Planifier.
Bâtir.
Entretenir.

Sécurité des ressources informationnelles de la SQI

DIRECTION GÉNÉRALE DES TECHNOLOGIES DE L'INFORMATION

11/2022

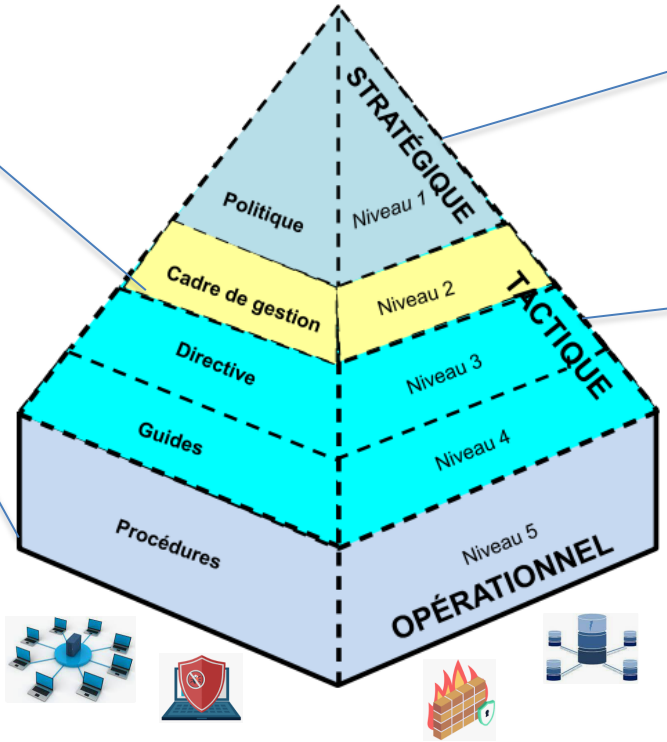
Société québécoise des infrastructures
Québec

GOUVERNANCE ET CONDITIONS DE SUCCÈS

À la SQI, la mise en place du programme de cybersécurité s'est faite graduellement en commençant par les éléments stratégiques et tactiques.

Cadres de gouvernance et bonnes pratiques existantes (SCT et MCN)

Formation
Compétences techniques



Engagement des dirigeants

Mobilisation - Adhésion

La cybersécurité est essentiellement un processus de gestion des risques, une fois les mesures de mitigations choisies, celles-ci se réalisent sous forme de projets

Accepter

Éviter

Transférer
(ex. infonuagique)

Mitiger
(projets en
cybersécurité)

Traitement des risques

Identification des actifs

Analyse des risques

On ne peut protéger que ce que l'on connaît

« Registre de risques » et arrimage avec les risques d'entreprise

Méthodes quantitatives
Méthodes qualitatives

Plusieurs standards

COBIT
Mehari
NIST
ISO

La mise en place des mesures de mitigation technologiques en cybersécurité se fait avec la méthode Agile

Source: CGI Québec/Centre d'Excellence Agile

Pas de projets en cascades (Waterfall)

