Une défense intelligente : s'unir pour repérer et contrer les cyberattaques

Kevin Parent | Gestionnaire, Initiatives en cybersécurité | CANARIE
Jill Kowalchuk | Directrice exécutive | CanSSOC
Martin Vezina | Architecte de solutions de sécurité | CanSSOC

Le 18 mai 2021 | Le 28 mai 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.

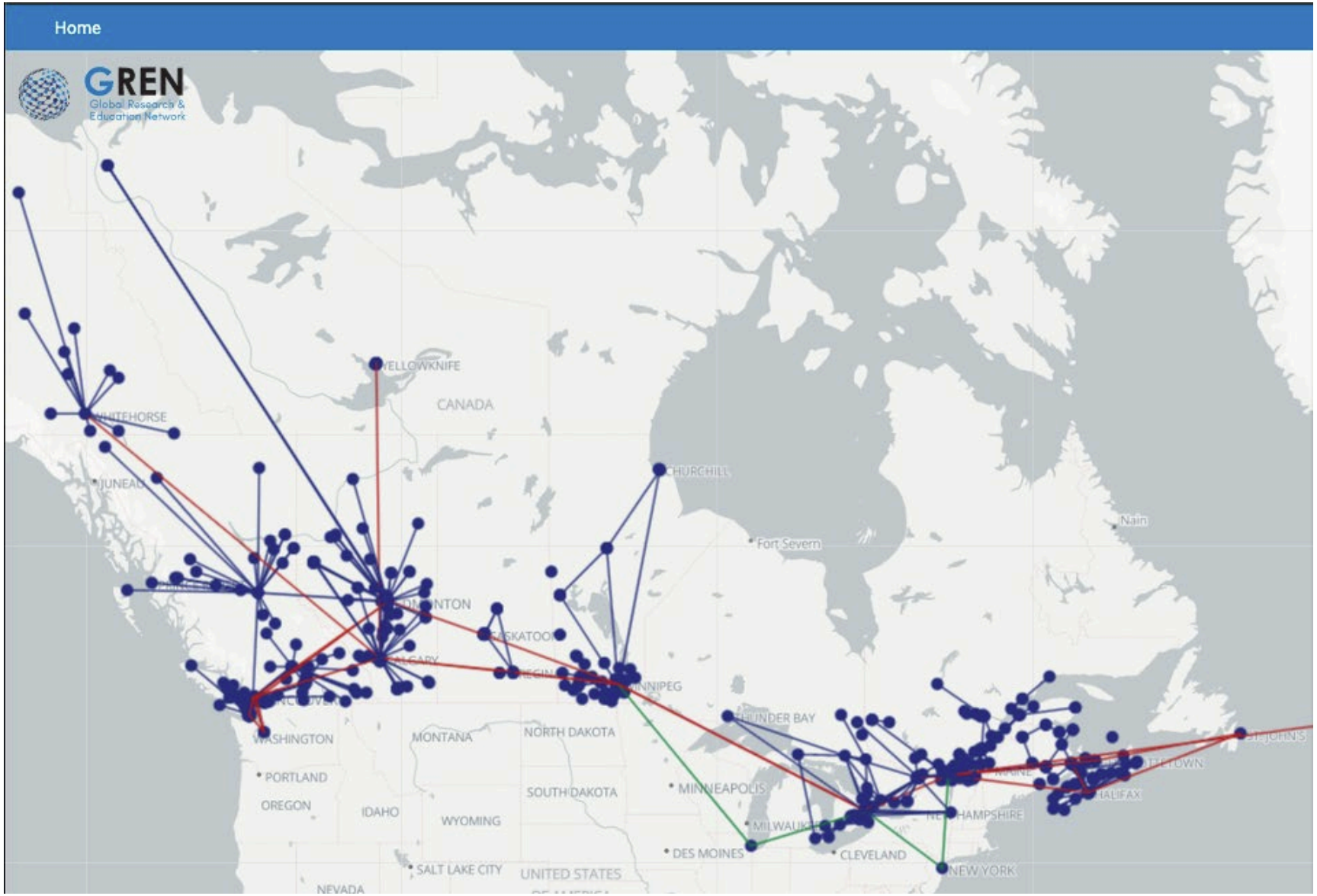
Toutefois, si la fonction « participation audio » a été activée, le fichier vidéo inclura votre voix.

