Programme Initiatives en cybersécurité : *S'harmoniser à l'échelon national, pour un plus grand impact local*

15 décembre 2020

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.

Aperçu de la présentation

1. Le problème
2. La possibilité
3. Les avantages
4. Les précisions

Urgence de sécuriser les milieux de la recherche et de l'éducation (R-E)

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future | Mo

NEWS

Home | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Enterta

Family & Education

Hackers beat university cyber-defences in two hours

By Sean Coughlan
BBC News family and education correspondent

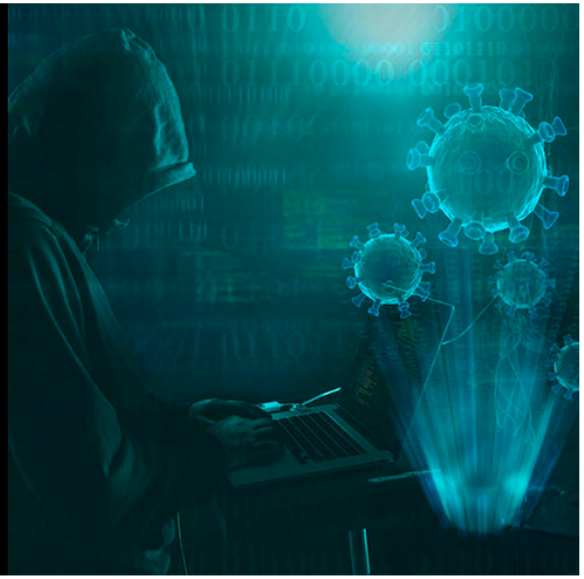
UAAU University Affairs Affaires universitaires

News | Opinion | Features | Career Advice | Subscribe | Magazine | Search Jobs

Canadian COVID-19 researchers face a growing threat of cyber-espionage

Foreign hackers are prying into COVID-19 research from around the world, and Canadian universities are not immune.

