RETEX
Cyber-attaque
du 12/10/23

GEOSDIS 2024 - Pau - du 26 au 28/03/2024

SDIS 64
Sapeurs-Pompiers
Pyrénées-Atlantiques

Ordre du jour

> Cyberattaque

- Contexte SSI
- Remédiation / Reconstruction
- Adaptation SIG
- SGO
- Conclusion

SDIS 64

Cyberattaque – Contexte SSI

> 12/10/2023 : Détection de l'attaque

- Attaque du SI SDIS 64 par cryptogiciel de forte ampleur avec des impacts majeurs :
  - > Détection du virus par le plateau CTA et l'astreinte GDSI dans la nuit avec pour symptômes un changement de fond d'écran sur un bureau à distance et de forts ralentissements START
  - > Transversalité de l'attaque sur le SIAF et le SIOP par le biais d'une passerelle technique entre les deux SI
- Causes de l'attaque : vol d'identifiants d'un compte SPV via leak de données sur un réseau externe
- Perte totale de l'administration des infrastructures par le SDIS64 due à la violence de l'attaque
- Diagnostic et plan de remédiation de l'attaque fait par les équipes IR de la société Airbus Protect sous mandat ANSSI et le GDSI du SDIS 64

SDIS 64

Cyberattaque – Contexte SSI

> Qu'est-ce qui change ou va changer?

- On reconstruit nos Systèmes d'Information suivant 4 principes :
  - > Repartir sur ce qu'on avait mais en plus sécurisé
  - > Respecter les préconisations en matière de sécurité de l'ANSSI
  - > Anticiper la Directive NIS2
  - > Anticiper la compatibilité avec NexSIS
- Politique de mots de passe
- Plus de port USB pour le stockage
- Gestion des accès à nos SI, mise en œuvre de bastions (SIAF et SIOPE)
- Séparation complète des SIAF et SIOP
- Tiering de l'AD
- Respect du guide d'hygiène de l'ANSSI

SDIS 64

Cyberattaque – Contexte SSI

> Plan de remédiation

- En toute première urgence :
  - > Externalisation de tous les applicatifs hébergeables par les éditeurs
  - > Externalisation du SIOPE à J+2 de l'attaque (reprise partielle de l'activité numérique)
  - > Dématérialiser tous les flux métiers éligibles
  - > Priorisation du fonctionnement « essentiel » du SDIS64
- Remise à plat totale des deux infrastructures :
  - > Ré-adressage de tout le réseau
  - > Création d'un nouveau domaine
  - > Renouvellement matériel de tous les équipements obsolètes (Serveurs, PC, …)
  - > Redesign des architectures (tiering, sauvegardes, échanges de flux AF – OPE)
  - > Reconstruction from scratch des AD (OPE ET AF)

SDIS 64

Adaptation SIG

> Comme tous les services, RAZ

- En toute première urgence :
  - > SIG fait partie du GDSI donc aide aux autres services :
    - Récupération de tous les PC et équipements numériques en vue de reboot complet
    - Paramétrage copieurs
    - Inventaires…
  - > Distribution des équipements blancs
- Inventaires des données rapidement mobilisables :
  - > OpenData : Hydrants via GIP
  - > ESRI : jeu de données test de juin 2023
  - > BD Topo IGN