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

Le programme Initiatives en cybersécurité (PIC)

Programme national, axé sur la collaboration, s’adressant au milieu canadien de la recherche et de l’éducation

Conçu par la communauté, pour la communauté

Qu’est-ce que le PIC?

- Le gouvernement du Canada finance CANARIE pour qu’il investisse dans des initiatives prioritaires qui renforceront le secteur de la recherche et de l’éducation (R-E) dans son ensemble.
- L’exécution des initiatives subventionnées dans les organisations admissibles a été confiée aux partenaires provinciaux et territoriaux du RNRE.

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

Coordination nationale, plus grand impact local

Profiter de la nature collaborative du secteur

Atténuer les risques à chaque palier

Bâtir sur les initiatives antérieures

Amener la communauté à progresser

L'approche et de la stratégie élaborées pour le PIC ne peuvent aboutir sans la collaboration de nos partenaires.

Avantages pour les organisations admissibles

- Consolider l'infrastructure existante en cybersécurité
- Jauger l'impact des initiatives sur l'organisation
- Collaborer avec une communauté nationale d'experts en sécurité du milieu R-E
- Rehausser les compétences et l'expertise en sécurité de l'équipe de l'institution; le programme comprend de la formation et un soutien technique
- Sécuriser l'organisation davantage

Sans que cela coûte un sou. Participer est votre façon d'investir.

Les trois premières initiatives

Implantation, soutien et formation dans 210 organisations admissibles

cira
D-ZONE DNS FIREWALL

CANSSOC
Threat Feed

Intrusion
Detection
System

En s’intégrant mutuellement, ces initiatives renforcent la cybersécurité localement, ce qui sécurisera l’ensemble du secteur.

Des fonctions complémentaires qui renforcent l'organisation

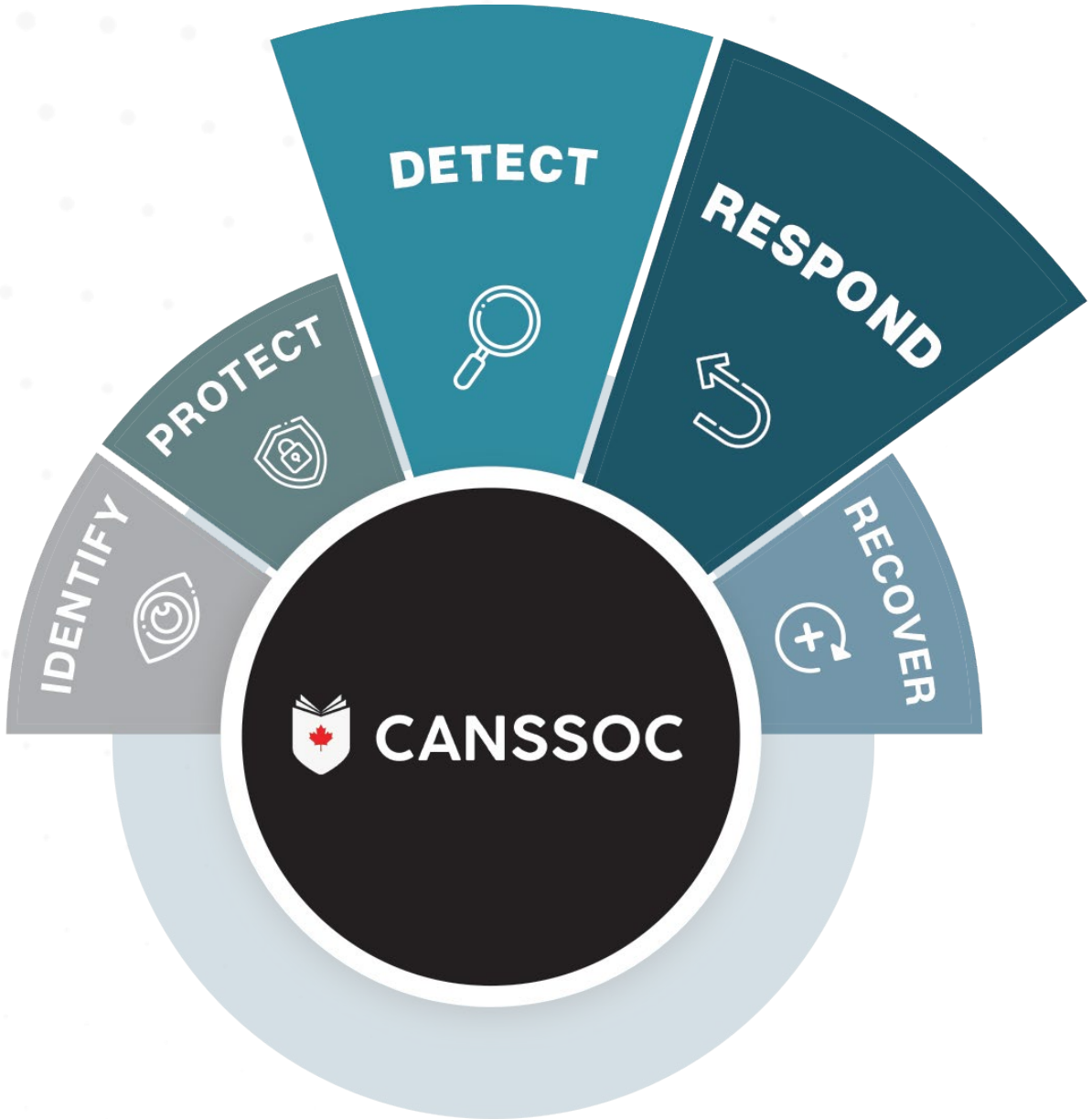
	Pare-feu DNS	Fil de menaces	IDS
Empêche l'utilisateur d'accéder à des sites Web malveillants	X		
Renseigne les dispositifs pour bloquer le trafic		X	
Signale les comportements suspects aux analystes en sécurité			X
Actualise le système quand surgissent de nouvelles menaces	X	X	X

