Nouvelle initiative subventionnée : **Système de détection des intrusions (SDI)**

Kevin Parent | Gestionnaire de programme, Initiatives en cybersécurité
Julian Corduneanu | Directeur, Cybersécurité

5 août 2021 | 18 août 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 harmonise et coordonne ses efforts.

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

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

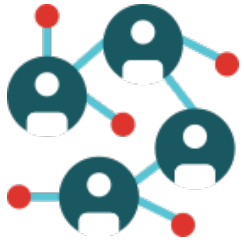
Conçu par la communauté, pour la communauté

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 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	SDI
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

Système de détection des intrusions (SDI)

Qu’est-ce que l’initiative Système de détection des intrusions (SDI)?

- *Cette initiative vise la création d’une communauté de spécialistes en sécurité qui renforcera la sûreté générale du secteur de l’enseignement supérieur en faisant ressortir les problèmes de sécurité dans les institutions et en analysant les vulnérabilités potentielles de ces dernières.*

- Cette initiative est le prolongement du Projet conjoint en sécurité (PCS).
- Les participants se joindront aux 138 institutions déjà inscrites à l’initiative.

SDI : résultats escomptés

1. Les employés des institutions canadiennes collaborent pour mettre en place et améliorer un système de sécurité reposant sur des données.

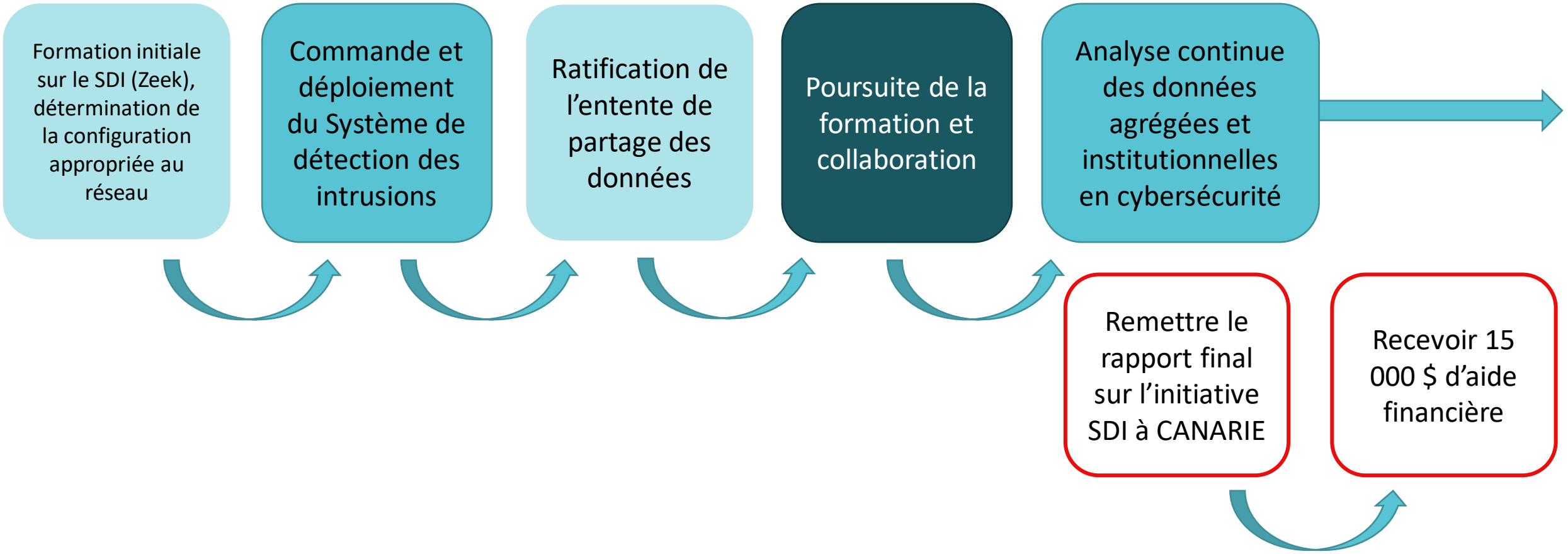
2. Des outils d’analyse surveillent le trafic qui circulent sur le réseau et renseignent les institutions sur les menaces et les vulnérabilités courantes.

SDI : résultats escomptés

3. Combinés aux informations glanées sur les menaces, des politiques et des processus normalisés de surveillance du réseau rendent les institutions plus sûres, afin qu'elles puissent collaborer plus étroitement dans l'avenir.

4. Éventualité d'une intégration future à d'autres initiatives qui concourront à sécuriser totalement et d'une manière cohérente le réseau des institutions raccordées au RNRE

Participation à l'initiative SDI : aperçu



Matériel fourni

- Serveur PowerEdge R440 de DELL (système d'exploitation recommandé : CentOS Stream et application Network Traffic Manager de Zeek pour détecter les anomalies avec le SDI)
- Points d'accès terminaux avec tablettes de support spéciales (IXIA ou GIGAMON)
- Émetteur-récepteur enfichable de petite taille (connexion optique ou filaire)

Contraintes techniques (installation et maintenance)

