



911
Médical

CCSC

CAUCA

Coordination et collaboration en crise : gérer l'imprévu lors d'une cyberattaque

Présenté par :

Andréanne Drolet - Coordonnatrice en conformité et efficacité opérationnelle (CCSC)

Dave Boucher - Superviseur aux opérations (CAUCA)

CCSC en quelques mots...



Situé dans la région de Québec



Reçoit et traite les appels 9-1-1
secteur santé



Couvre les territoires de la Capitale-
Nationale, du Saguenay–Lac-St-Jean
et du Nord du Québec



Dessert 1.5 M de population



Moyenne de 400 appels par jour

CAUCA en quelques mots...



CAUCA



Situé dans la région de Chaudière-Appalaches



Reçoit et traite les appels 9-1-1 secteur santé mais également Centres primaire 9-1-1 et secondaire incendie



Couvre le territoire de Chaudière-Appalaches pour le secteur santé et 580 municipalités en 9-1-1 et incendie



Dessert 1.7 M de population



Moyenne de 150 appels par jour pour le volet santé

Cyberattaque Janvier 2024

Contexte :

En pleine nuit, une cyberattaque majeure paralyse le CCSC, forçant le transfert complet des appels d'urgence vers CAUCA.

Défis :

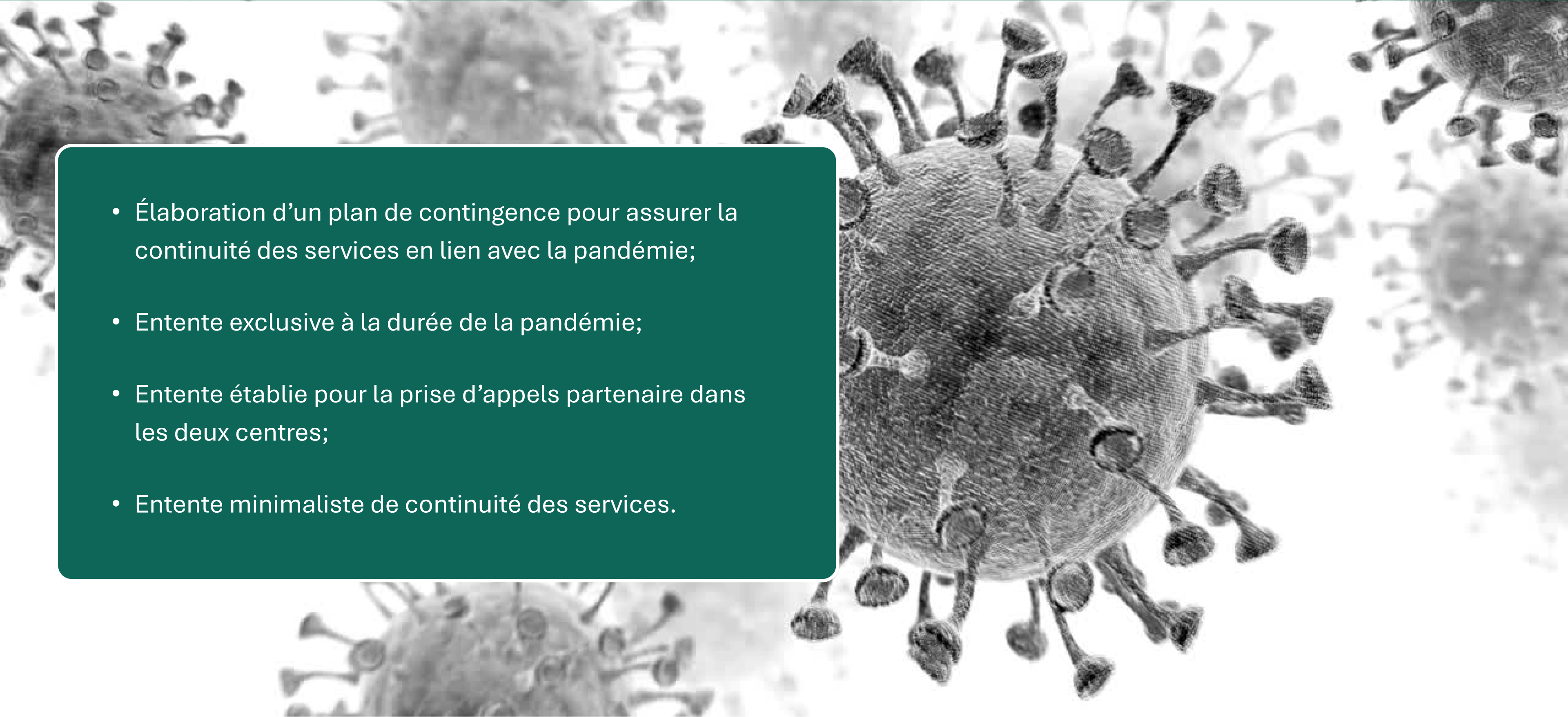
- Surcharge d'appels;
- Coordination logistique;
- Gestion technique en temps réel.

