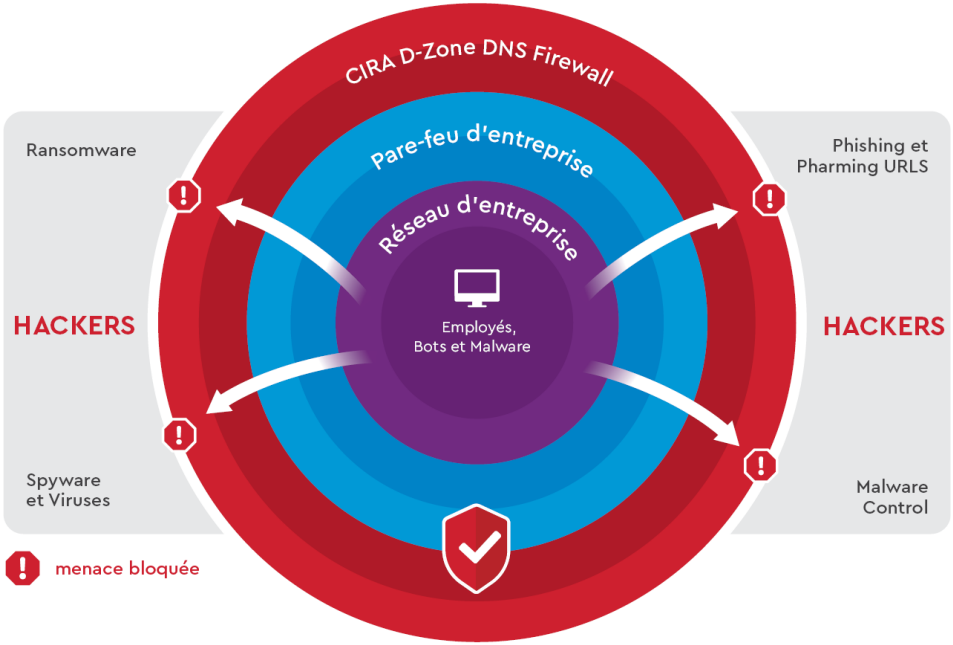
Intrusion
Detection
System
(Join the JSP)

CIRA – Mark Gaudet



Pare-feu DNS de l'ACEI

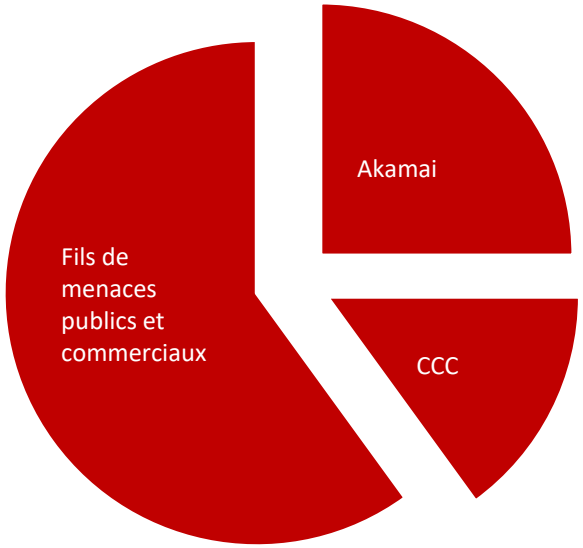
- ✓ Couche extérieure à l'organisation qui assure une protection très efficace contre les logiciels malveillants, les tentatives d'hameçonnage et les réseaux de zombies
- ✓ Déjà déployé dans 57 institutions de recherche et d'enseignement du Canada
- ✓ Plus de 2 millions d'utilisateurs canadiens dans les organismes gouvernementaux et publics



Ce qu'offre le pare-feu DNS de l'ACEI

Un service DNS de haute performance au taux de blocs cinq fois plus élevé que celui des autres services similaires du secteur public.