BY ANDRÉANNE APABLAZA
OCT 15 2020



Search jobs | Sign in | Search | The Guardian | International edition

News | Opinion | Sport | Culture

World ▸ Europe US Americas Asia Australia Middle East Africa Inequality Citie

Australian National University hit by huge data breach

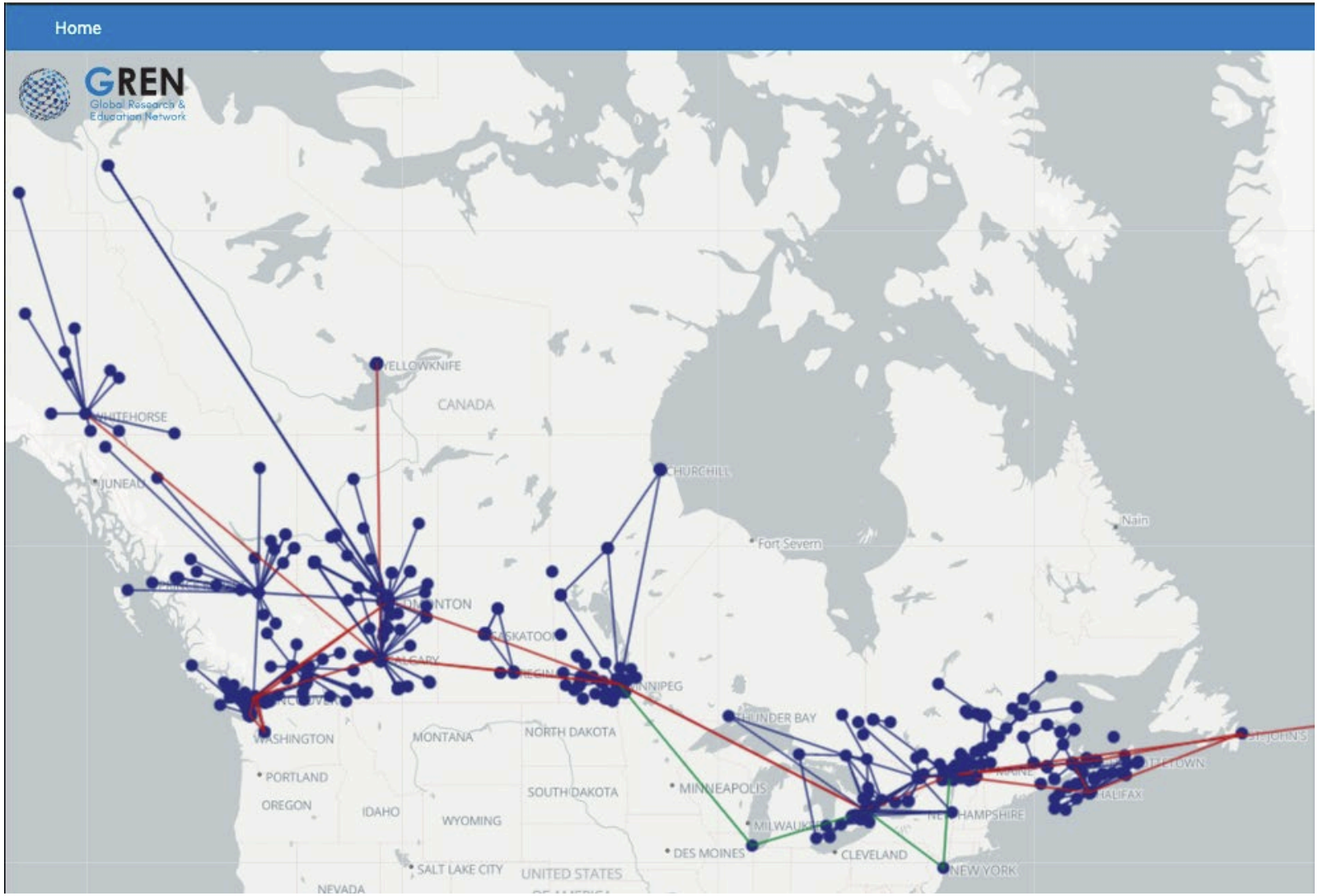
Lisa Martin
@LMARTI

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.

Organisations connectées au RNRE canadien



La vision : un Canada plus sûr

Se coordonner à l'échelon national pour un plus grand impact à l'échelon local

- Élaborer en commun une approche nationale qui tirera parti de la nature collaborative naturelle du secteur
- Atténuer les risques à chaque palier
  - Dispositifs de l'utilisateur
  - Réseau de l'organisation
  - Infrastructure du RNRE
  - Ensemble du secteur
- Profiter des initiatives en cours
- Mobiliser la communauté pour maîtriser la situation et évoluer

La possibilité

Participer à un programme de cybersécurité national articulé sur la collaboration qui répondra aux besoins des milieux canadiens de la recherche et de l'éducation

Forgé par la communauté, pour la communauté

La collaboration de nos partenaires est indissociable de l'approche et de la stratégie élaborées pour le programme.

Qu'est-ce que le programme Initiatives en cybersécurité?

- Le gouvernement du Canada finance CANARIE pour qu'il investisse dans des initiatives prioritaires qui renforceront le secteur R-E dans son ensemble.
- L'exécution des initiatives subventionnées dans les organisations admissibles sera confiée aux partenaires provinciaux et territoriaux du RNRE canadien.
  - Les initiatives seront définies et priorisées par les milieux canadiens de la recherche et de l'éducation (R-E).

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

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

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

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

Votre seul investissement : participer

Avantages pour le secteur R-E canadien

> Ensemble du secteur plus sûr

> Mécanisme permettant de quantifier l'impact du programme en vue du financement de nouvelles initiatives

> Plus vaste communauté nationale d'experts en sécurité spécialisés dans le secteur R-E

> Uniformisation des pratiques exemplaires en sécurisation des données R-E dans tout le pays

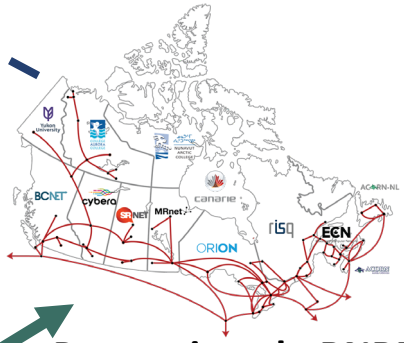
Fonctionnement

Institutions de recherche et d'enseignement

Elles participent au programme en déployant les initiatives subventionnées et en partageant leurs données de façon sécuritaire avec leurs contreparties.

Partenaires de l'initiative

Ils mettent l'initiative en œuvre dans les organisations admissibles.



Partenaires du RNRE

Ils promeuvent et administrent les initiatives auprès des organisations admissibles.

canarie

Il harmonise et coordonne les priorités nationales et finance les initiatives.

