Cybersécurité
Vivre une attaque de l'intérieur et préparer la résilience de demain

3 juin 2026 – Assises du numériques

ANNECY

ANNECY

Vincent de Crayencour

3e adjoint en charge de la sécurité
et de la tranquillité publique

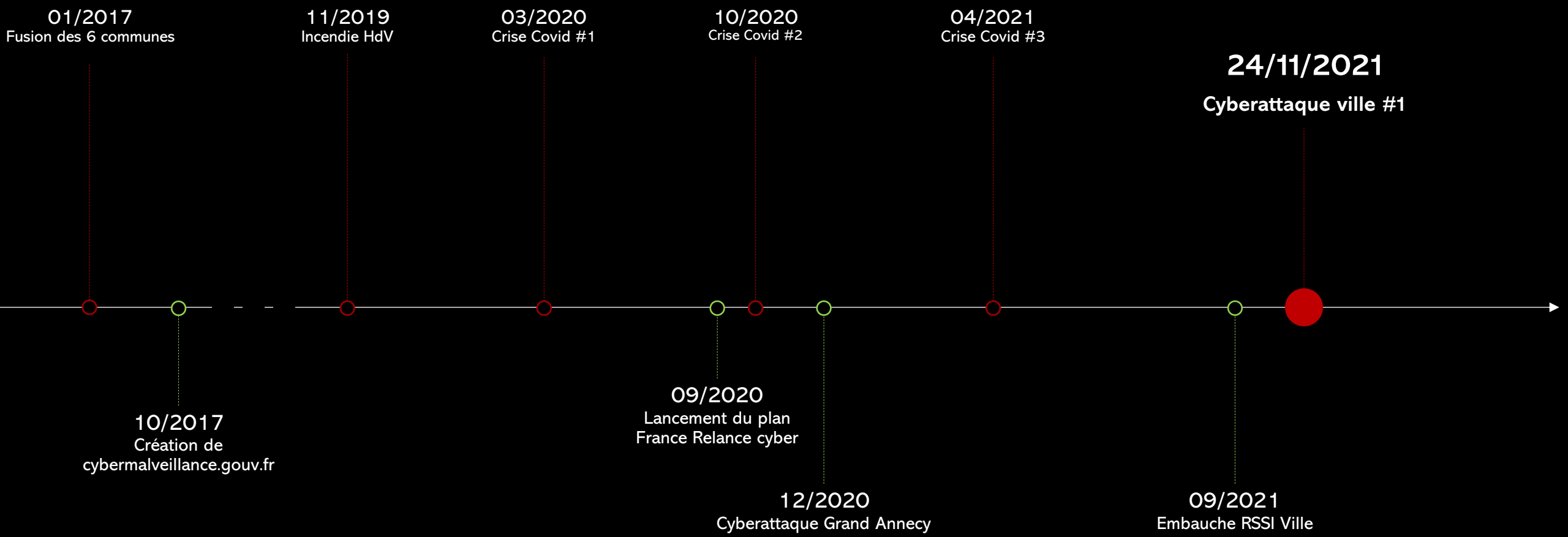
Benoît Christin

Directeur des usages numériques et
des systèmes d'information

Jean-Loup Depoisier

Responsable de la sécurité des
systèmes d'information

L'histoire était écrite…



2009 – Création de l'ANSSI

2015 – Création des délégués régionaux ANSSI

24 novembre 2021 – 10h du matin

Laroche Cyrille <Cyrille.Laroche@ssi.gouv.fr> | Depoisier Jean Loup | 24/11/2021

[CERT-FR] Signalement d'activité malveillantes à l'encontre de votre SI

Il s'agit de la version la plus récente, mais vous avez apporté des modifications à une autre copie. Cliquez ici pour afficher les autres versions.
Vous avez transféré ce message le 16/12/2021 16:39.

Bonjour,

L'ANSSI [1] a été destinataire d'un signalement concernant des activités potentiellement malveillantes sur un SI potentiellement sous votre juridiction ou lié au votre.

Le 2021-11-23 à 22:25:15 (UTC), une machine nommée SRV-DC1$ appartenant au domaine AD ANNECYCN aurait communiqué vers de l'infrastructure malveillante liée à un attaquant rançongiciel. A tout hasard, je vous transmets l'adresse IP finale de l'attaquant 46.166.161[.]93 mais il est probable que ce dernier ait communiqué via un réseau d'anonymisation comme un VPN ou Tor.

En cherchant, nous avons trouvé le nom de domaine annecycn.fr qui semble correspondre et avons constaté que les registres MX de ce nom de domaine pointaient vers des sous-domaines de ville-annecy.fr et, jadis, de agglo-annecy.fr. Nous pensons donc que vous pouvez être en capacité d'identifier le réseau touché et la machine infectée.

