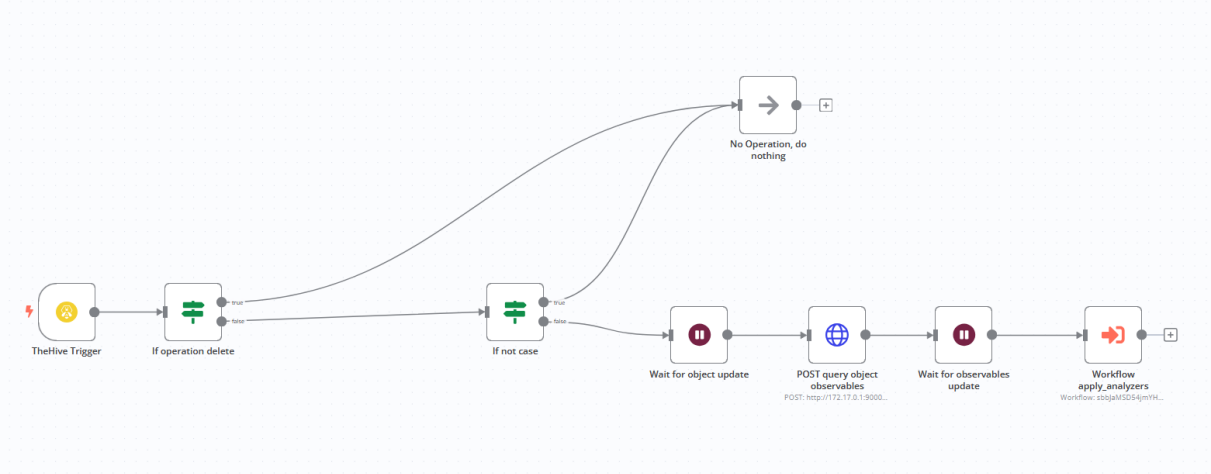
CAPTURES D'ECRAN : N8N, THEHIVE ET SPLUNK

Novembre 2024

Table des matières

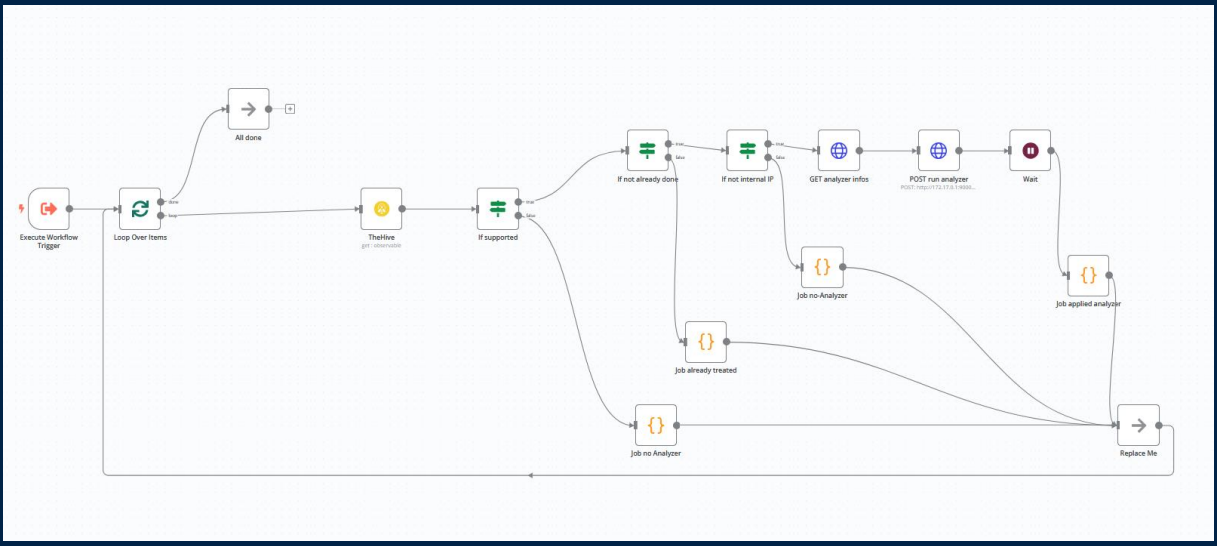
Workflow N8N

Workflow Principal



- Le workflow trie les événements pour ne considérer que les créations et mises à jour de *cases* (`case_create` et `case_update`) dont il récupère les observables avec le nœud « `POST query object observables` ».
- Il est quand même à l'écoute de tous les événements TheHive (via un Webhook) : on peut ainsi le modifier pour s'appliquer à d'autres événements si nécessaire.
- Le workflow « appelle » un sous-workflow dédié à l'exécution des analyzers (voir ci-dessous). L'idée de définir un sous-workflow spécifique est de pouvoir l'appeler plusieurs fois par exemple si on décide d'étendre le workflow principal à d'autres événements TheHive.