Le Fil de menaces du CanSSOC : une nouvelle initiative subventionnée pour le secteur canadien de la recherche et de l'éducation

UN FRAGMENT DU **MÊME TISSU**

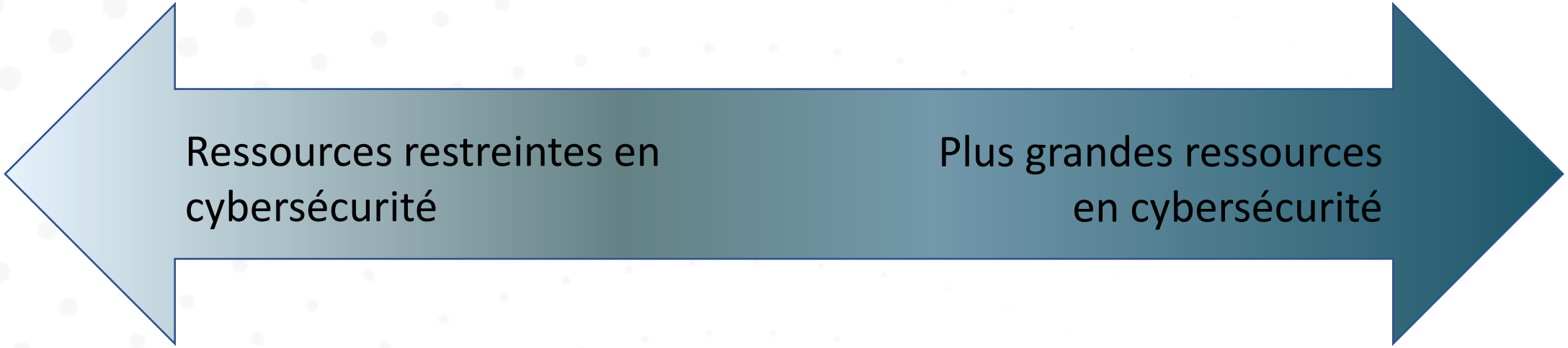
S'allier pour faire mieux que chacun séparément, toujours par le partenariat