Réponse :

Collaboration intercentre exemplaire, mobilisation rapide des équipes et maintien de la continuité du service 9-1-1 santé.

2020 : Pandémie mondiale

- Élaboration d'un plan de contingence pour assurer la continuité des services en lien avec la pandémie;
- Entente exclusive à la durée de la pandémie;
- Entente établie pour la prise d'appels partenaire dans les deux centres;
- Entente minimaliste de continuité des services.



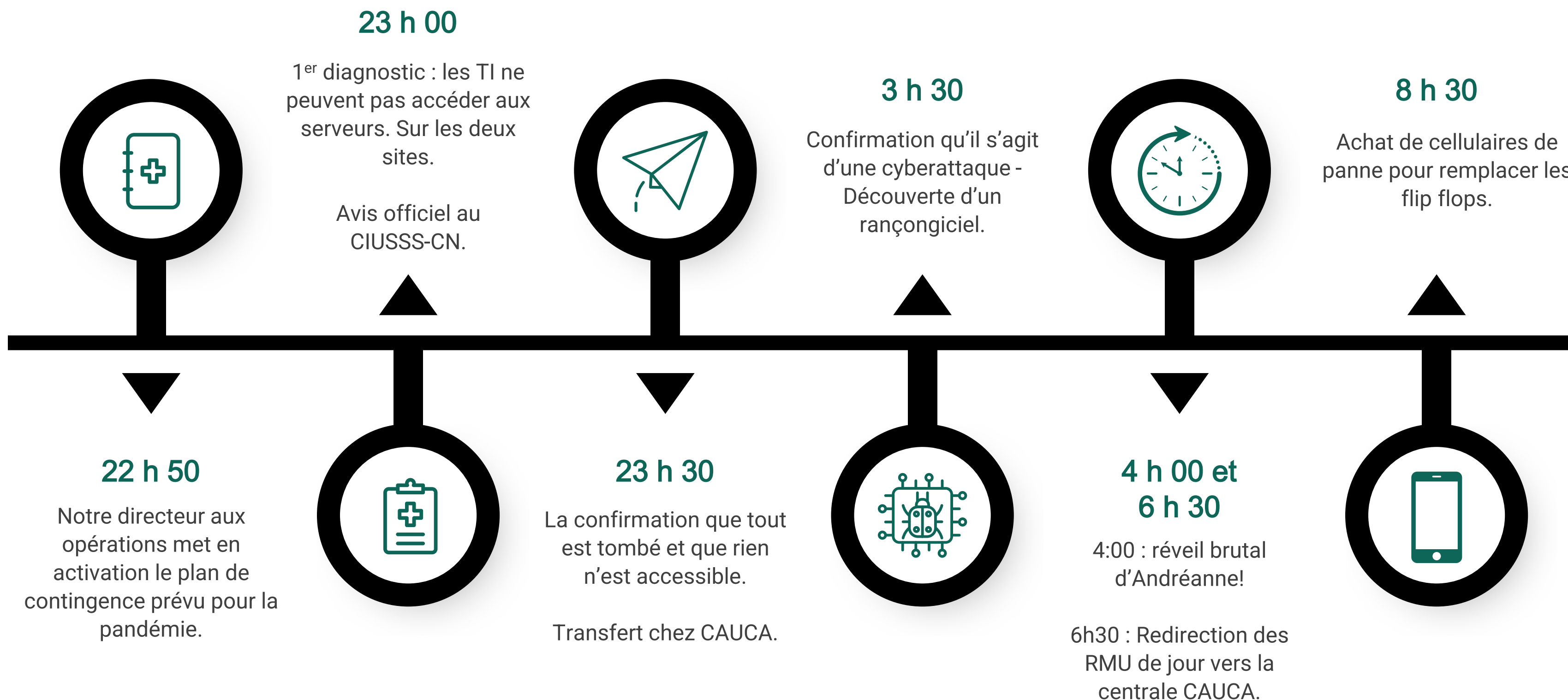
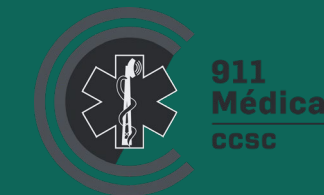
24 janvier 2024 - 22 h 45