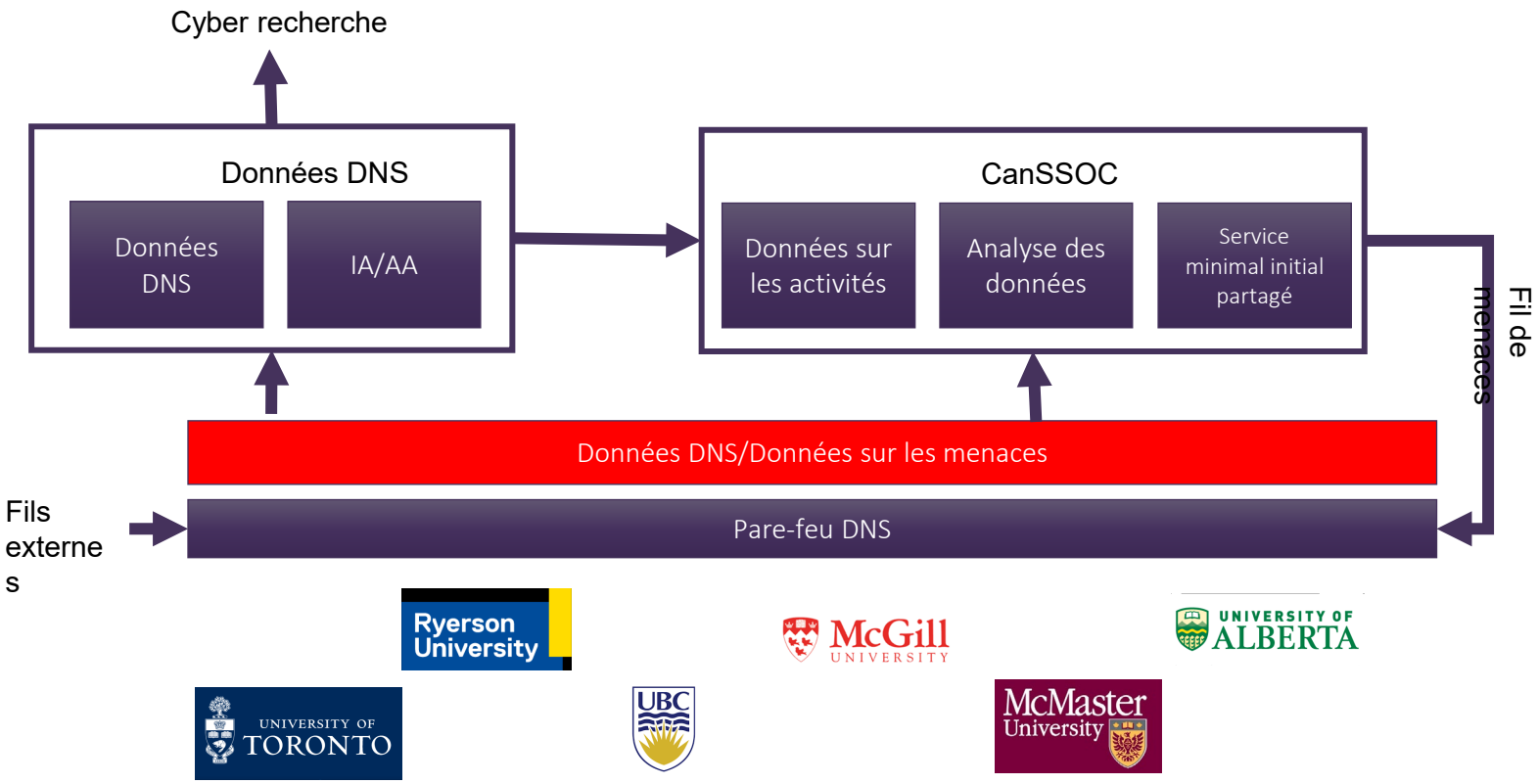
- ✓ Service DNS de première qualité répondant à 13 milliards de demandes par mois avec un **temps de réponse médian de 18 ms** – meilleur que celui de Google 888.
- ✓ En moyenne, au-delà de **100 000 nouvelles menaces s'ajoutent** à la liste de blocage chaque jour
- ✓ **1,3 M de menaces bloquées par mois** sur les RNRE ou 2 blocages par utilisateur du réseau*



Sources du blocage des menaces

- Données durant la pandémie. Nombre de blocages 30 % plus bas que la normale sur les réseaux scolaires.

Vision d'un pare-feu DNS national



(membres fondateurs du CanSSOC)