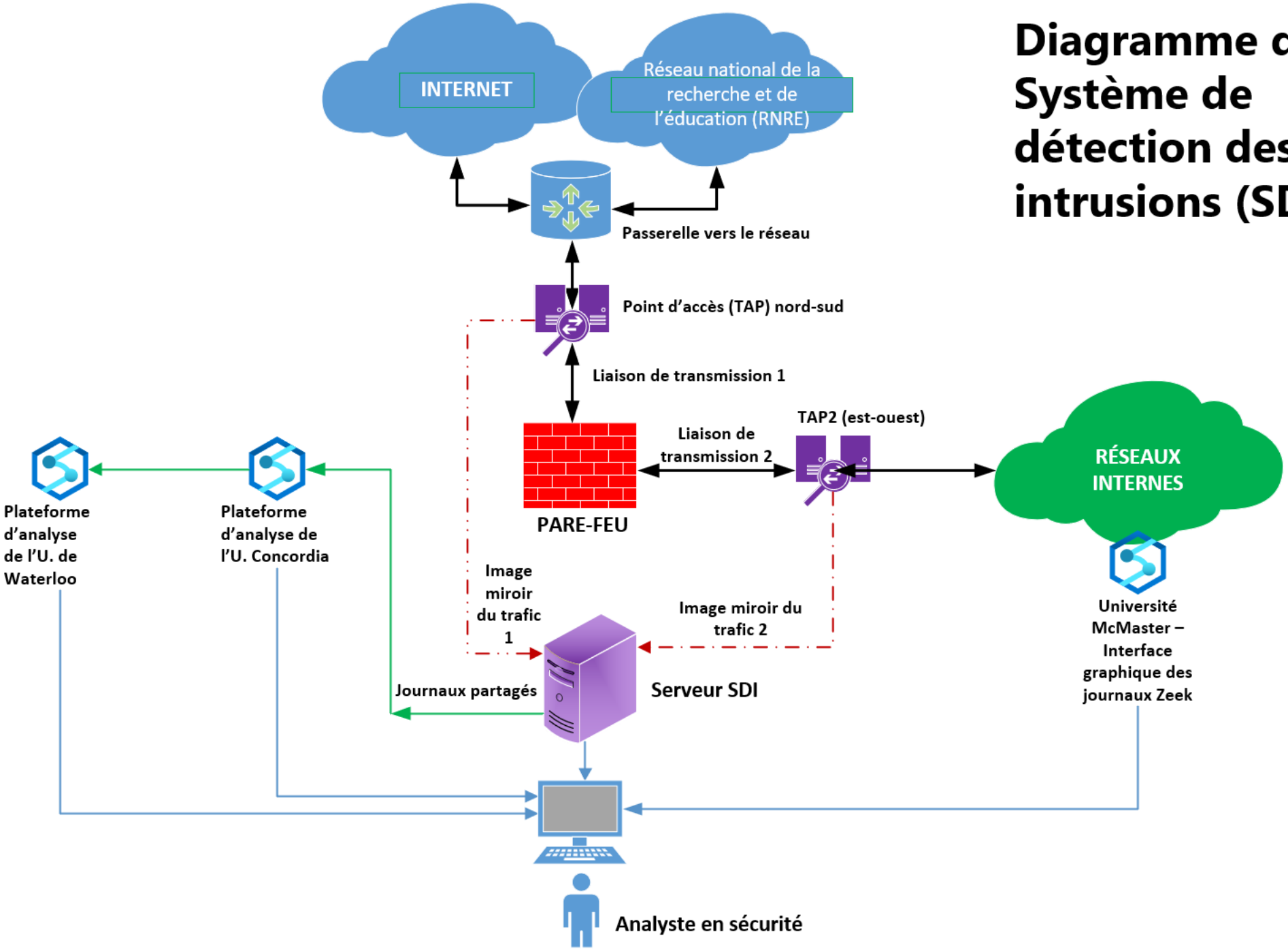
- Espace pour un serveur 1U sur le râtelier, avec prise de 120V
- Connexion optique ou filaire de 1 G ou 10 G du serveur au réseau par les deux points d'accès terminaux (connexion optique passive ou filaire active) ou ports en miroir sur l'équipement réseau existant
- Connexion 1 G au serveur en tant qu'administrateur pour mettre à jour le logiciel et envoyer les données choisies par l'utilisateur aux plateformes d'analyse du SDI

Outils d'analyse du SDI

Trois outils d'analyse en cybersécurité, mis au point par des chercheurs, sont à votre disposition

1. Université Concordia – son portail Web fournit des résultats détaillés à partir des données que l'institution veut bien partager; même analyse pour toutes les institutions sous une forme agrégée, qui préserve l'anonymat
2. Université de Waterloo – son portail Web fournit des résultats détaillés à partir des données que l'institution veut bien partager; même analyse pour toutes les institutions sous une forme agrégée, qui préserve l'anonymat
3. Université McMaster (désormais appuyée par FyeLabs, une filiale) – outil installé localement permettant d'examiner toutes les données du SDI directement à l'institution

Diagramme du Système de détection des intrusions (SDI)



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 choisir le SDI et les autres initiatives en même temps.

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 SDI.
2. Après remise du formulaire, CANARIE vous enverra l'entente de participation au SDI.
3. Une fois l'entente signée, vous serez convié à une séance d'information qui vous aidera à choisir l'équipement convenant le mieux à votre infrastructure.
4. Envoyez votre bon de commande.
5. Lorsque vous aurez reçu l'équipement, nous reprendrons contact avec vous pour vous expliquer comment le configurer et vous dispenser la formation.

Que se passera-t-il après l'installation du serveur du SDI et des points d'accès terminaux (TAP) sur le réseau?

1. Établissez quelles données vous partagerez avec les autres institutions.
2. Signez l'entente de partage des données.
3. Amorcez le partage des données avec les plateformes des universités Concordia et de Waterloo.
4. Accédez aux portails d'analyse en cybersécurité.
5. Participez aux réunions de coordination régulières avec les autres institutions.


R
Q

canarie

canarie.ca | @canarie_inc

cip@canarie.ca