

Conférence Innovative City 2015



Table ronde « Cybersécurité : enjeu majeur de la transformation numérique et de la transition énergétique »

Smart City et cybersécurité

Patrick CHAMBET
Métropole Nice Côte d'Azur

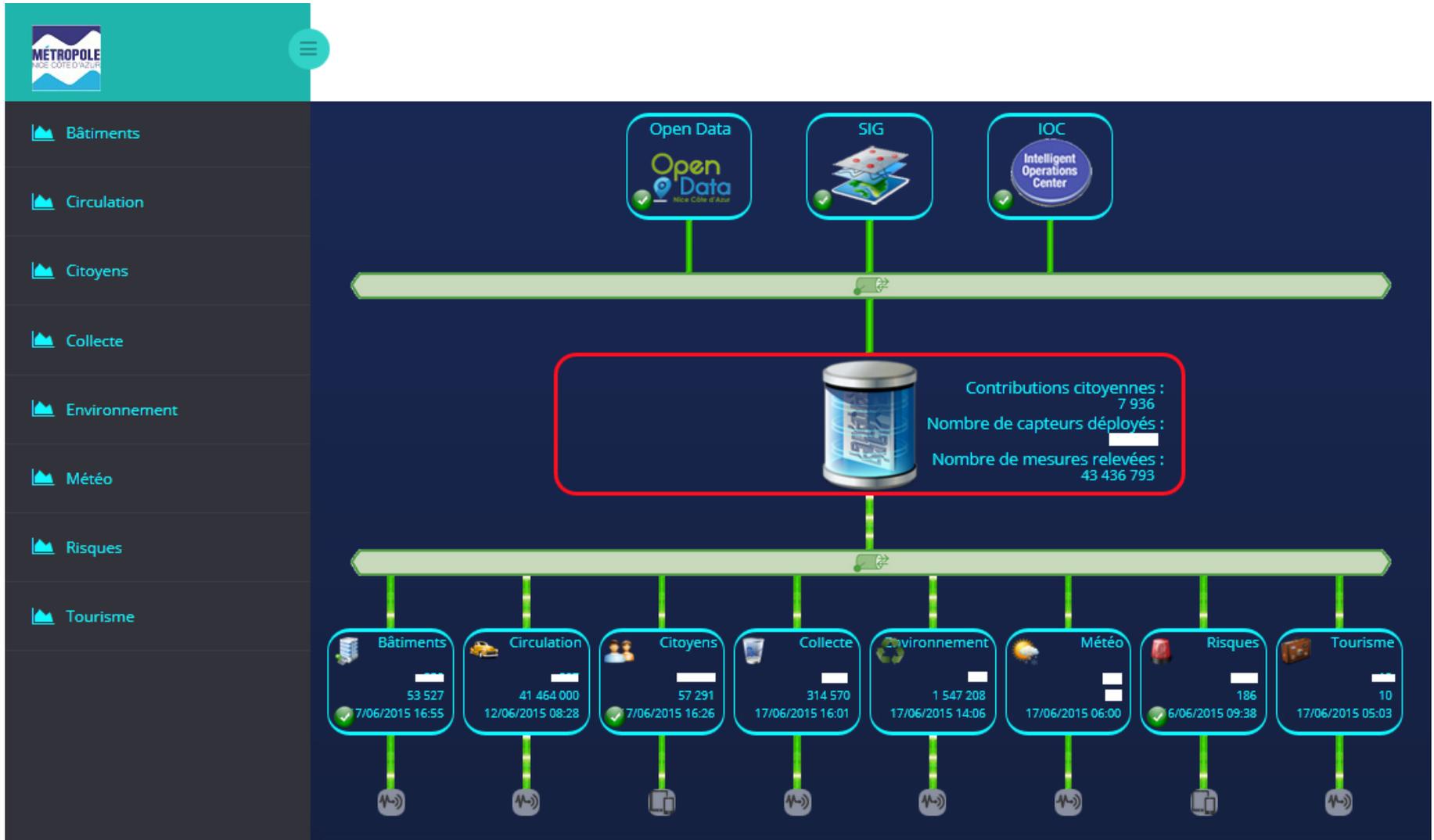


- **Il ne peut y avoir de Smart City ou de transformation numérique en général sans sécurité des informations échangées et stockées**
- **Rencontre de nombreux dispositifs venant de mondes différents**
 - Capteurs / actionneurs / objets connectés
 - Gestion technique bâtementaire (GTB)
 - Systèmes géographiques
 - Systèmes industriels / automates / SCADA
 - Informatique et réseaux
 - Applications participatives
- **Il faut faire dialoguer les différents acteurs en confiance, et donc de manière sécurisée**

Smart City: capteurs



SmartCity: collecte et stockage des données issues des capteurs



Smart City: supervision



- « **D I C T** »
- **Disponibilité des équipements et des données**
 - Capteurs
 - Actionneurs
 - Systèmes de gestion et de pilotage
- **Intégrité des données**
 - Confiance dans les mesures remontées par un capteur: pas de perturbation parasite ou de modification en chemin
- **Confidentialité des données**
 - Protection des données collectives
 - Protection des données individuelles (vie privée / CNIL)
- **Traçabilité**
 - Qui/quoi a effectué quelle action, quand et depuis où ?

- **Sécurité périmétrique**

- Réseaux privés non accessibles depuis Internet
- Filtrage réseau (firewalls)
- Protection des applications Web publiées

- **Défense en profondeur**

- Protection des flux échangés (interopérabilité des protocoles, chiffrement)
- Protection intrinsèque des équipements contre les attaques et détournements
- Contrôle d'accès aux équipements
- Protection des données (dans les applications et les bases de données)
 - Données anonymisées
 - Stockées dans un entrepôt de données dédié
 - Dans des Data Centers situés en France

- **Supervision de la sécurité**

- Détection d'intrusions
- Détection et correction des vulnérabilités (scans, audits)
- Gestion de crise et réponse sur incident

- **Gouvernance de la sécurité**

- Evaluation des risques
- Politique de sécurité
- Sensibilisation des acteurs à la cybersécurité
- Intégration de la sécurité dans les produits, les équipements, les contrats
 - Travail avec les constructeurs et les éditeurs de logiciels
 - Ajout de clauses de sécurité dans les contrats avec les partenaires

→ On applique la même méthodologie que pour les SI traditionnels

- L'essentiel est de bien les choisir... 😊



- **La cybersécurité ne vient pas empêcher ou gêner la circulation des données**
- **Au contraire, elle vient l'accompagner et l'améliorer, du fait de la meilleure confiance que les différents acteurs peuvent avoir dans les données échangées**
- **C'est pourquoi il ne peut y avoir de développement de la Smart City sans conception en amont des principes de sécurité à mettre en œuvre**
- **Les citoyens sont de plus en plus en demande de sécurité autour de leurs données et de leur vie en général**
 - Cf affaire Snowden
 - Pas de « low cost » dans ce domaine

QUESTIONS ?

Patrick CHAMBET
Responsable de la Sécurité des SI
Métropole Nice Côte d'Azur
Membre du CA du CESIN