La garde informatique est
avisée d'anomalie dans le
système

1^{er} système touché est le
système téléphonique

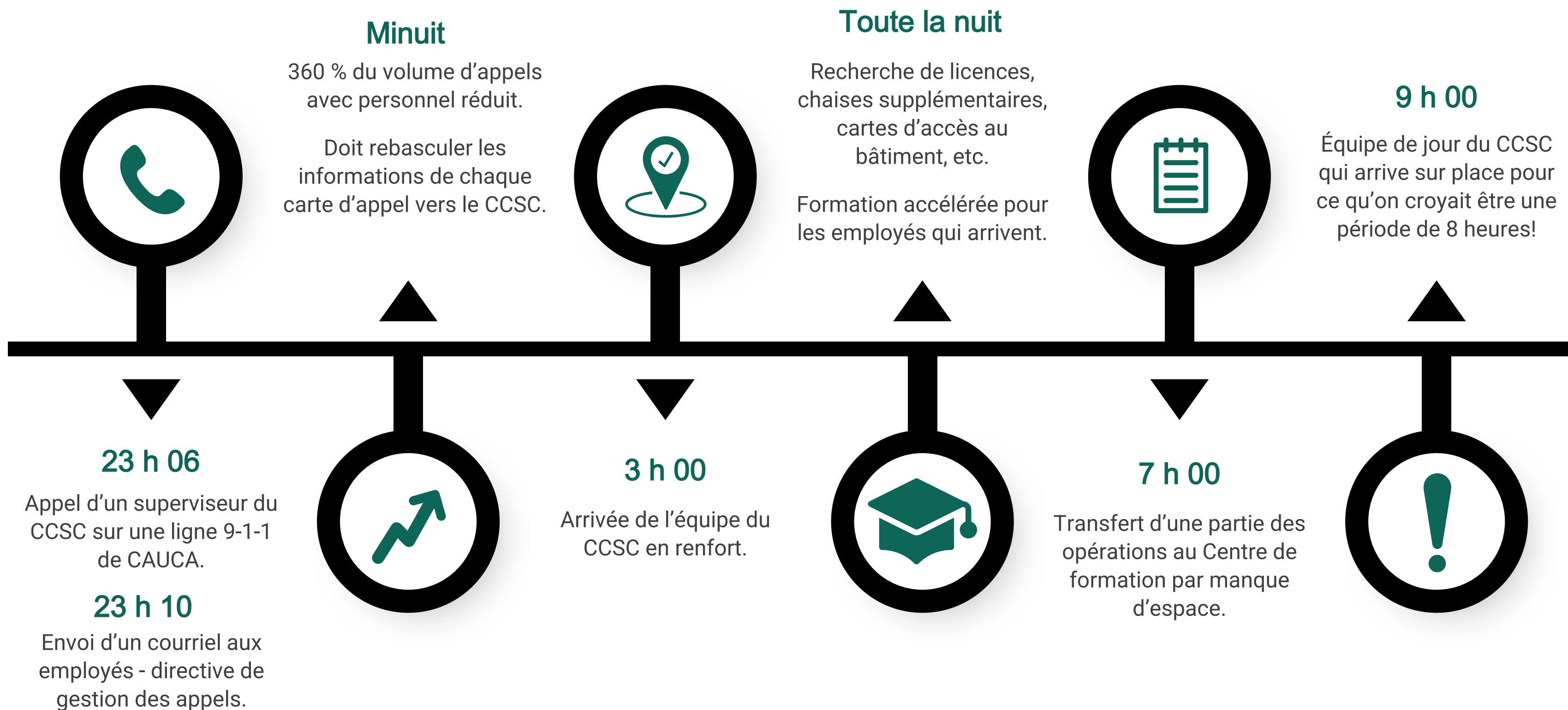
110 postes et serveurs sont
affectés presque
simultanément

Chaque minute compte - CCSC



Chaque minute compte - CAUCA

CAUCA



Déploiement du plan de contingence au CCSC

TOUT EST UNE QUESTION *DEMING*

L'heure à laquelle la panne s'est produite:

- Au CCSC, c'est la transition entre les équipes de soir et de nuit;
- Volumétrie d'appels réduit;
- Circulation fluide;
- Équipe de nuit expérimentée.

