MISE EN PLACE D'UN SOC, EN RÉPONSE À UN INCIDENT DE SÉCURITÉ EN JUILLET 2021

Retour d'expérience

Arnaud HAUWELLE, Maire de Villepinte

Mélanie MARQUES, AISI

VILLE DE VILLEPINTE

AISI Pure player Infrastructure & Cybersécurité

AISI Pure player Infrastructure & Cybersécurité

ORDRE DU JOUR

1. Contexte
2. Intervention
3. Temporalité
4. Mise en place du SOC

1. Le Contexte

DINSI

La Direction de l'Innovation Numérique et des Systèmes d'Information

Gère l'infrastructure et les services informatiques mis à disposition des employés de la Ville de Villepinte.

- Services de la Mairie : état civil, paie, RH, reprographie, etc.
- Services publics : écoles, police municipale, vidéosurveillance, etc.
- Services mutualisés : messagerie, backup, WI-FI.

Equipe informatique à taille humaine

- 1 DSI
- 2 ETP avec un niveau d'ingénieur / admin
- 2 techniciens de proximité

Pure player Infrastructure & Cybersécurité

1. Le Contexte

Alerte remontée le soir du 29 juin par le prestataire de vidéosurveillance

= un serveur d'infra a été chiffré.

De suite l'équipe IT a coupé les accès internet =

SI complètement Offline et plus aucun service rendu.

=> Bonne pratique

L'équipe IT a ensuite constaté les preuves de la présence des attaquants.

Pure player Infrastructure & Cybersécurité

1. Le Contexte

Soumission de l'incident
sur la plateforme
Cybermalveillance.gouv.fr
mise en relation avec AISI

=> Bonne pratique

Déclenchement d'une réponse
à incident de sécurité.

Conférence de cadrage
envoi sur site de l'équipe AISI
assistée par ExaTrack

Pure player Infrastructure & Cybersécurité

2. L'Intervention

DEUX CHANTIERS EN PARALLÈLE

ANALYSE FORENSIQUE

ExaTrack

- Le patient zéro, le vecteur d'infection initiale, les mécanismes de propagation, les souches virales utilisées
- Le groupe d'attaquants ainsi que leurs techniques, tactiques et procédures (TTPs) à partir des observables.
- Etablir une timeline des attaquants et rédaction d'un rapport.

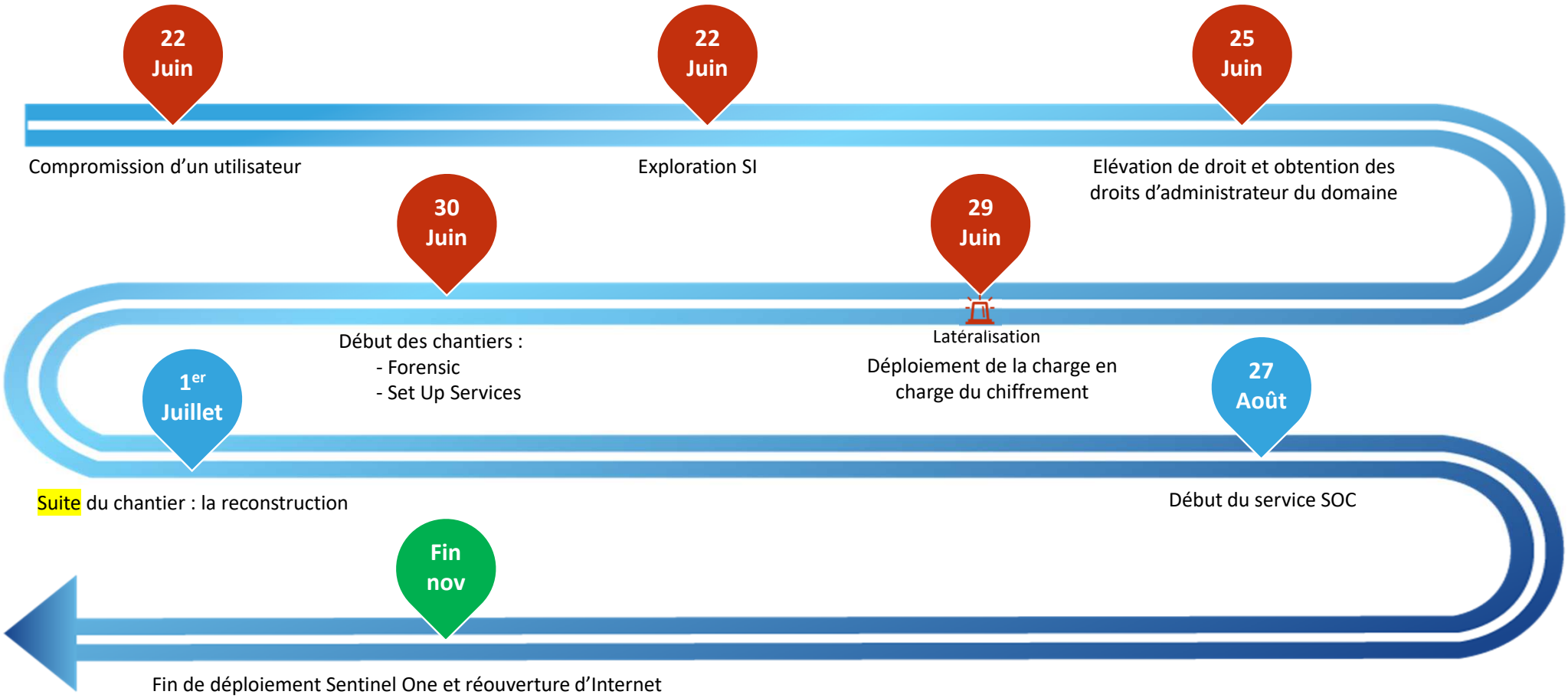
RECONSTRUCTION PARTIELLE DU SI

AISI Pure player Infrastructure & Cybersécurité

- Relancer les services définis comme prioritaire (chaîne critique).
- Construire les fondations d'une nouvelle infrastructure moins sensible aux attaques.