CIRA DNS Firewall

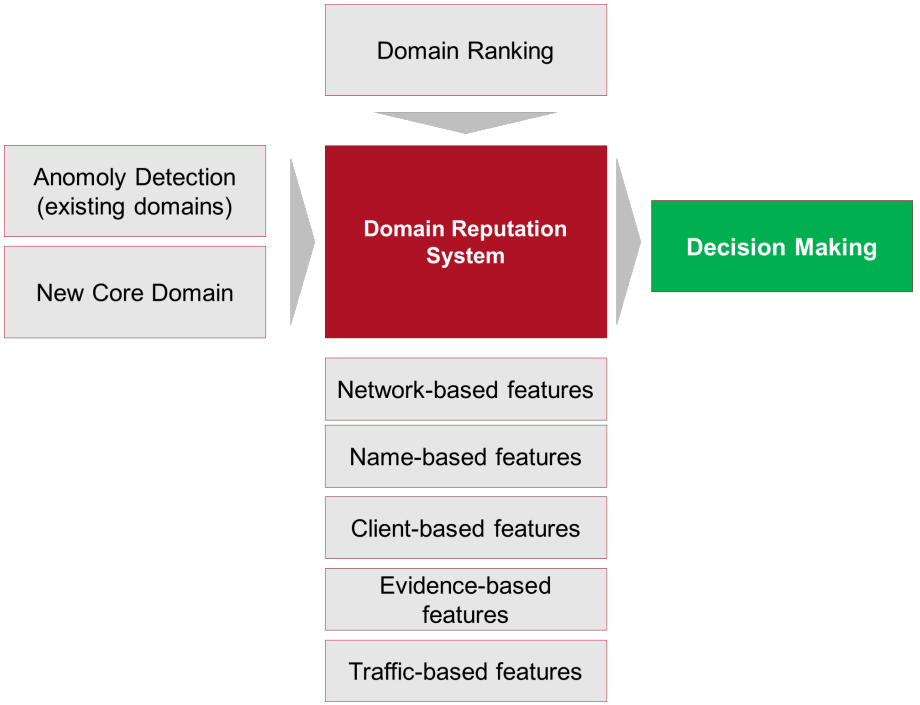
Architecture

- ✓ Deux nuages à unidiffusion aléatoire
- ✓ Serveurs redondants aux nœuds
- ✓ Redondance du réseau
- ✓ Appairage avec les IXP canadiens
- ✓ Temps de réponse DNS médian de 18 ms pour les clients du RNRE
- ✓ Réponses à 13 milliards de demandes par mois

Système de défense

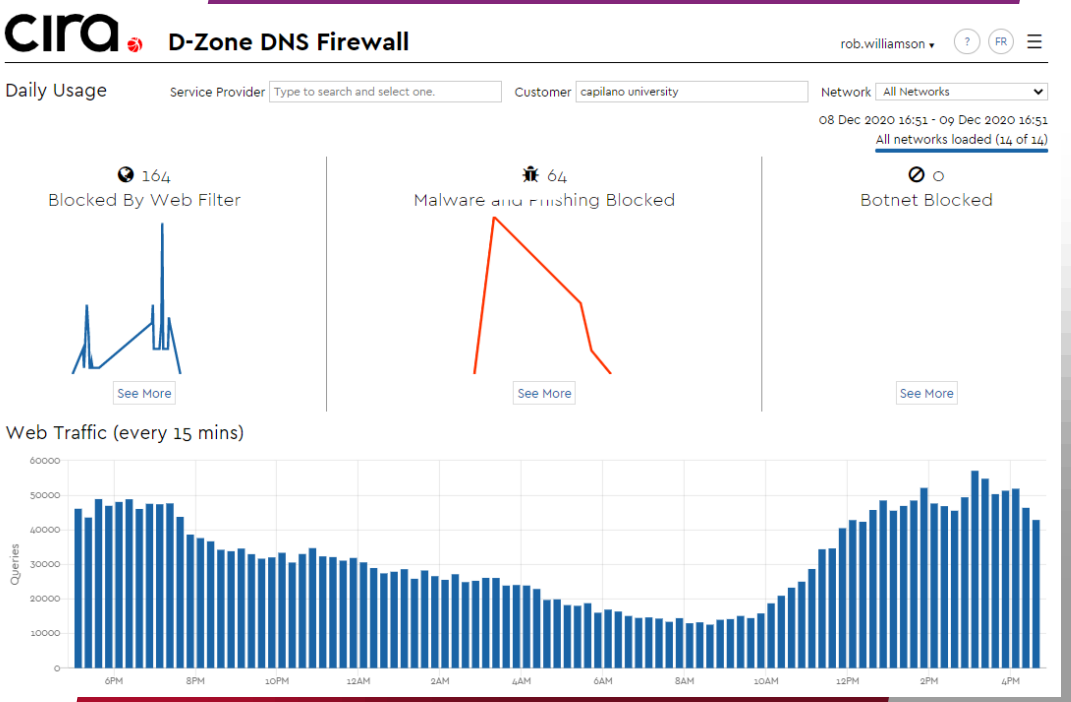
Plus de 40 % des menaces détectées le sont exclusivement par le pare-feu DNS de l'ACEI; les autres (60 %) sont détectées par les fils publics et commerciaux.

- Analyse d'un million de demandes par seconde sur un réseau mondial de serveurs DNS
- Intervalle inférieur à 14 minutes entre la demande initiale et l'ajout à la liste de blocage
- En moyenne, plus de 100 000 nouvelles menaces ajoutées chaque jour à la liste



Particularités

- ✓ Gestion de nombreux réseaux à partir du même portail
- ✓ Plus de 60 catégories de filtres spéciaux pour le contenu ainsi que gestion des listes blanche et noire
- ✓ Blocs de page adaptables en fonction du contenu et des logiciels malveillants
- ✓ API complète pour une meilleure intégration des rapports



Configuration

1

Obtenir l'accès

1. Remplir le formulaire de l'ECCO de CANARIE.

2. Prendre rendez-vous pour une séance d'information OU demander simplement l'accès au portail

https://www.cira.ca/cybersecurity-services/canarie-cybersecurity-initiatives-program