Coût des services (financement)

Demande de service

Prestation du service

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

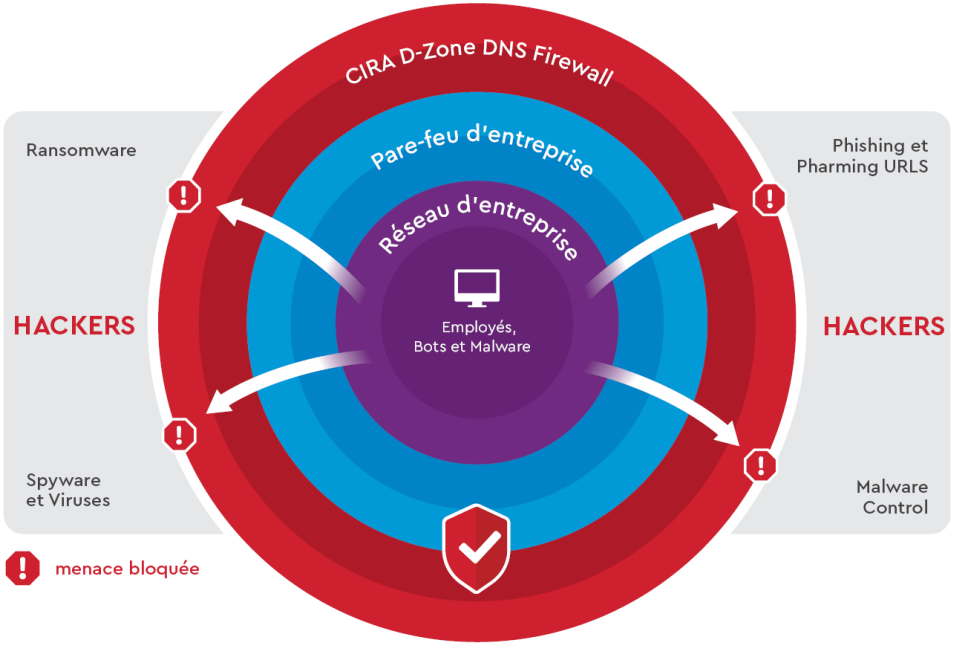
Intrusion Detection System *(Join the JSP)*

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.

Pare-feu DNS de l'ACEI

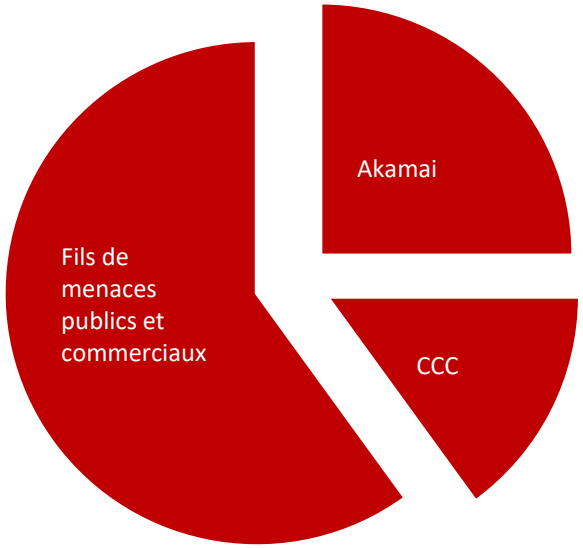
- ✓ Couche extérieure à l'organisation qui assure une protection très efficace contre les logiciels malveillants, les tentatives d'hameçonnage et les réseaux de zombies
- ✓ Déjà déployé dans 57 institutions de recherche et d'enseignement du Canada
- ✓ Plus de 2 millions d'utilisateurs canadiens dans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