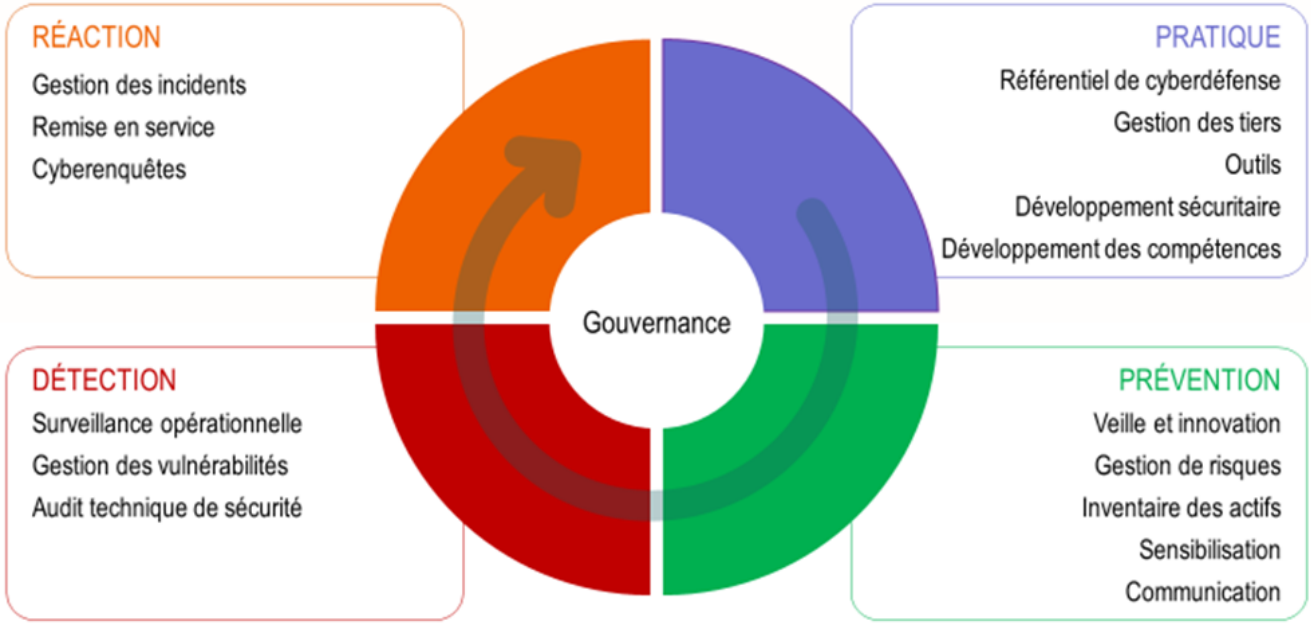
Livraisons par itérations

Carnet de produit en cybersécurité

MVP : Minimal Viable Product

Service opérationnel de cyberdéfense (SOC) à la SQI

En collaboration avec les 26 centres opérationnels de cyberdéfense (COCD) et le Centre gouvernemental de cyberdéfense (CGCD) du Secrétariat du Conseil du trésor



Conditions de succès

- **Commencer par les dirigeants** : les convaincre, parler leur langage, mettre en place des comités de suivi
- **Planifier à court et moyen terme** : un an est une éternité
- **Livrer par itération** : gains rapides, Pareto (20/80), Produit Minimal Viable (MVP)
- **Aller plus loin que la conformité** : faire plus que les directives gouvernementales
- **Se faire accompagner** : se faire auditer et challenger par des entités indépendantes
- **S'arrimer avec les unités affaires** : collaborer dans la transparence, ajouter de la valeur d'affaires

CYBERDÉFENSE

Les restrictions imposées par les gouvernements en réponse à la pandémie de coronavirus ont encouragé les employés à travailler à domicile. En conséquence, la technologie est devenue encore plus importante dans notre vie professionnelle et personnelle. Là où les réunions professionnelles se tenaient traditionnellement en présentiel, la plupart se déroulent désormais virtuellement.

Les entreprises accélèrent donc leur transformation numérique et la cybersécurité est désormais une préoccupation majeure.

Cette nouvelle réalité apporte son lot de problèmes relié à la cybersécurité. Les utilisateurs ne profitant pas du même niveau de protection et de dissuasion à la maison que sur les lieux de travail.