2

Configurer le profil du réseau

1. Ajouter les adresses IP du réseau

2. Adapter les blocs de page

3. Configurer le filtrage du contenu et téléverser les listes d'adresses bloquées existantes ainsi qu'activer CanSSOC*

3

Envoyer les demandes DNS

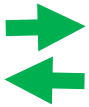
1. Désactiver ou régler l'antémémoire pour raccourcir les délais

2. IPv4 163.219.51.2
169.219.50.2

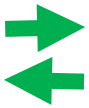
IPv6 2620:10a:8054::2
2620:10a:8055::2

DoH https://dns.cira.ca/dns-query

DNS

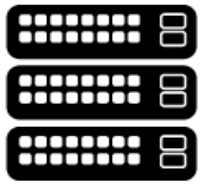


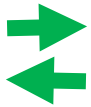
DNS

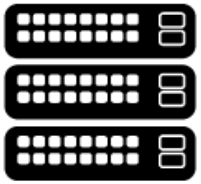


✓ DNS

X Block de page







Résolveur sur le réseau

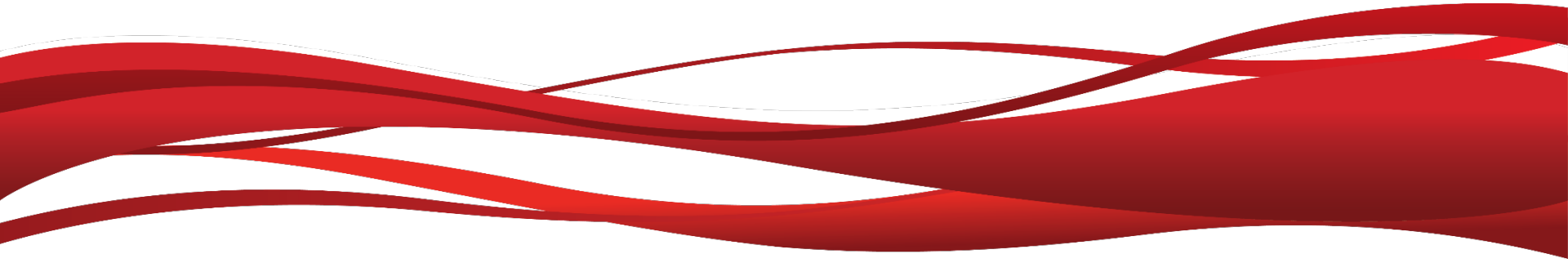
Nuages du pare-feu DNS de l'ACEI

Vérification

Fil de menaces

cira

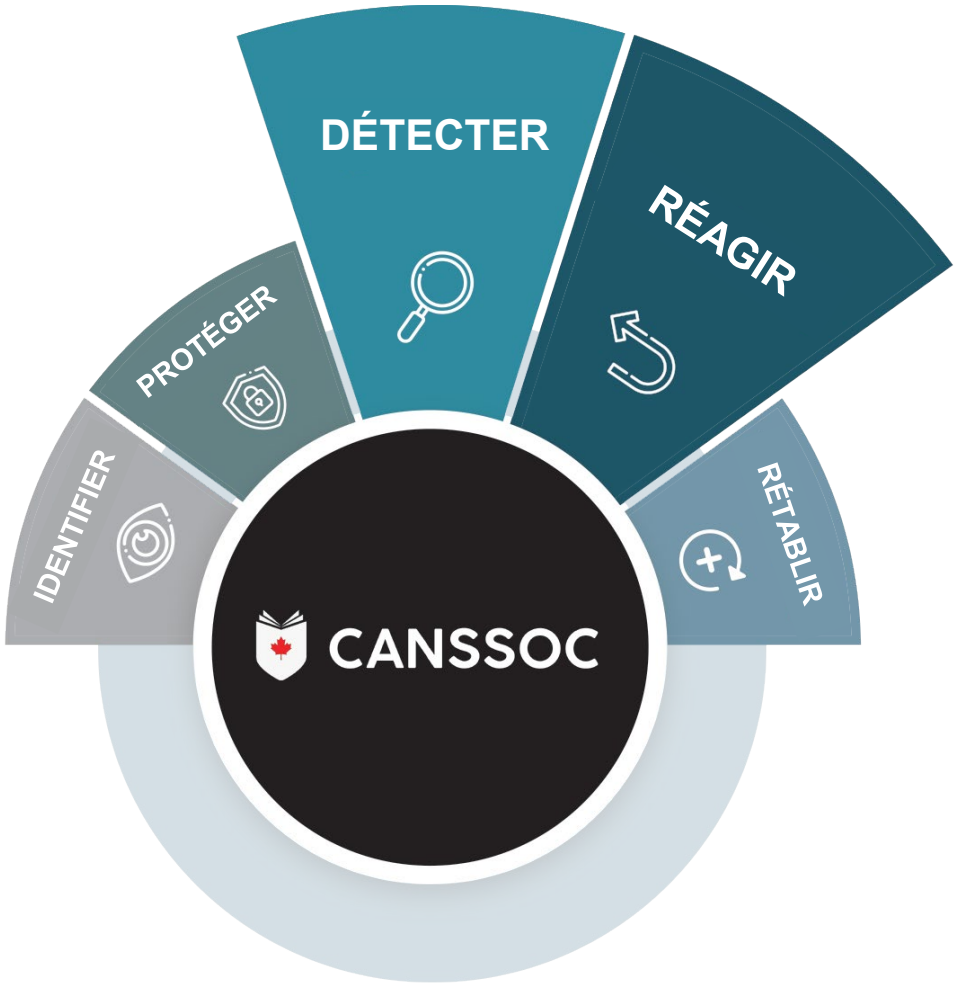
CanSSOC – Jill Kowalchuk



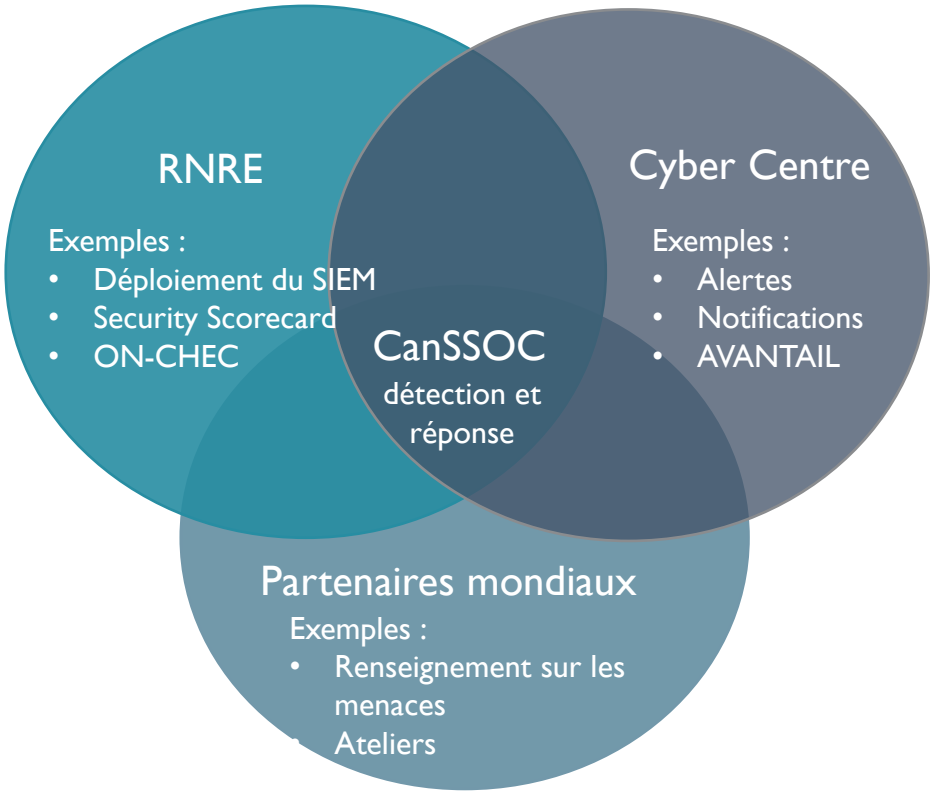
CANSSOC

Mieux que ce qu'il est possible d'accomplir chacun pour soi, et toujours en partenariat.