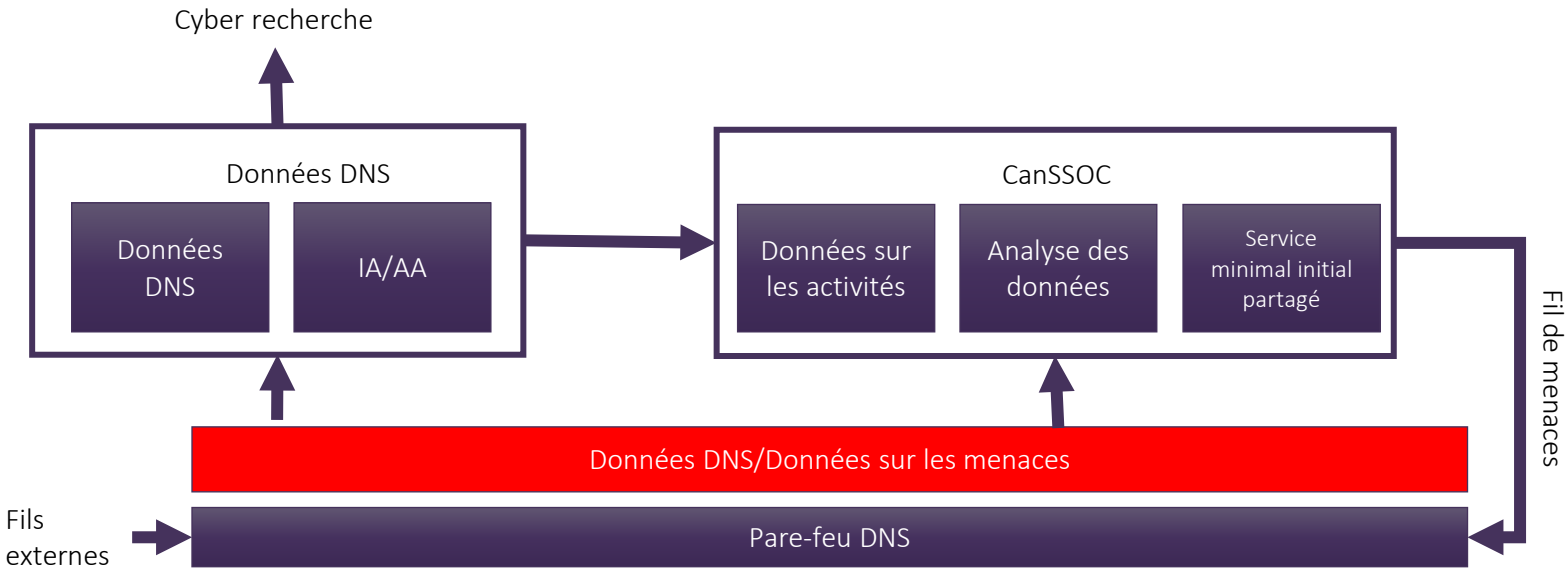
- ✓ Service DNS de première qualité répondant à 13 milliards de demandes par mois avec un **temps de réponse médian de 18 ms** – meilleur que celui de Google 888.
- ✓ En moyenne, au-delà de **100 000 nouvelles menaces s'ajoutent** à la liste de blocage chaque jour
- ✓ **1,3 M de menaces bloquées par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