Les communications identifiées sont faites par un code malveillant nommé SystemBC, qui est notamment utilisé en dernière phase d'attaque par des attaquants rançongiciel. Il y a donc de forte chance que ce réseau soit en danger imminent de se faire chiffrer. Si vous disposez d'interconnexions avec ce SI, il n'est pas impossible que votre propre réseau soit également en danger. Je ne peux donc que vous recommander d'identifier avec diligence, au mieux de vos capacités, le réseau concerné et avertir son gestionnaire.

Une première mesure d'urgence que vous pouvez conseiller au responsable du réseau compromis si vous l'identifiez est de lui dire de déconnecter ses sauvegardes de son réseau si ce n'est pas déjà le cas pour empêcher une perte totale de données au cas où il n'arriverait pas à endiguer les actions de l'attaquant.

Cordialement,

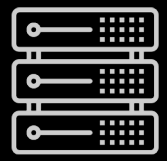
Là encore, l'histoire était écrite…

Login / mot de passe d'un utilisateur

Mot de passe jamais changé depuis l'arrivée (mot de passe par défaut de création du compte)

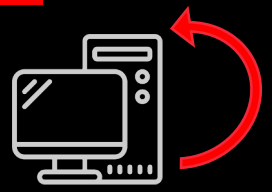
Absence de filtrage

Faible sécurité des postes de travail



Mauvaise architecture réseau

Propagation



Utilisateur administrateur de sa machine

Récupération de tous les comptes connectés sur la machine

Récupération du compte admin du domaine

Administrateur du domaine

Mauvaises pratiques d'administration

Les premières heures critiques

ANNECY

Confirmation de l'intrusion

Déconnexion de l'ensemble de nos sauvegardes

Coupure des accès internet et interruption de tous les services rendus

Déclaration d'un incident sur cybermalveillance.gouv.fr

Prise de contact avec un prestataire spécialisé en réponse à incident

Communication Comité exécutif

Ouverture des cellules de crise internes (stratégique et opérationnelles)