SDIS 64

Adaptation SIG

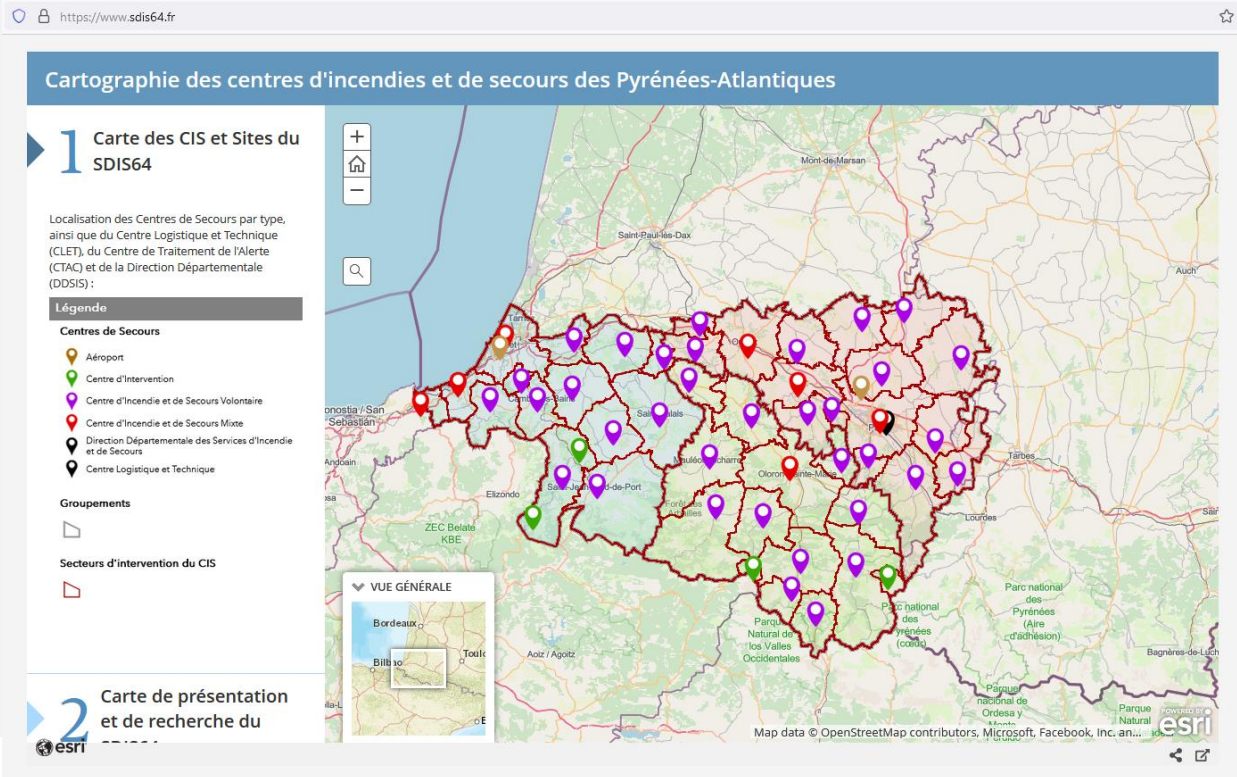
- Constat de l'utilité de garder du papier en ultime secours :
  - > Cf nos discussions du GéoSDIS2023 : Numérique/papier
  - > Plus de géoweb, ni appli webcarto
  - > Les CIS reçoivent les inters par tel
  - > Cherchent le lieu ou la voie dans l'index
  - > Et localisent sur le plan mural et dans l'atlas
  - > Guidage GPS au carreau 400m toujours possible…



