La cybersécurité dans un contexte de sécurité civile

COLLOQUE SUR LA SÉCURITÉ CIVILE – OCTOBRE 2022

1

CONTEXTE

Il était une fois…

Une infrastructure essentielle

Un environnement hostile

Principaux moyens utilisés par les acteurs de la menace

Exfiltrations

Rançongiciels

Dénis de service

2

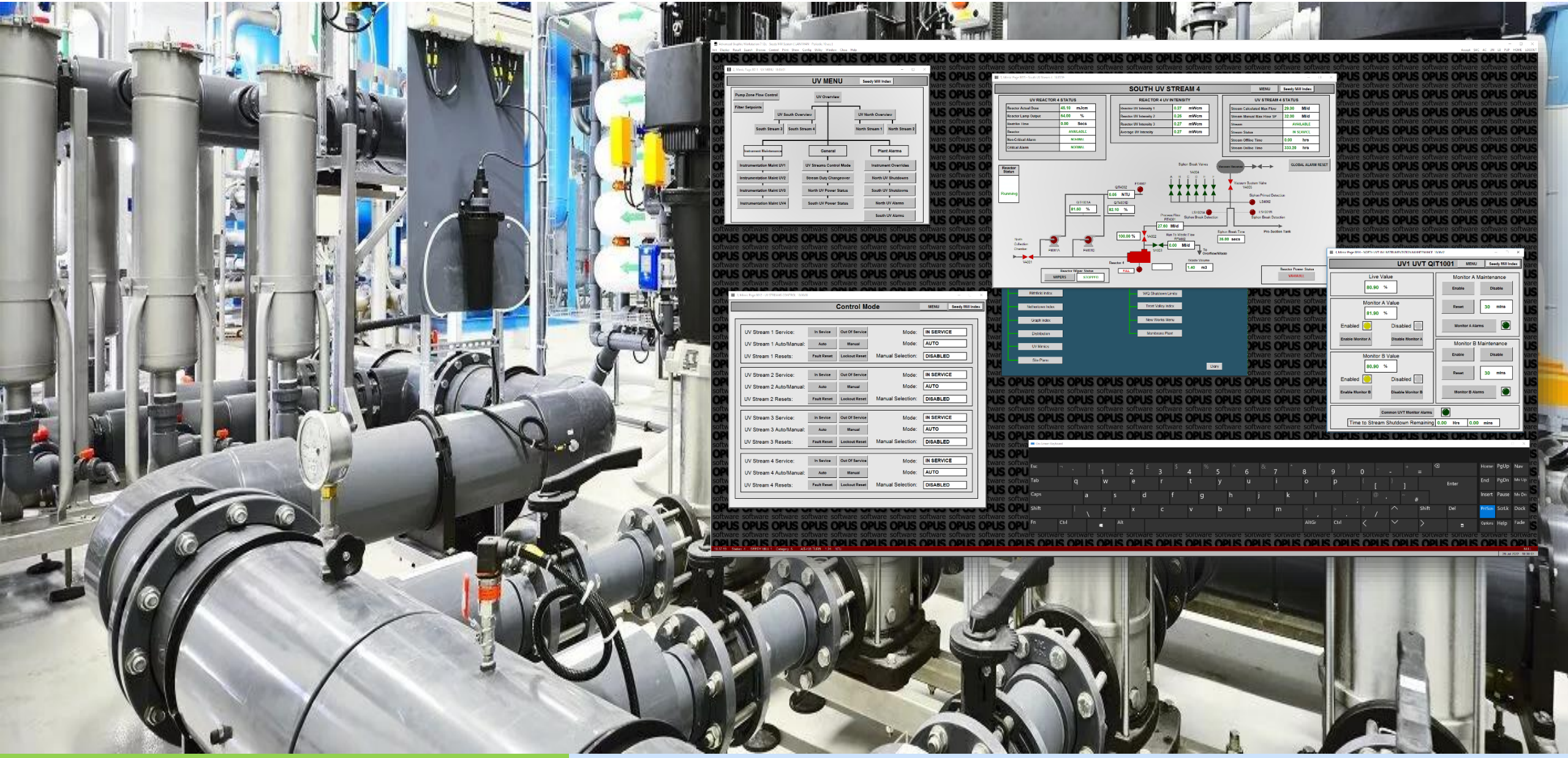
IMPACTS CYBERPHYSIQUES

