



# FIL DE MENACES CANSSOC

Le Fil de menaces CanSSOC est une **plateforme qui renseigne sur les cybermenaces** qui ciblent le secteur de l'éducation.

Il **consolide et regroupe** plusieurs fils de menaces afin de **collecter des renseignements** qui émanent des :

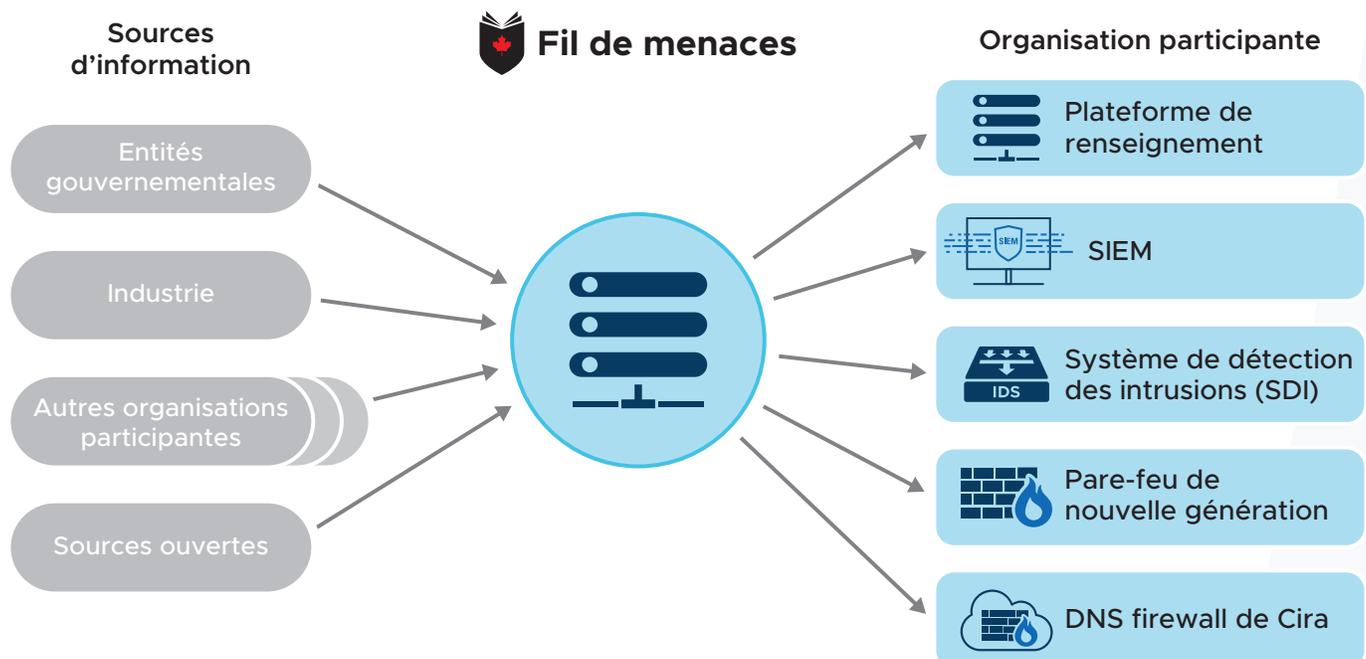
- entités gouvernementales
- services de renseignement commerciaux sur les menaces informatiques
- organisations participantes à l'initiative
- sources ouvertes

Une fois collectées, ces informations sont **regroupées et analysées** afin de dresser une **liste de blocages et d'autorisations de sites** que vous pourrez ensuite **déployer sur vos systèmes de sécurité existants**.

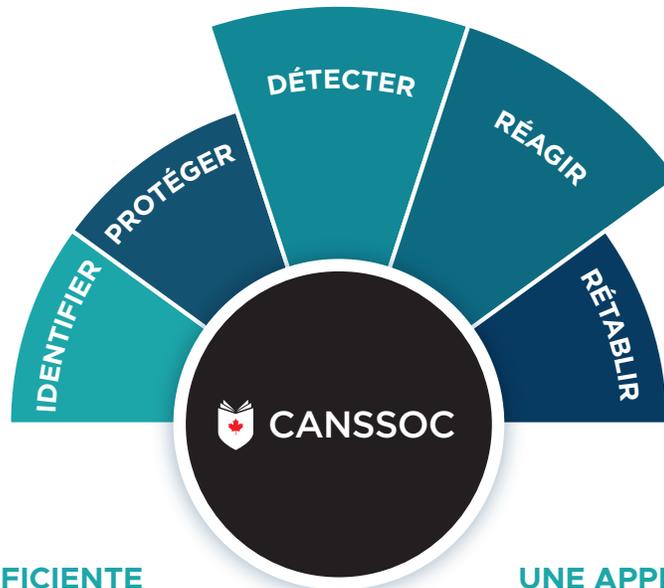
## OBJECTIF

Permettre une approche collaborative de la cybersécurité afin de mieux détecter et bloquer les cybermenaces qui visent spécifiquement vos organisations.

## FONCTIONNEMENT



# AVANTAGES



## UNE PLATE-FORME EFFICIENTE

- Collecte et analyse des données de plusieurs sources pertinentes, et est constamment actualisé avec de l'information directement exploitable par vos équipes des TI et de sécurité.
- Renforce vos mesures de protection existantes grâce à des informations sur les menaces qui vous visent spécifiquement.
- Bloque automatiquement les adresses IP, les URL et les domaines malveillants.
- Nécessite peu de maintenance.

## UNE RÉALISATION D'ÉCONOMIES VARIÉES

- Permet d'exploiter des renseignements et des fils de menaces disponibles dans le commerce.
- Alloue un gain de temps important grâce à un fil consolidé et contrôlé qui bloque automatiquement les cybermenaces.
- Ne requiert pas d'expertises spécifiques si ce n'est que la capacité de gérer un pare-feu.

## UNE APPROCHE COLLABORATIVE DE LA CYBERSÉCURITÉ

- Permet aux différentes organisations participantes à l'initiative d'utiliser et de partager facilement les renseignements collectés sur les menaces.
- Offre la possibilité de se servir de la plateforme uniquement à des fins d'enquêtes ou de recherches.

## UNE INTÉGRATION SIMPLE ET RAPIDE

- S'intègre facilement, et en seulement quelques heures, à la plupart des pare-feux de la prochaine génération (Palo Alto, Fortigate de Fortinet et Fire power de Cisco) ainsi qu'aux systèmes de détection des intrusions (SDI) et d'analyse des incidents (SIEM).

Le programme d'initiatives financées en cybersécurité pour les CSS et CS est actuellement financé jusqu'en 2025.

## INFORMATION

Vous souhaitez obtenir plus d'information au sujet de cette initiative? Contactez-nous dès maintenant par courriel à [sam@risq.quebec](mailto:sam@risq.quebec).

[www.risq.quebec](http://www.risq.quebec)