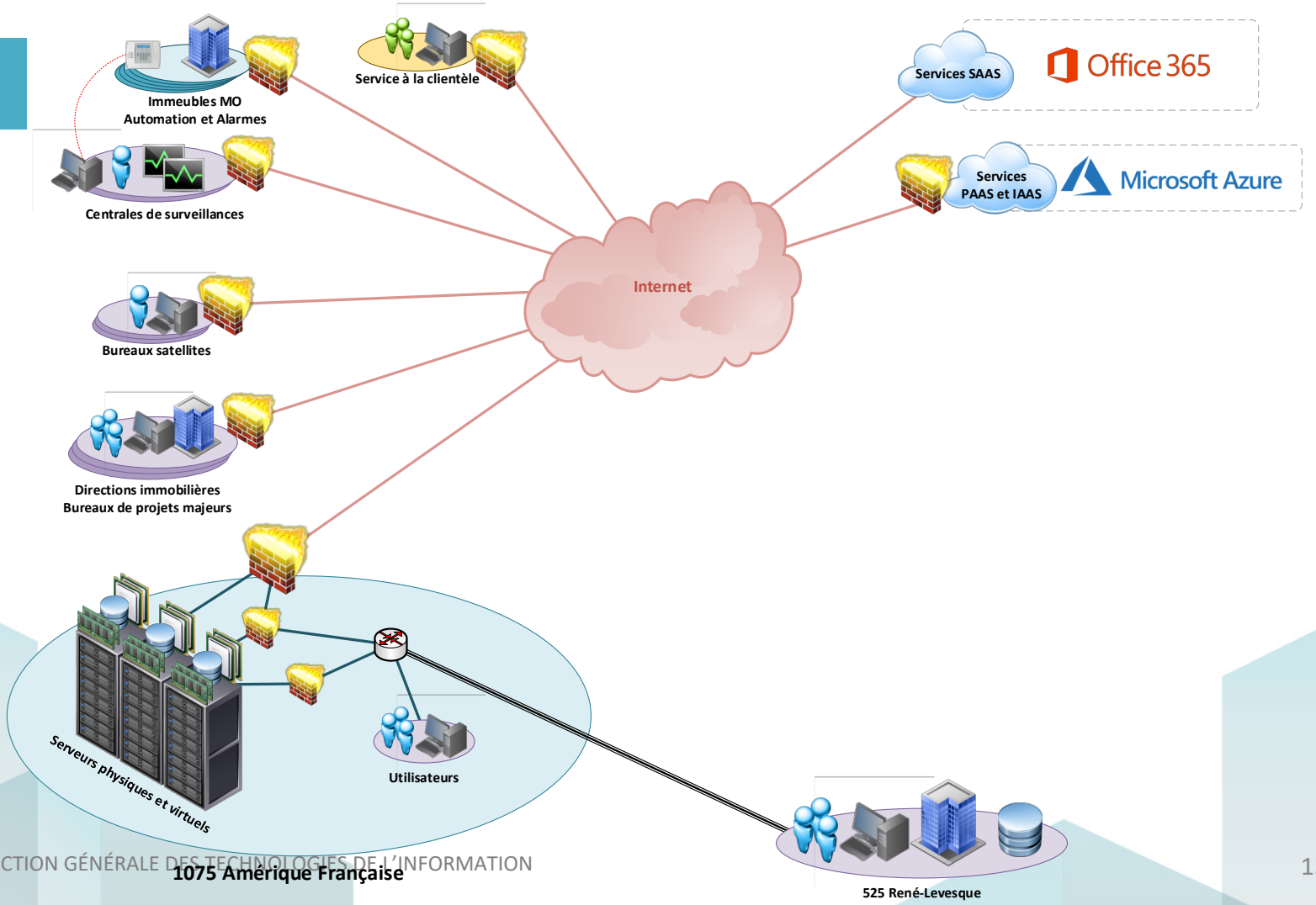
En avril 2020, à peine 1 mois après le début de la pandémie le « National Cyber Security Center » enregistrait des données records sur les cyberattaques. Hameçonnages, sites web frauduleux et attaques directes contre les entreprises (« ransomware ») ont augmenté de 200 % à 250 % comparativement aux mois et années précédentes.

Les cyberattaquants perçoivent la pandémie comme une occasion d'intensification de leurs activités criminelles en exploitant la vulnérabilité des employés travaillant à domicile et en capitalisant sur le vif intérêt des gens pour les nouvelles liées aux coronavirus. De plus, les employés travaillant à domicile ne bénéficient pas du même niveau de mesures de protection que ceux travaillant en présentiel.