Secteur des transports

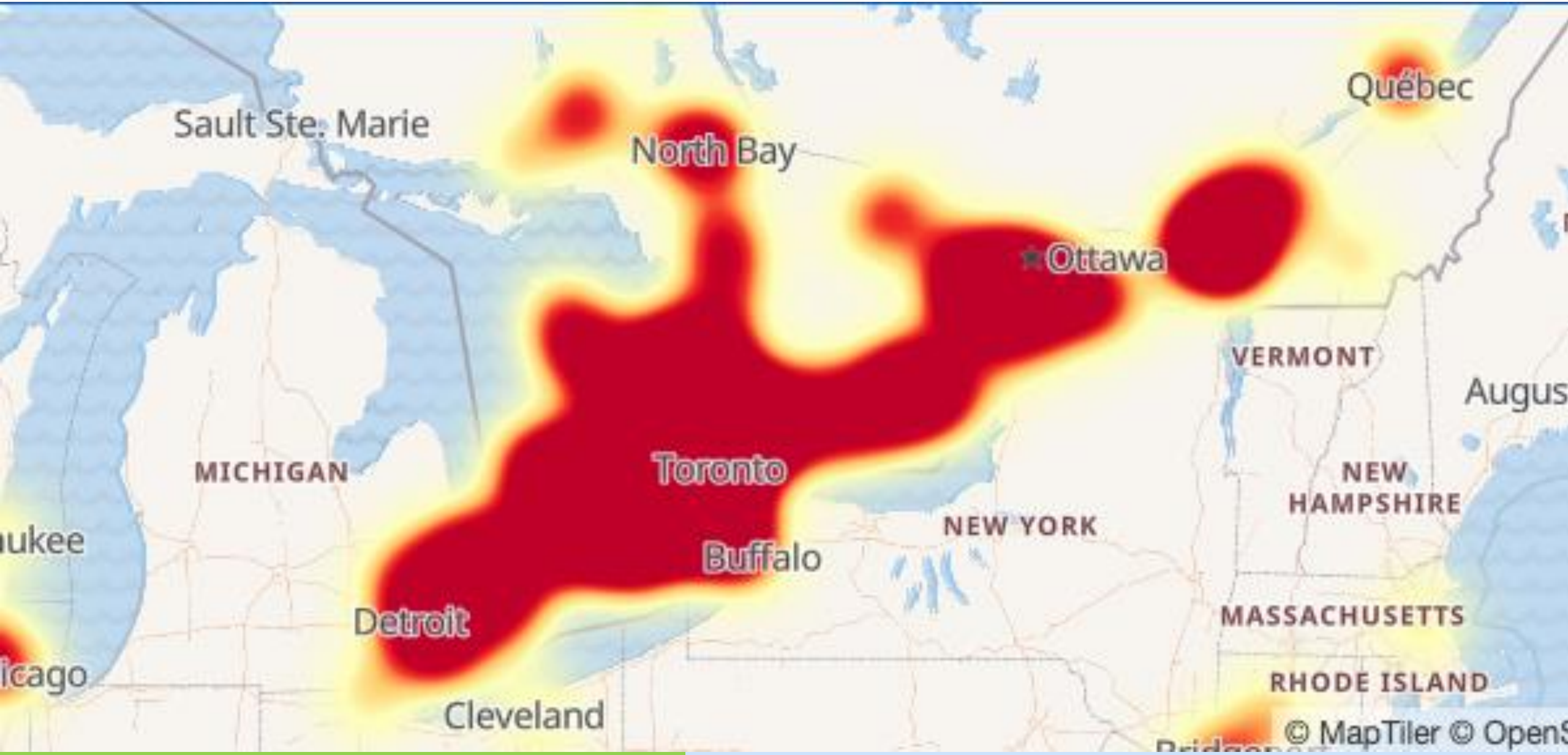
Secteur de la santé

Secteur de l’énergie

Secteur de l’eau



Secteur des télécommunications



Autres

3

RÉPONSE AUX INCIDENTS MAJEURS

Escalade vers un incident majeur

Incident de cybersécurité

Incident de cybersécurité majeur

Mesures d’urgence

Gérer un incident de cybersécurité.