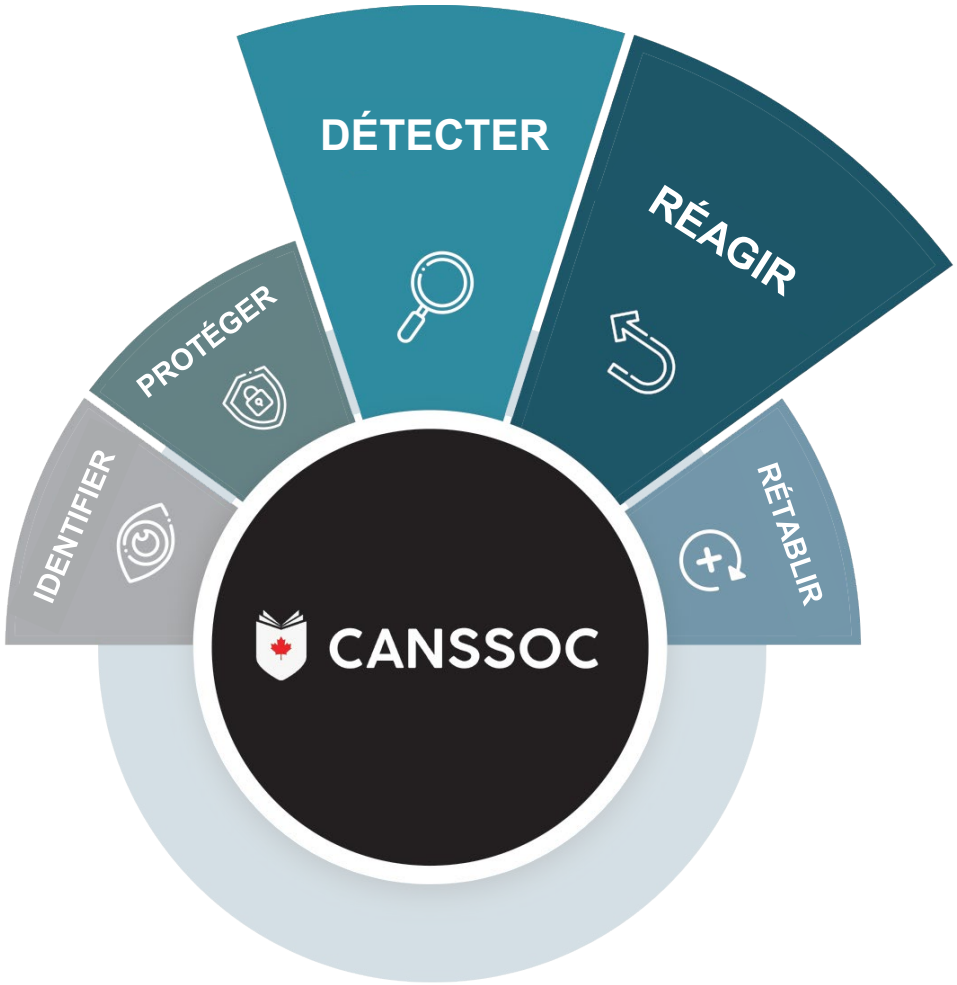


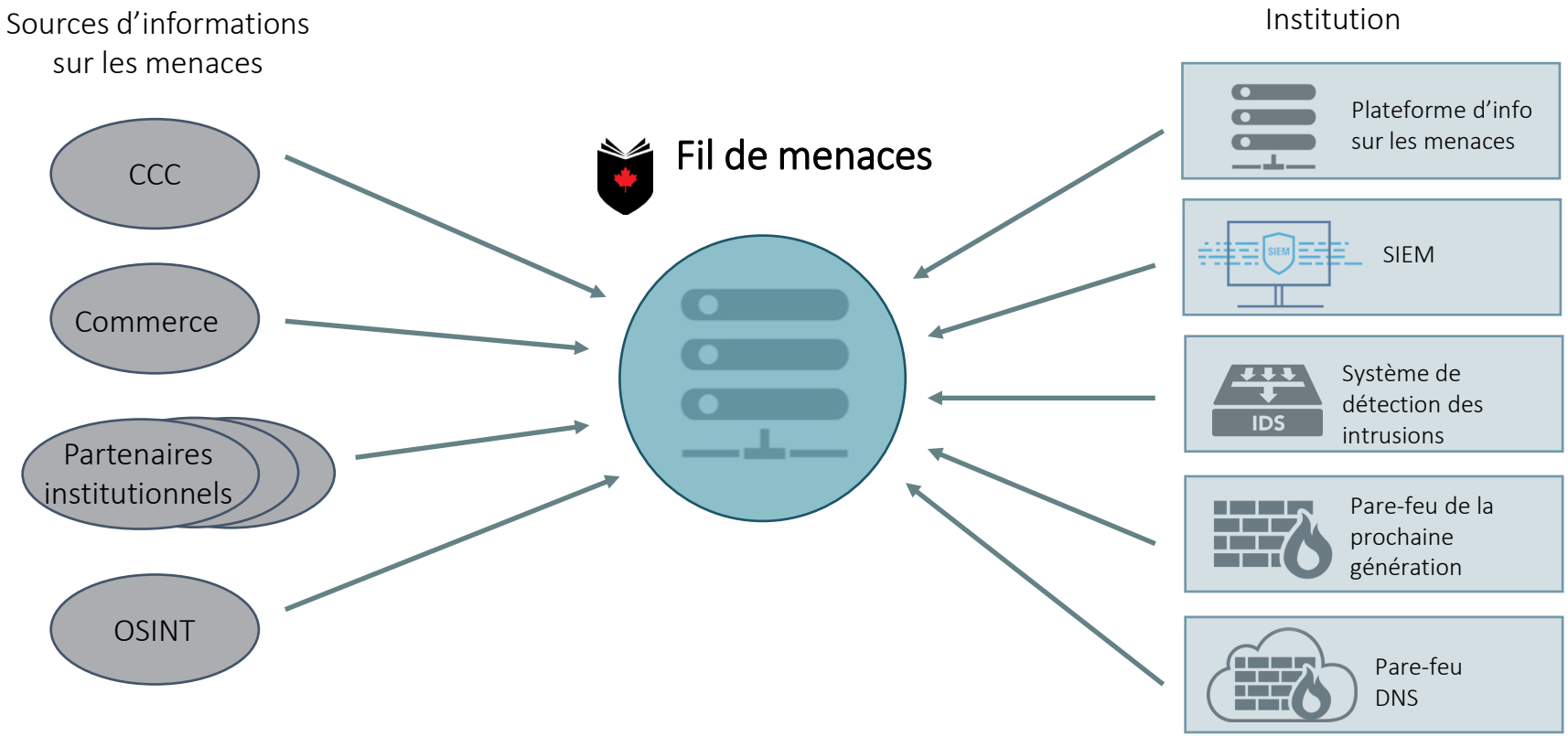
(membres fondateurs du CanSSOC)