SPÉCIALISÉ DANS
LA **DÉTECTION**
ET LA
RÉACTION



CANSSOC

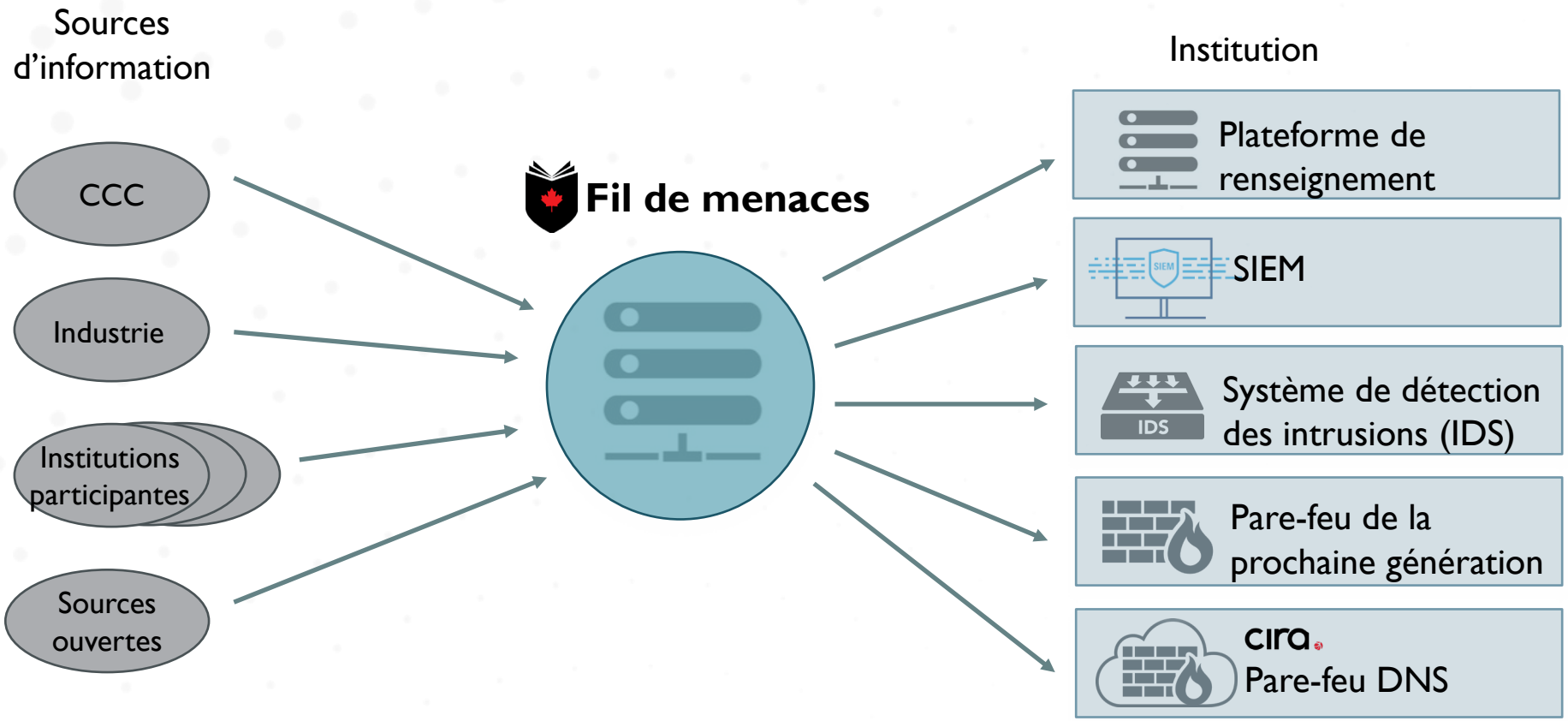
PERSONNEL REQUIS POUR LE FIL DE MENACES



1-3 heures de l'administrateur du pare-feu – une seule fois

Épargne du temps aux analystes, qui peuvent se consacrer davantage à la détection et à la réaction

QU'EST-CE QUE LE FIL DE MENACES?