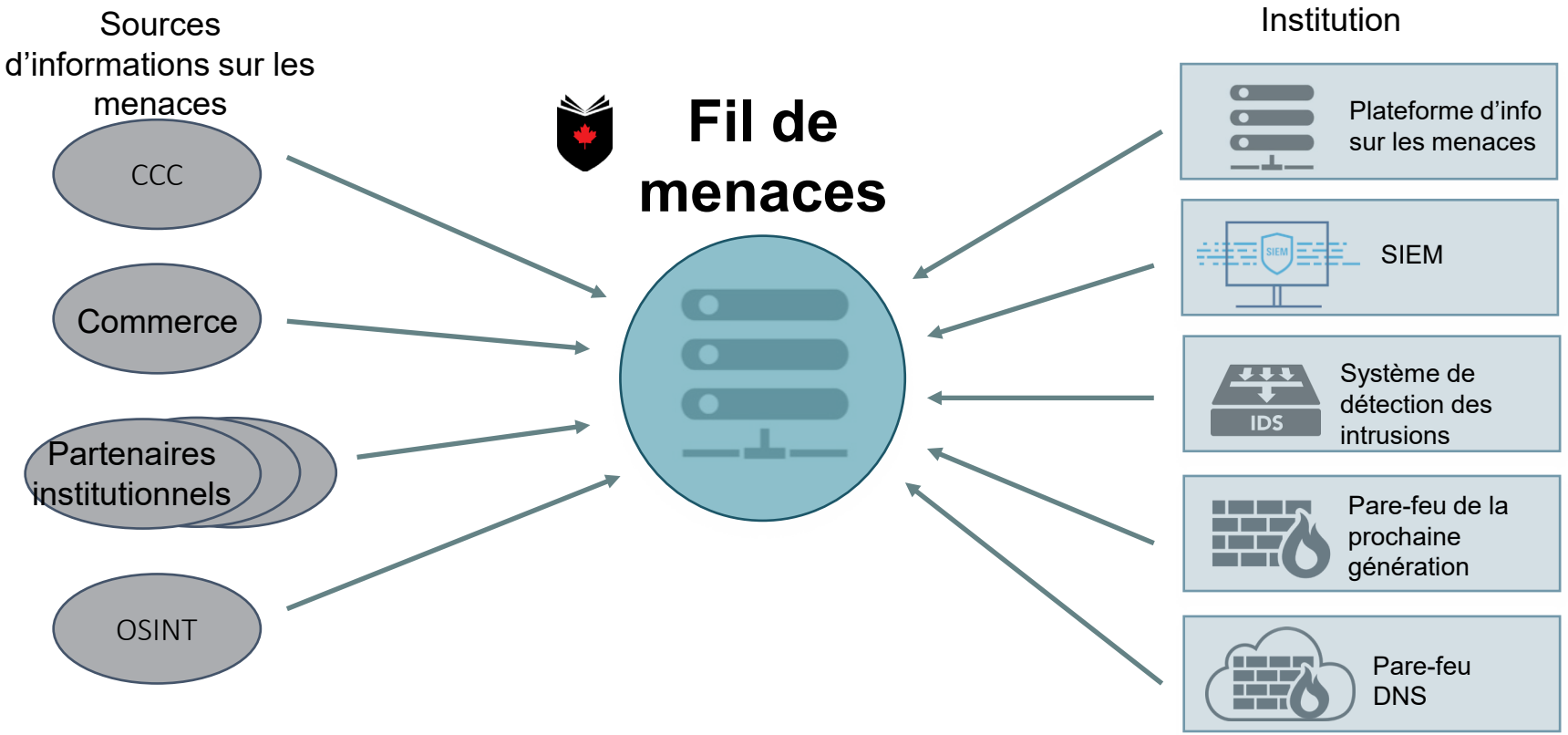
DÉTECTION ET RÉPONSE



COORDINATION OPÉRATIONNELLE DE LA DÉTECTION ET DE LA RÉPONSE

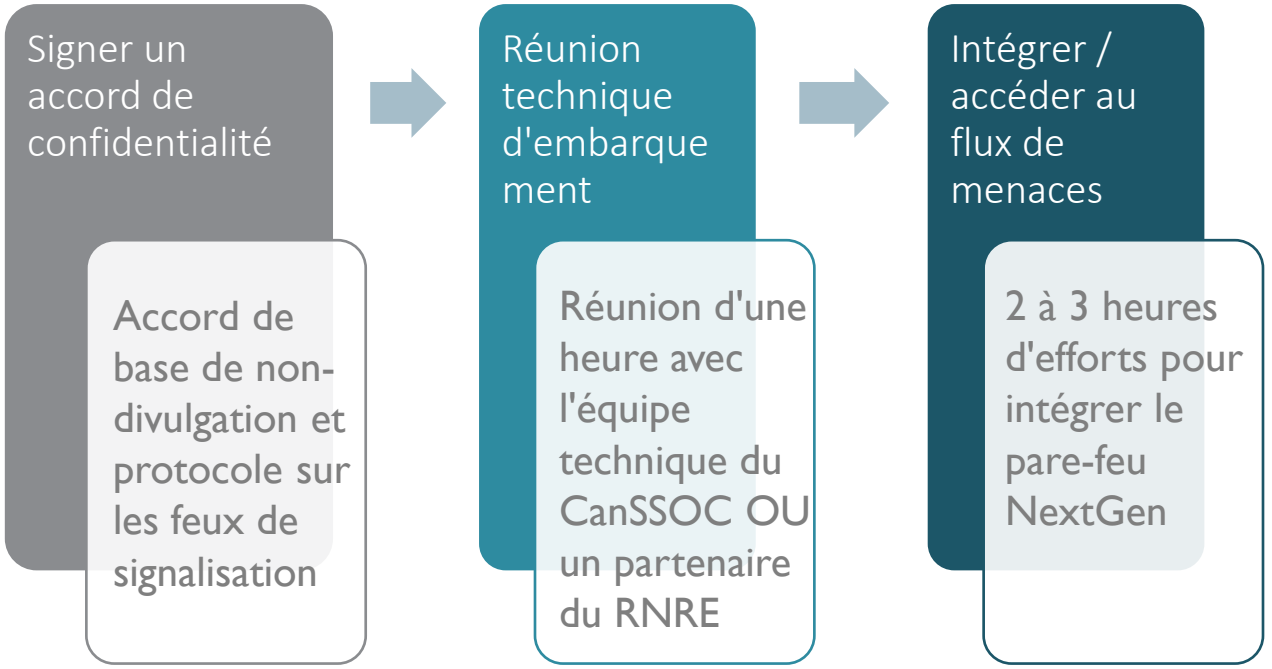


CANSSOC


Sources d'informations sur les menaces
CCC
Commerce
Partenaires institutionnels
OSINT