Sous-workflow d'exécution des analyzers Cortex



- Le sous-workflow d'exécution des analyzers boucle sur les observables listés dans le workflow principal.
- Pour chaque observable, le sous-workflow détermine si le dataType est pris en charge (par l'un des analyzers) et s'il a déjà été traité précédemment dans ce *case* en vérifiant la présence d'un tag spécifique « cortex analyzer ».
- Si ces deux tests sont passés, le workflow exclue les IP internes pour qu'elles ne soient pas soumises à l'analyzer de réputation d'IPs, identifie l'analyzer adéquat et l'exécute (Nœud « `POST run analyzer` »).
- Quand tous les observables ont été traités par le workflow, la branche « `Done` » est suivie et le processus termine.

Résultats du workflow

1er *case*

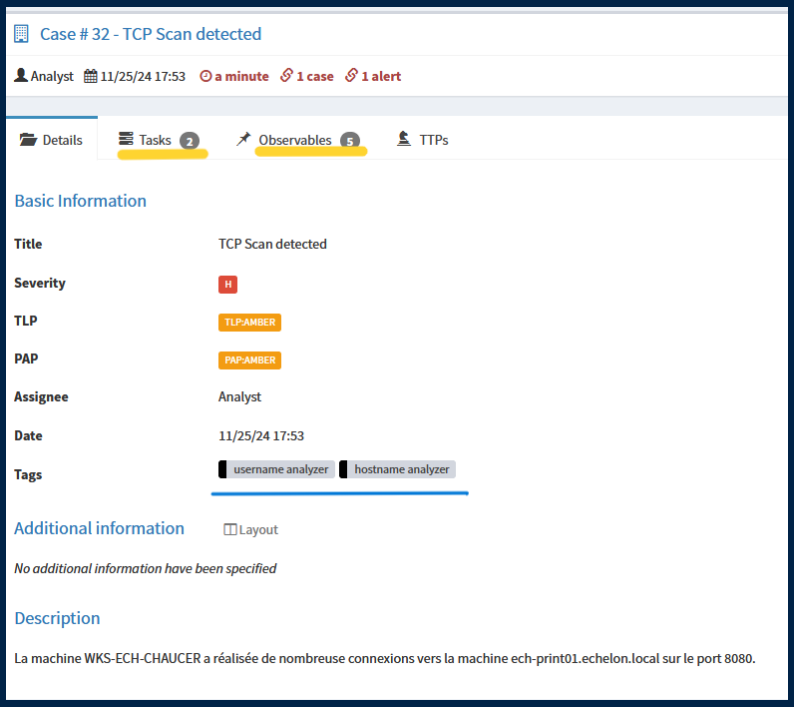


Figure 1 Vue d'ensemble case

On peut voir que le *case* est mis à jour avec 2 tags informatifs et la création de 2 *tasks*.