CANSSOC

POURQUOI LE FIL DE MENACES DU CANSSOC?

- Les analystes locaux passeront moins de temps à trier les informations sur les menaces.
- Le service du CanSSOC regroupe de nombreux fils pour en faire une source d'information homogène.
- Les analystes du CanSSOC actualisent le fil grâce aux renseignements de source ouverte (OSINT).
- Il intègre les menaces spécifiques à l'institution (automatiquement et manuellement).

PLATEFORME DE RENSEIGNEMENT ET FIL DE MENACES

Plateforme de renseignement (MISP)

- Dépôt regroupant l'ensemble des indicateurs et des attributs
- Emplacement central facilitant l'examen des informations sur les indicateurs
- Solution de source ouverte reconnue par une communauté de plus en plus vaste
- Plateforme évolutive, sans lien avec les fournisseurs

Fil de menaces (MineMeld)

- Intégration automatique par les dispositifs de protection
- Solution de source ouverte – devra être remplacée à l'automne 2021

PIPELINE D'INFORMATIONS SUR LES MENACES

CANSSOC

INTÉGRATION AU PARE-FEU DE LA PROCHAINE GÉNÉRATION

- La plupart des pare-feu de la prochaine génération acceptent l'intégration des fils de menaces.
- Configuration simple (1-3 heures pour l'administrateur)
- Plus besoin de s'en occuper une fois l'intégration terminée
- Avantage : réduction d'environ 30 % des connexions malveillantes très facilement

SOUTIEN

- Collaboration entre les analystes du RNRE et du CanSSOC
- Moyen principal : canal Slack
  - #institution-canssoc – tout le personnel; sert surtout au soutien et au signalement de problèmes
  - #threatfeed – tous le personnel; mises à jour sur le service
  - #threatintel – membres de la sécurité de l'information seulement; doivent accepter le parallélisme; partage d'informations sensibles
  - #threatfeed_documentation – tout le personnel; documentation

SÉANCE DE FORMATION

1. Signature de l'entente de confidentialité (CANARIE)
2. Réservation d'un moment pour la séance
3. Création des comptes par le CanSSOC : MISP et MineMeld
4. Formation technique d'une heure : CanSSOC ou partenaire du RNRE
5. Intégration au pare-feu ou à un autre dispositif de protection ou de détection au point terminal

INFORMATIONS EXPLOITABLES

- Partenaire de confiance pour la divulgation : report@canssoc.ca
- Le Fil de menaces est à la base de la détection et de la réaction.
- Mécanisme simple, d'origine sectorielle, permettant le partage de l'information

Alerte

Avis signalant aux institutions que des indicateurs de compromission pourraient s'être glissés dans le réseau

Avis

Menaces à risque élevé spécifiques au secteur et observations anonymisées sur les alertes et les divulgations émanant des institutions

Adhésion
Si l'organisation s'est déjà inscrite au PIC…

1. Le partenaire du RNRE de votre province ou territoire vous enverra le lien conduisant au formulaire d'inscription du Fil de menaces.
2. Après remise du formulaire, CANARIE vous enverra l'entente de confidentialité du CanSSOC.
3. Signez l'entente.
4. Votre partenaire du RNRE prendra contact avec vous pour organiser la séance de formation technique.

Adhésion
Si l'organisation ne s'est pas encore inscrite au PIC…

1. Contactez votre partenaire du RNRE pour savoir si l'organisation est admissible.
2. Si c'est le cas, le partenaire du RNRE vous enverra un lien menant au formulaire d'inscription du PIC. Vous pourrez vous inscrire au Fil de menaces par la même occasion.
3. Après avoir reçu le formulaire, CANARIE vous enverra l'entente concernant le PIC (ECCO) et l'entente de confidentialité du CanSSOC.
4. Signez l'ECCO de CANARIE.
5. Signer l'entente de confidentialité du CanSSOC.
6. Votre partenaire du RNRE vous contactera pour organiser la séance de formation technique.


A
Q

canarie

canarie.ca | @canarie_inc

cip@canarie.ca