Ouverture des mains courantes de réponse à cyberattaque

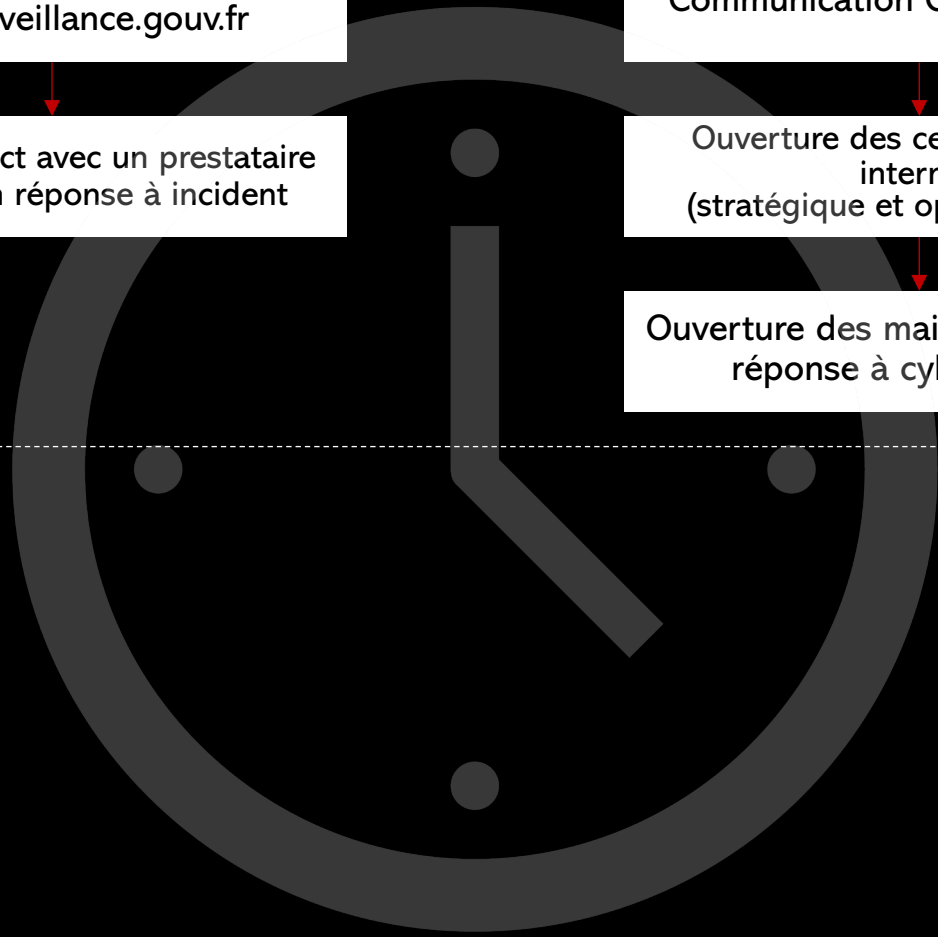
24/11

25/11

Oubli d'un accès

Déclenchement du ransomware

Arrêt brutal de tout le SI de gestion



Des services municipaux sans outil numérique

- Qui mange à la cantine à midi ?
- Mais au fait, qu'est qu'on mange à midi ?
- Je viens déclarer la naissance de mon enfant
- Je souhaite enterrer un défunt
- Il reste de la place dans ce parking ? Chouette, c'est gratuit !
- Vous êtes sûr que vous aviez réservé pour cette pièce de théâtre ?
- Désolé, nous ne pouvons plus assurer de prêt de livres…ni prendre vos retours de livres
- Euh, il se ferme comment l'hôtel de ville de Seynod ?
- …

Ça c'était en 2021, en 2026 la liste des services publics numérisés s'est bien allongée…

L'opportunité

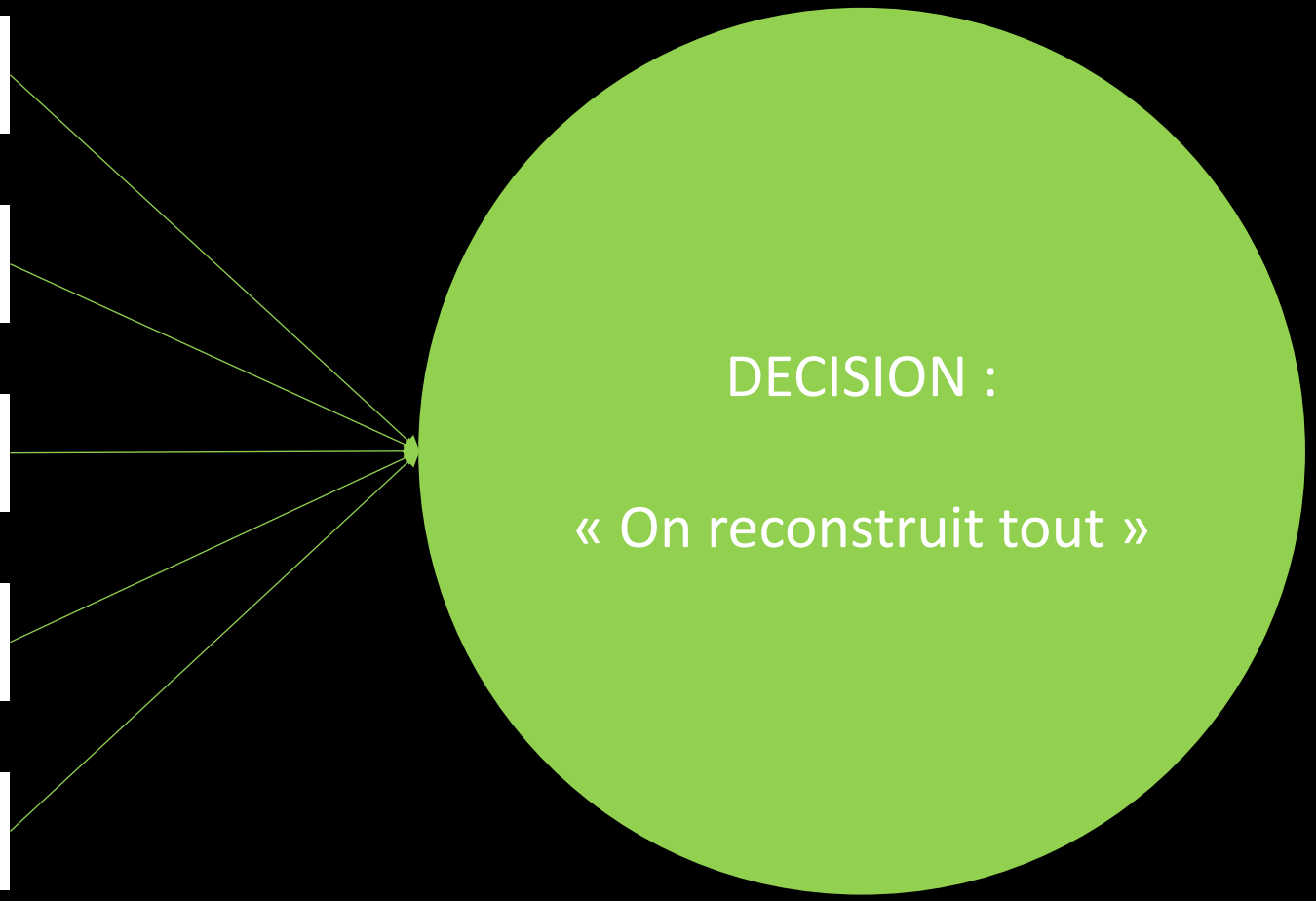
L'**ensemble du SI est touché**, impossible de distinguer avec certitude ce qui est bon de ce qui ne l'est pas