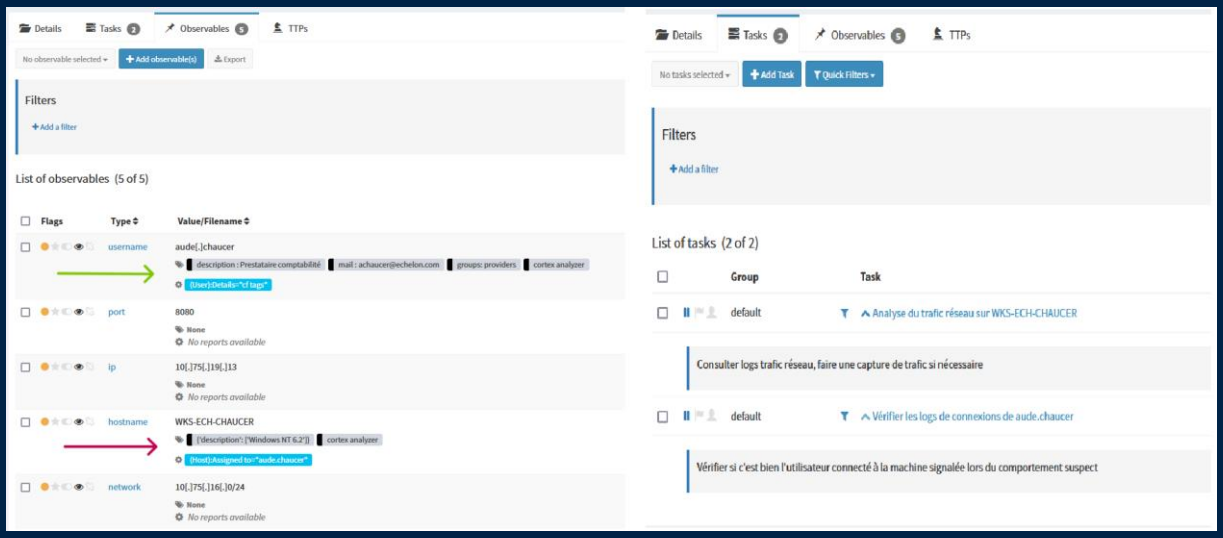


Figure 2 Enrichissement des Observables et création de Tâches

L'observable `hostname` est analysé : le champ « `description` » est tiré de l'annuaire OpenLDAP et ajouté aux tags et le nom d'utilisateur est extrait pour créer un nouvel observable de type `username`. Celui-ci est à son tour analysé et enrichi avec les informations qui le concernent dans OpenLDAP

Chaque analyzer provoque la création d'une tâche spécifique à l'observable analysé.

2e *case*

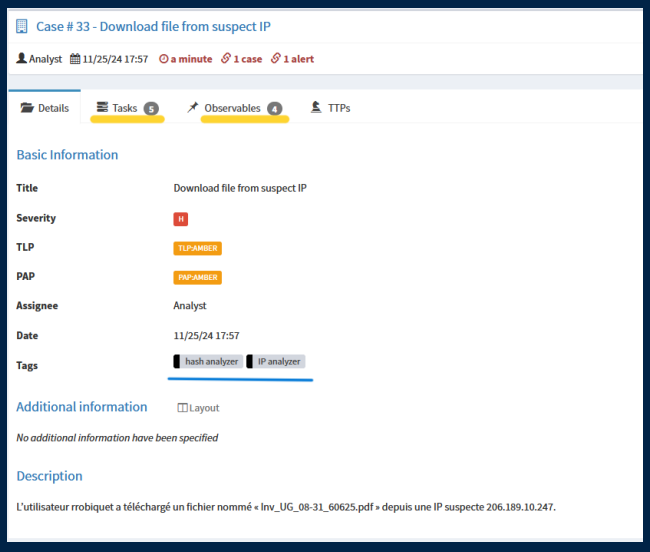


Figure 3 Vue d'ensemble case

Mise à jour du *case*, similaire à l'exemple précédent.