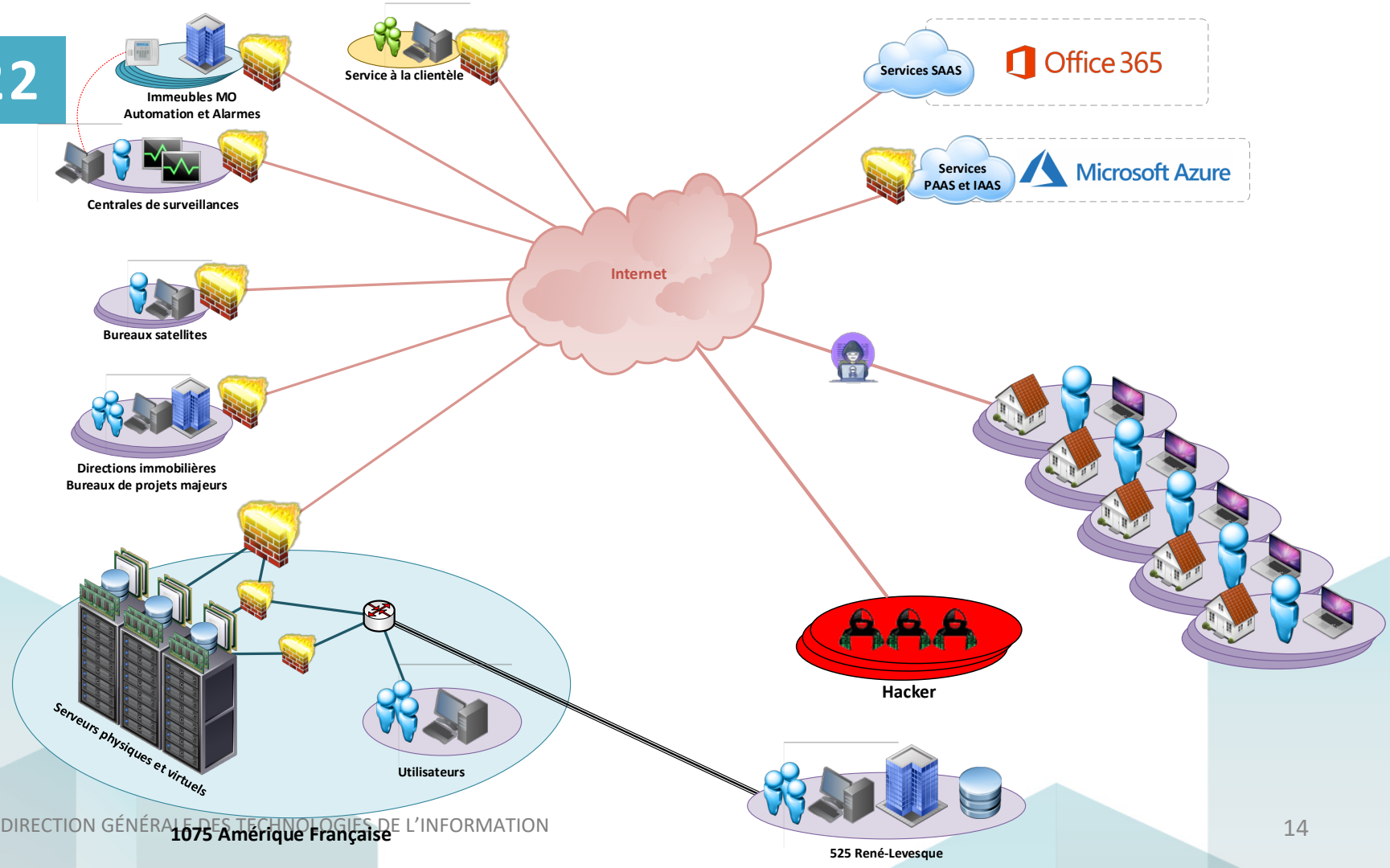
POSTES DE LA SQI 2020 VS 2022

PROTECTION DE L'ENVIRONNEMENT DE TRAVAIL

2020


Immeubles MO
Automation et Alarmes
Service à la clientèle
Services SAAS
Office 365
Centrales de surveillances
Services
PAAS et IAAS
Microsoft Azure
Internet
Bureaux satellites
Directions immobilières
Bureaux de projets majeurs
Serveurs physiques et virtuels
Utilisateurs
1075 Amérique Française
525 René-Levesque

2022


Immeubles MO
Automation et Alarmes
Service à la clientèle
Services SAAS
Office 365
Centrales de surveillances
Services
PAAS et IAAS
Microsoft Azure
Internet
Bureaux satellites
Directions immobilières
Bureaux de projets majeurs
Hacker
Serveurs physiques et virtuels
Utilisateurs
1075 Amérique Française
525 René-Levesque

PROTECTION DE L'ENVIRONNEMENT DE TRAVAIL

PROJET INTUNE (MEM)

Mise à jour

- Coupe feu Local
- Antivirus nouvelle génération
- Réduction surface d'attaque
- Gestion des vulnérabilités
- Détection et réponse des postes
- Examen et correction automatisés
- Accès au SOC de Microsoft

MERCI

Société québécoise
des infrastructures
Québec