Fil de menaces
Institution
Plateforme d'info sur les menaces
SIEM
Système de détection des intrusions
IDS
Pare-feu de la prochaine génération
Pare-feu DNS

CANSSOC

Threat feed onboarding



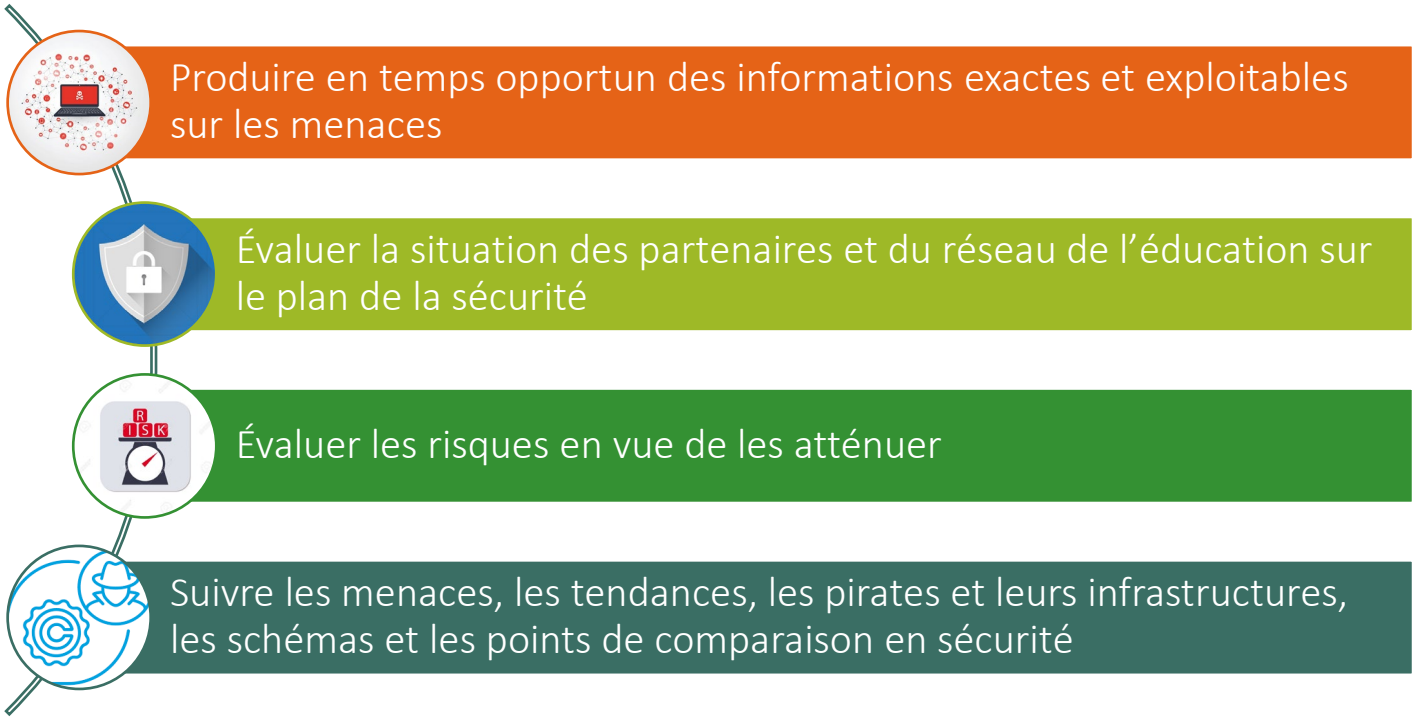
IDS – Dr. Mourad Debbabi, Concordia University