- **Détecter et analyser**
- **Confiner**
- **Éradiquer**
- **Rétablir – retour à la normale**

Se préparer aux incidents majeurs (1)

- **Savoir reconnaître un incident majeur**
- **Définir les rôles et responsabilités des parties prenantes**
- **Définir des critères de mobilisation**
- **Avoir un plan d’intervention**

Se préparer aux incidents majeurs (2)

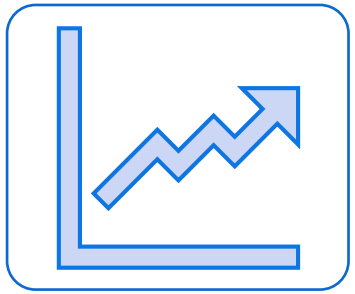
- **Tester l’exécution du plan**
- **Faire face à nos obligations de divulgation**
- **Aller chercher de l’aide externe si nécessaire**

La proactivité est la clé

Gérer un incident de cybersécurité **majeur**

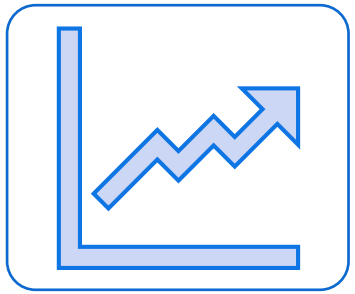
- **Intégrer la cybersécurité aux plans d’urgence**
- **Avoir des plans de communication**
- **Être enligné avec le positionnement du gouvernement**

En résumé



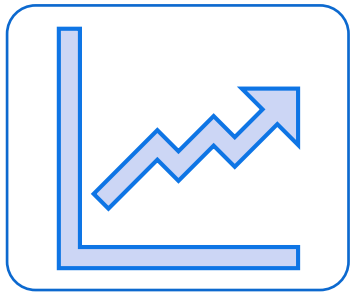
Augmentation des cybermenaces

- Le contexte géopolitique mondial est instable
- Augmentation notre exposition



Niveau de préparation

- Doit être proactif
- Les plans doivent être pratiqués



Gestion de la crise

- S’intégrer à ses Mesures d’urgence

Merci !

La cybersécurité dans un contexte de sécurité civile

La cybersécurité dans l'administration publique du Québec

Colloque de la Sécurité Civile du Québec

20 octobre 2022

Steve Waterhouse, CD, CISSP

Sous-ministre adjoint à la sécurité de l'information gouvernementale et de la cybersécurité