Adaptation SIG

> Comme tous les services, RAZ

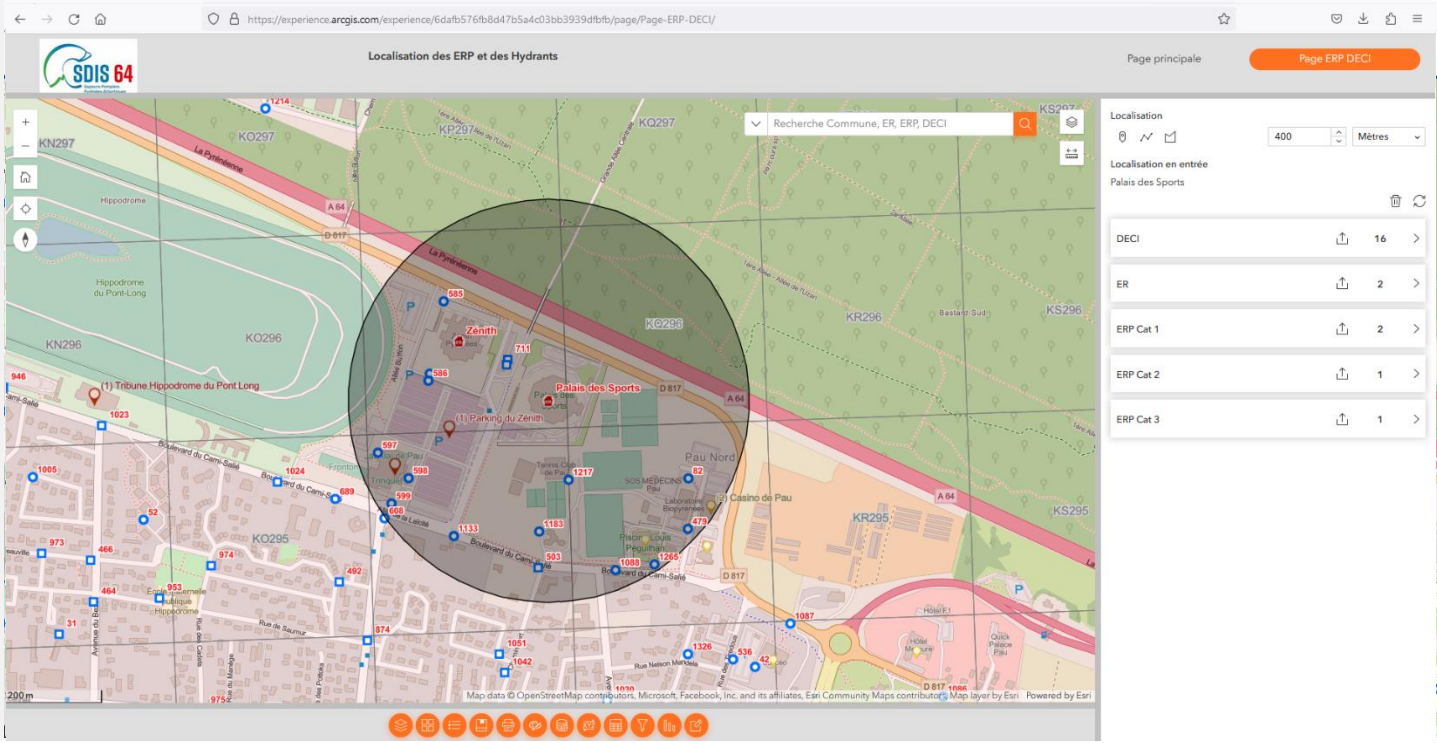
- Récupération d'un PC blanc pour le SSIG
- Reconstruction sur AGOL
  - > Carte de présentation du SDIS sur site sdis64.fr
  - > Application de recherche de lieux/voies pour le CTAC



Adaptation SIG

> Création d'applis sous AGOL

- Tests d'Expérience Builder
  - > Recherches Hydrants
  - > Recherches ERP
  - > Remontées
  - > Suivi de modifs…



Adaptation SIG

> Résilience en attendant le retour progressif à la normale

- Lien IGN pour démonstrateur : appariement BD routes SDIS/BD Topo
- Stage Tech SIG en avril 2023 avait dégrossi le sujet
- pas de màj possible : faire le maximum du rapprochement
  - > Problématiques des doublons en limites de voies
  - > Identifier les apports du SDIS64
  - > Commencer à analyser les divergences
  - > Test Espace co, plug in QGIS
  - > Définition stratégie remontées
  - > Les données à continuer à gérer en interne (ZICAD, Espagne…)
- Automatisation récupération des données IGN pour màj via FME
  - > Appropriation et adaptation script SDIS81

SDIS 64

Adaptation SIG

> Retour progressif à la normale

- Récupération BD SQL-Server (sv du 7/10/23) le 16/01/2024
- Déploiement de nouveaux serveurs + tiering
- Récupération sauvegarde cartes, atlas (aprx, pdf,) et données (gdb, shapes…)
- Nouvelles demandes de cartes à la demande (zones de desserte, localisation, plans, atlas DFCI)
- Mise en place du nouveau portal (v11.1) à compter du 23 Mai
  - > Montée de version
  - > Remise en place des applis principales (recherche, risques…) via Expérience Builder
- Applications web : évènements importants
  - > Fêtes de Bayonne : du 10 au 14/07/24
  - > Tour de France : 13-14/07/24

SDIS 64

Lien Start et suites à donner

> Réinternalisation courant 2024

- Sur des serveurs SDIS
- Remise en place d'un GéoConcept
- Remise en place d'un géoweb, de la cartodb (Oracle->Sql Server)
- Acquisition de géodataweb pour les transferts
- Scripts FME pour suivi et comparaison des mises à jour
- Acquisition d'un logiciel de gestion des PEI

> Conclusion et ouverture

- Encore beaucoup de projets en cours, à reconstruire, tout en gérant les besoins quotidiens

SDIS 64

MERCI
DE VOTRE
ATTENTION



Contact :

sebastien.boyer@sdis64.fr

adrien.carpentier@sdis64.fr