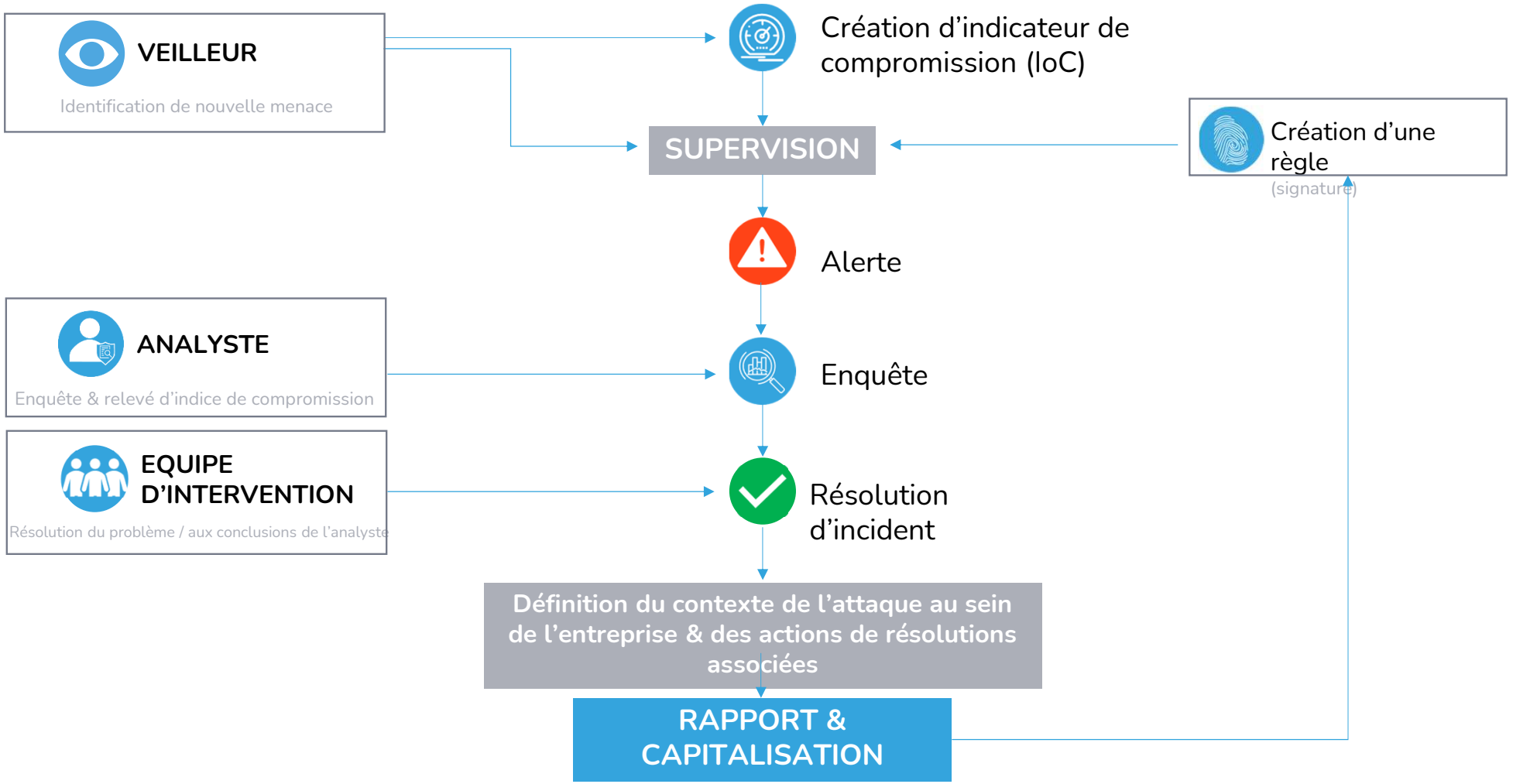
AISI Pure player Infrastructure & Cybersécurité

3. Temporalité



Pure player Infrastructure & Cybersécurité

4. Mise en place du SOC, COS



Pure player Infrastructure & Cybersécurité

4. SOC : Outillage – Détection & Réponse

SCOUT

Récupération des éléments d'enquêtes

Récupération des :

- Ruches systèmes et utilisateurs
- Logs systems
- Fichiers suspicieux
- Fichiers systèmes utiles (USN,...)
- Connexions réseau
- Des processus avec leurs propriétés

COMMODORE

Traitement de masse des archives chiffrées

- Analyse et traitement des ruches
- Analyse et traitement des logs
- Analyse des fichiers suspicieux
- Enrichissement de données
- Mis en format homogène Json (récupérable par pandas)

THE EYE

Visualisation et traitement par l'analyste

- Basé sur ELK
- Intégration des sorties de Commodore
- Visualisation de Dashboard pour aider l'Analyste
- Recherche par mot clé dans l'ensemble des traces

HUNTER

Répond à l'incident

- Supprime le maliciel
- Supprime les traces de persistance (les taches planifiées, les services, les clés de registre, les objets WMI,...

Merci !

Avez-vous des questions ?

Pure player Infrastructure
& Cybersécurité