L'état de **faiblesse extrême du SI** ne permet pas de redémarrer

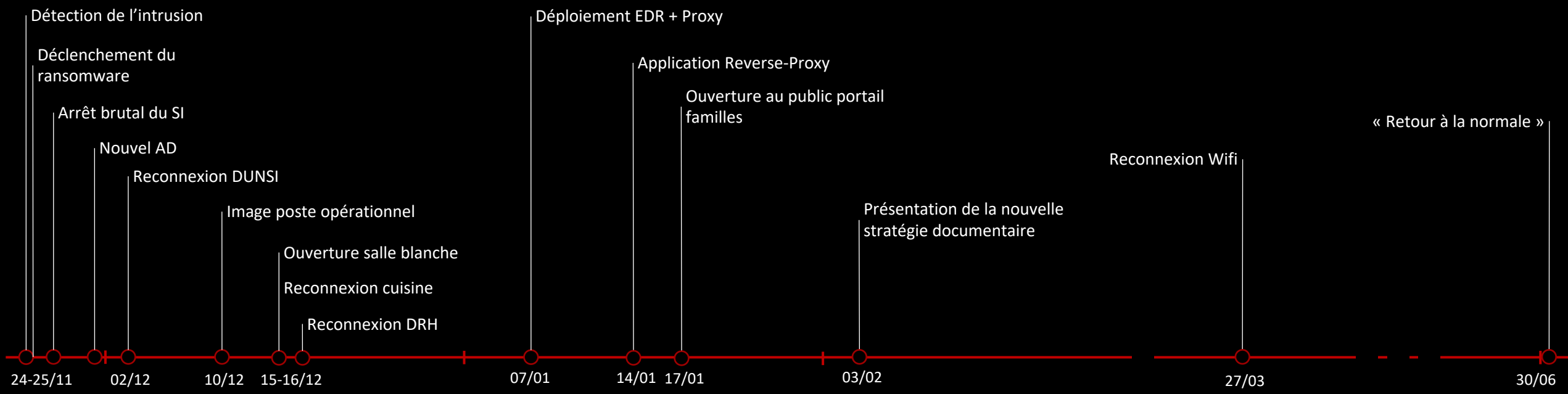
La DUNSI dispose d'un **plan long terme détaillé de remise à niveau de TOUT le SI**

La direction générale de la collectivité accorde une **confiance totale** au tandem DSI/RSSI

La ville d'Annecy n'est **pas soumise à la pression économique** du secteur privé



Les premières semaines



En 3 mois

- +90 sites reconnectés
- +1900 postes collectés
- +1200 postes masterisés et redistribués, avec formation des agents
- +60 applications reconstruites, testées et réouvertes
- +60 applications reconstruites, testées et réouvertes

7 mois

pour retrouver un fonctionnement normal

4 ans après…

- Vive la cyberattaque !
  - 7 mois de travail intense de reconstruction méthodique pour 4 ans de tranquillité (et plus si possible)
  - Un SI à l'état de l'art
  - Un SI maîtrisé, s'appuyant sur un ensemble de socles, apte à être développé
- Des impacts RH importants à la DSI : 1/3 de turnover
  - Nouvelles méthodes de travail
  - Nouvelle organisation
  - Montée en expertise des profils
- Une bonne maturité organisationnelle, méthodologique et opérationnelle
- Prise en compte des enjeux de l'informatique industrielle
- Le souvenir s'efface côté utilisateurs et décideurs
- Il est toujours difficile d'intégrer le numérique dans les discussions stratégiques

Demain…

- La ville est et sera de plus en plus « connectée »
  - Augmentation de la surface d'attaque
  - Plans de résilience (exemple du tunnel courrier)

- Les menaces et les outils évoluent…plus vite que les protections
  - Maintien et développement du niveau de sécurité
  - Nouvelle réglementation NIS2

- Souveraineté? Contraintes économiques?
  - Maintien des compétences
  - Maîtrise interne des systèmes
  - Ecosystème de fournisseurs

- Coordination / Coopération de territoire, sur le bassin annécien voire sur la Haute-Savoie