Votre gouvernement

Québec

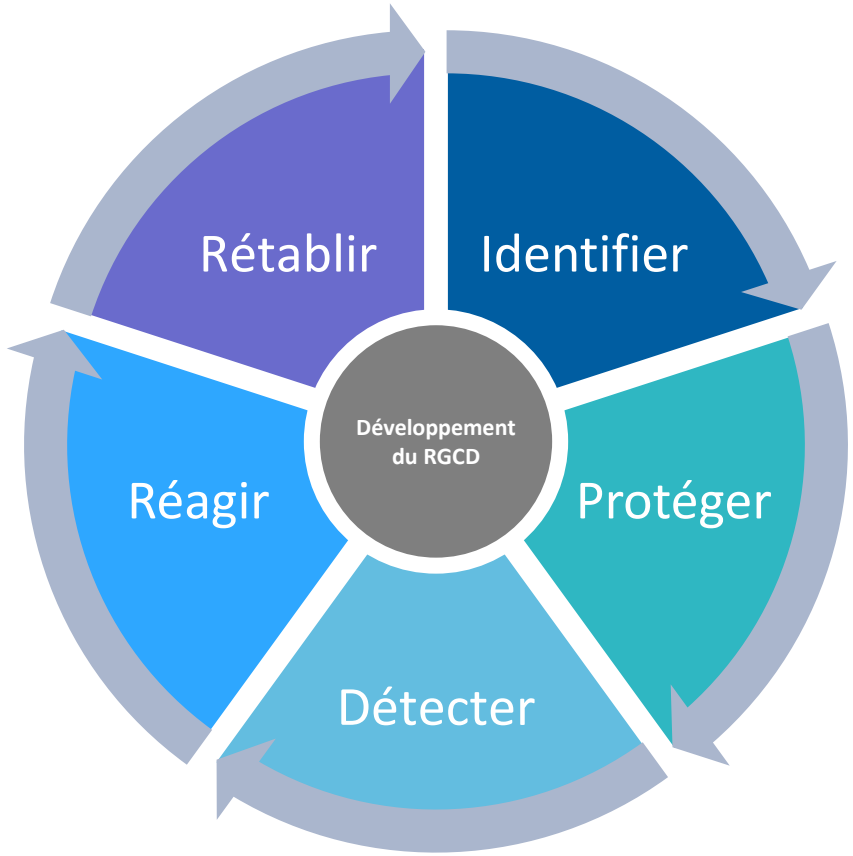
Mission du MCN

- Diriger et coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique
- Proposer au gouvernement les grandes orientations en ces domaines, déterminer les secteurs d'activités où il entend agir en priorité et conseiller le gouvernement et les organismes publics (OP)
- Proposer au gouvernement des mesures en vue d'accroître l'efficacité de la lutte contre les cyberattaques et les cybermenaces au Québec
- Favoriser la transformation numérique des OP
- Concentrer et développer une expertise interne en infrastructures technologiques communes
- Contribuer à rehausser la sécurité de l'information numérique au sein des OP et la disponibilité des services aux citoyens et aux entreprises
- Permettre l'utilisation accrue d'infrastructures technologiques partagées sécuritaires et performantes

Centre gouvernemental de cyberdéfense (CGCD)

NOS SERVICES

- Remise en service
- Développement du RGCD
- Gestion des incidents
- Cyber enquêtes
- Audits de sécurité
- Vulnérabilités
- Surveillance opérationnelle



- Portrait des mesures et outils de protection des actifs
- Évaluation d'impacts
- Veille et innovation
- Sensibilisation
- Communication
- Référentiel
- Gestion des tiers
- Développement sécuritaire
- Outils
- Développement des compétences

INSPIRÉ DE *The National Institute of Standards and Technology (NIST)*

Le projet de loi C-26 (fédéral)

Loi sur la Protection des cybersystèmes essentiels (LPCE)

4 secteurs:

1. Les services de télécommunication;
2. Les systèmes de pipelines et de lignes électriques interprovinciaux ou internationaux;
    A. Les systèmes d'énergie nucléaire;
3. Les systèmes de transport relevant de la compétence législative du Parlement;
4. Les systèmes bancaires;
    A. Les systèmes de compensations et de règlements.

Le projet de loi C-26 (fédéral)

Programme de cybersécurité

L'exploitant désigné est tenu d'établir un programme de cybersécurité relativement à ses cybersystèmes essentiels et d'y inclure des mesures raisonnables en vue, conformément à tout règlement :

a) d'identifier et de gérer les risques organisationnels pour la cybersécurité des cybersystèmes essentiels, notamment les risques associés à la chaîne d'approvisionnement de l'exploitant désigné et à l'utilisation par celui-ci de produits et services de tiers;

b) de protéger ses cybersystèmes essentiels contre toute compromission;

c) de détecter les incidents de cybersécurité qui touchent ou pourraient toucher ses cybersystèmes essentiels;

d) de réduire au minimum les conséquences des incidents de cybersécurité qui touchent les cybersystèmes essentiels;

e) de prendre toute mesure prévue par règlement.

La loi 25 (Québec)

Entrée en vigueur 21 septembre 2022

- Obligation d'exercer la fonction de responsable de la protection des renseignements personnels ou de la déléguer par écrit à une autre personne et de publier les coordonnées du responsable
- Obligation de former un comité sur l'accès à l'information et la protection des renseignements personnels
- Obligation d'aviser la Commission et la personne concernée de tout incident de confidentialité impliquant un renseignement personnel présentant un risque sérieux de préjudice et de tenir un registre devant être fourni à la Commission sur demande
- Nouvel encadrement de la communication de renseignements personnels sans le consentement de la personne concernée :
  - à des fins d'étude, de recherche ou de productions de statistiques
  - dans le cadre d'une transaction commerciale
- Obligation de divulguer toute banque de caractéristiques ou de mesures biométriques à la Commission au moins 60 jours avant sa mise en service
- Obligation de divulguer la vérification ou la confirmation d'identité faite au moyen de caractéristiques ou de mesures biométriques
- Modifications aux pouvoirs, fonctions et rôles de la Commission. Par exemple :
  - ajout d'une nouvelle vice-présidence
  - pouvoir d'élaborer des lignes directrices

Merci!

29