IDS – Détails de l'initiative

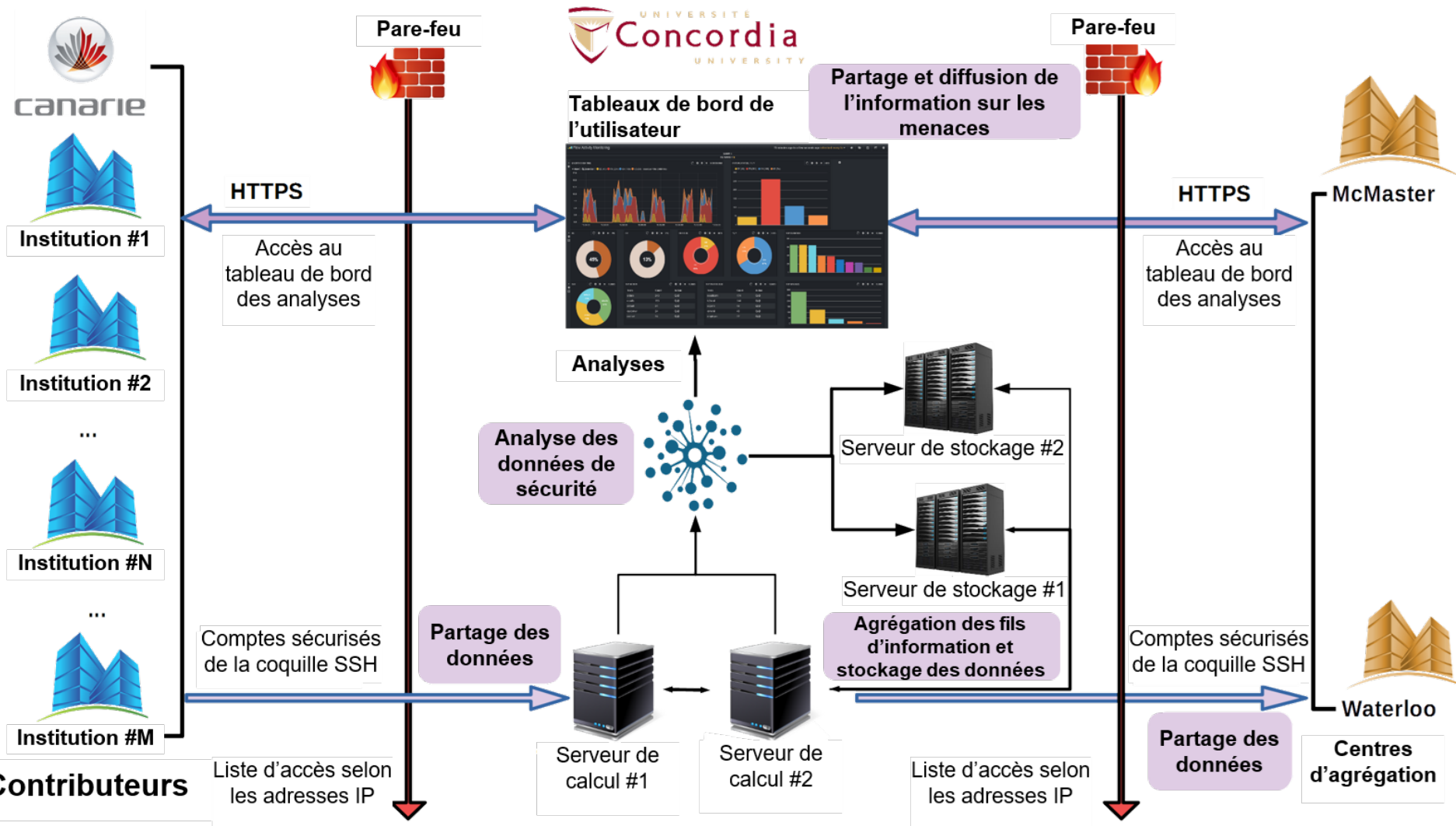
> Les organisations admissibles (qui ne participent pas encore au Projet conjoint en sécurité - PCS) recevront ce qui suit :
  - un serveur et le logiciel Zeek, installé;
  - 2 points d'accès terminaux au réseau;
  - de la formation;
  - 15 000 $ pour que son personnel IT installe, configure et maintienne l'équipement et le logiciel du système de détection des intrusions (IDS);
  - le soutien technique (canal Slack et portail hébergeant la documentation) du partenaire du RNRE de leur province ou territoire et de CANARIE

> Les institutions qui participent déjà au PCS continueront d'avoir accès aux plateformes d'analyse, profiteront des perfectionnements qui y sont apportés et pourront s'inscrire aux séances de formation en ligne.

Objectifs de l'IDS du PCS



Architecture de l'IDS du PCS



Concordia UNIVERSITY

Capacités de l'IDS du PCS

Analyse des vulnérabilités

Analyse des services ouverts et vulnérables

Analyse des alertes

Analyse des journaux d'alerte Zeek

Analyse des flux réseau

Analyse des flux réseau

Analyse locale

Analyse de l'infrastructure du réseau institutionnel

Évaluation des risques

Quantification de la situation sur le plan de la sécurité

Capacités de l'IDS du PCS

Analyse des vulnérabilités

Analyse des services ouverts et vulnérables

Analyse des alertes

Analyse des journaux d'alerte Zeek

Analyse des flux réseau

Analyse des flux réseau

Analyse locale

Analyse de l'infrastructure du réseau institutionnel

Évaluation des risques

Quantification de la situation sur le plan de la sécurité