FACTEURS DE VULNÉRABILITÉ

- L'heure de la panne (les partenaires la nuit);
- Les deux CCS sont sur des versions différentes de RAQ,
- L'entente de continuité des services n'a jamais été réellement testée.

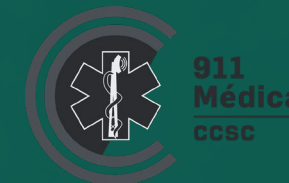
La collaboration : la clé du succès

CAUCA

CAUCA

- Prise d'appels de l'ensemble des secteurs des deux CCS confondus (volume 360 % vs leur moyenne);
- Établir un lien constant avec le CCSC pour transférer les informations des appels.

CCSC



- Faire la répartition manuelle des appels;
- Faire les suivis et ajustements avec tous les partenaires, quotidiennement.

PARTENARIAT

- Soutien indéniable;
- Présence de superviseurs ambulanciers sur le plateau;
- Prêt de tablettes informatiques liées chez CAUCA;
- Encouragements divers;
- Création d'un lien RÉNIR CAUCA-CCSC.

Bons coups des équipes



- La situation a rapidement été jugée critique et le plan de contingence a été déployé;
- Une partie de l'équipe de nuit a rapidement été dirigée vers le CCS CAUCA;
- Le lendemain matin, les RMU qui vont chez CAUCA constituent notre équipe test du NGCAD (version en production de la RAO chez CAUCA);
- Stabilité dans le déploiement de notre équipe.

CAUCA

- Polyvalence des équipes (9-1-1, incendie);
- Postes de travail polyvalents (incendie, santé) 22 postes de travail au total;
- Mobilisation de l'équipe (TI, partenaires);
- Mise en production de la salle de formation;
- Adaptation de l'équipe (accueil, formation sur le pouce, orientation, licences, soutien);
- Mise en place d'une cellule de crise inter-CCS évolutive, selon les besoins.

La résilience des équipes

- Adaptation à des horaires de 12 h;
- Une partie de l'équipe de Québec a quitté le CCSC avec en main une boîte à lunch et est revenue 8 jours plus tard;
- L'équipe RH : coordonne les repas, l'hébergement (contexte de tournoi de hockey);
- L'équipe de CAUCA s'est mobilisée pour que tout se passe le mieux possible;
- Des gens volontaires.

La phase de rétablissement

Collaboration continue :

- Transfert des cartes d'appels de la panne (classement particulier);
- Conservation et transfert des fichiers audio;
- Demande de dérogation à l'Académie pour la perte de données;
- Développement d'une nouvelle entente de continuité des services;
- Rétablissement à mobiliser plusieurs partenaires;
- Rebâtir l'ensemble de la documentation perdue (formation, politiques, grille d'affectation);
- Transformation numérique vers le cloud.

Leçons apprises : nos recommandations

1

Prendre en considération le lieu physique du centre de relève;

2

Établir un plan de déclenchement clair et précis;

3

Exercice conjoint préalable recommandé;

4

Maintien et continuité d'une entente de service;

5

Être prêt à travailler comme en 1990;

6

Version hors ligne du bottin téléphonique, des protocoles et directives, cahiers de référence, etc.



Les questions à se poser en lien avec votre plan de contingence

Où dormirons les équipes?

Avez-vous suffisamment de licences?

Comment avez-vous prévu donner accès à vos bâtiments?

Avez-vous assez de bureaux? De chaises?

Vos lignes peuvent-elle absorber un tel volume d'appels?

Comment les employés vont-ils se connecter chez vous (Login)?

Disposez-vous d'une cartographie du secteur de relève?

Avez-vous les bonnes coordonnées pour les personnes ressources (mouvement de personnel)?

CONCLUSION

- Victime - hasard (brèche dans un hôte);
- Plusieurs autres services d'urgence et hôpitaux aux États-Unis touchés dans la même semaine.

Il nous reste à travailler:

- Plan de continuité des services en répartition;
- Visuel en partage;
- Maintenir une version papier à jour.



Et si tout cela était arrivé
chez un fournisseur RAO?
Quel aurait été le plan?



PÉRIODE DE QUESTIONS - COMMENTAIRES



POUR NOUS JOINDRE



DAVE BOUCHER



ANDRÉANNE DROLET