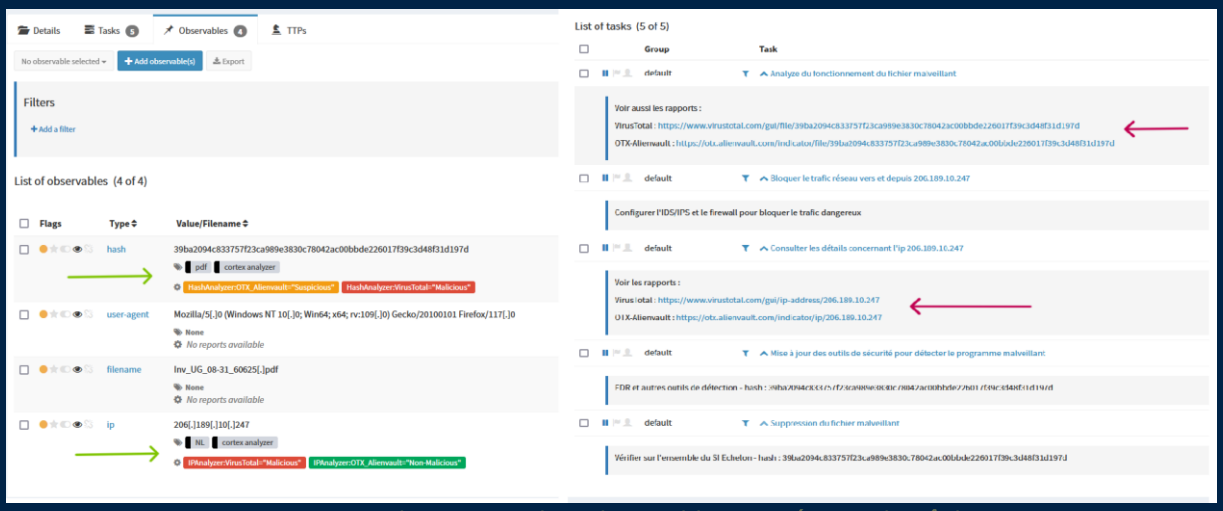
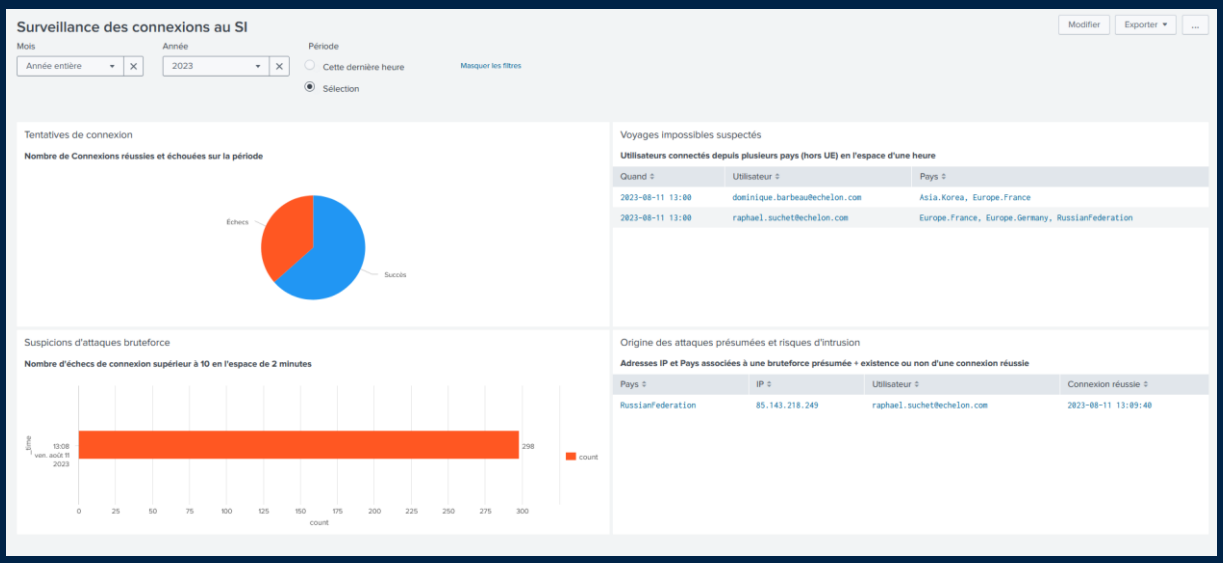


Figure 4 Enrichissement des Observables et création de Tâches

Les observables sont enrichis avec : un résumé des réputations trouvées via les sources externes (avec code couleur selon les réputations) + des tags (`pays` pour l'observable `IP` et `type de fichier` pour l'observable `hash`).

Chaque analyzer créé les tâches prévues en cas de présence de réputations « malicieux » ou « suspect ». Les adresses des rapports des sources externes sont incluses en description.

Dashboard Splunk



Le tableau de bord présente des données relatives aux tentatives de connexion au SI d'Echelon. Les données sont visualisées en relation à une période choisie en haut du tableau de bord :

- « Cette dernière heure » : offre une vue plus ou moins en temps réel
- « Sélection » : Sélection par année et par mois, avec la possibilité de visualiser une année dans son entièreté.

Le tableau de bord est divisé en 2 parties (supérieure et inférieure) avec 2 panneaux pour chaque parties :

- Partie supérieure :
  - Répartition des Echecs et Réussites de connexions – à gauche.
  - Relevé de suspicion de « voyages impossibles » (connexions dans et hors UE en l'espace d'une heure) – à droite.
- Partie inférieure :
  - Suspicions d'attaques par bruteforce (nombreux échecs de connexion sur un intervalle prédéfini) – à gauche.
  - Relevé des sources des attaques présumées par bruteforce : adresses IP, pays, nom d'utilisateur concerné, et présence ou non de connexion(s) réussie(s) par la même adresse IP – à droite.