CANSSOC

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

détection et réaction




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

Système de détection des intrusions (IDS)

Intrusion
Detection
System

- Renforce la sécurité générale en augmentant la sensibilisation et la compréhension des questions de sécurité institutionnelle et des vulnérabilités potentielles
- Soutient le développement d'une communauté de spécialistes de la sécurité organisationnelle
- S'appuie sur le succès des premières phases du Projet conjoint en sécurité (PCS) avec 137 organisations participantes
- Disponible pour les plus de 70 organisations de R-E qui ne participent pas encore au PCS

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.

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

> 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.

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

En savoir plus

> Webinaire sur la mise en œuvre

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

- 16 décembre 2020 : 12 h – 13 h HE
- 12 janvier 2021 : 13 h – 14 h HE

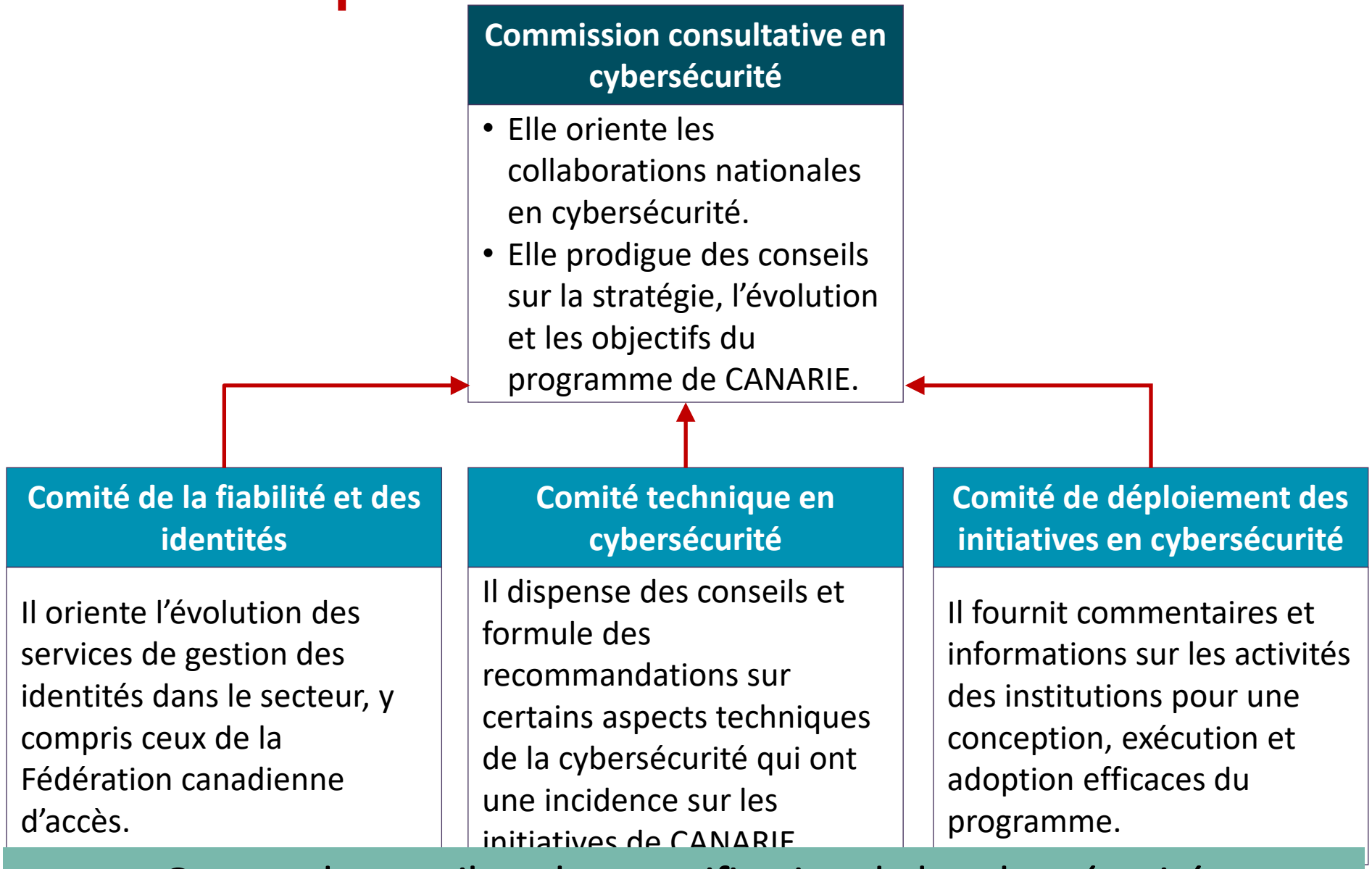
canarie.ca/cybersecurite

canarie

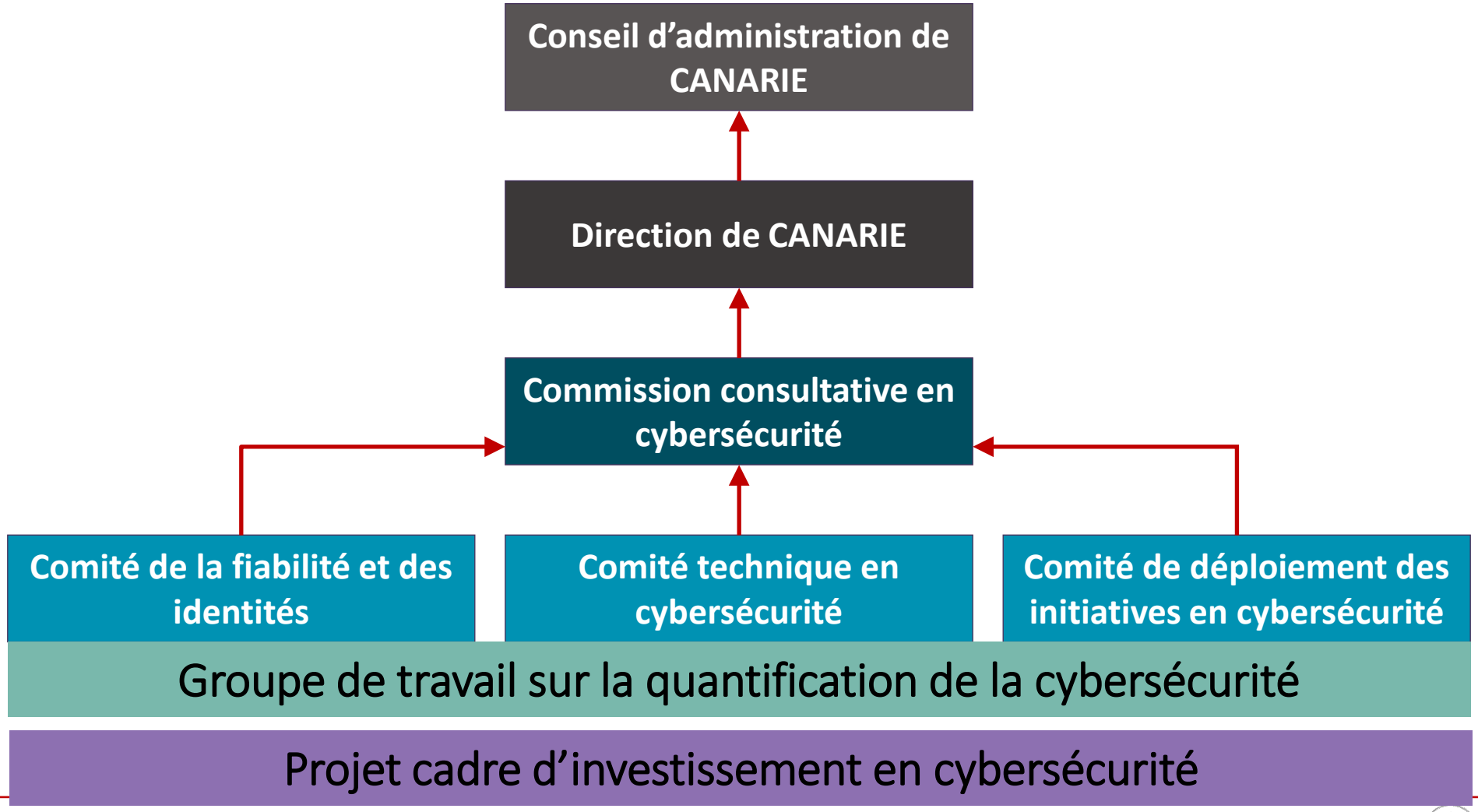
canarie.ca | @canarie_inc

Gouvernance et quantification

La Commission consultative en cybersécurité et ses comités permanents

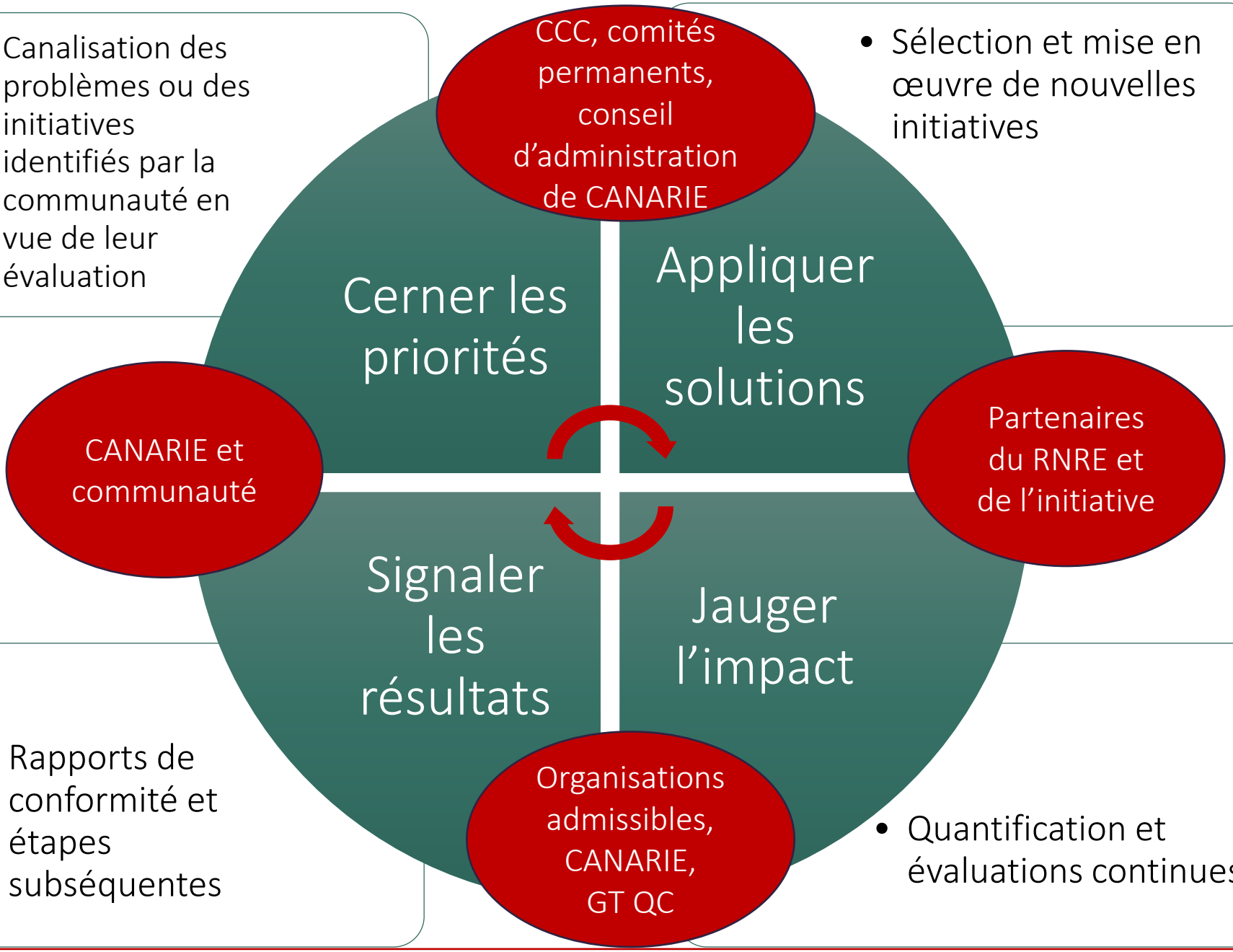


Gouvernance du programme



- Canalisation des problèmes ou des initiatives identifiés par la communauté en vue de leur évaluation

- Sélection et mise en œuvre de nouvelles initiatives



- Rapports de conformité et étapes subséquentes

- Quantification et évaluations continues