Rapport

24/02/2025 - R6.CYBER 04 - RÉPONSE À INCIDENT

MAHADALI Neil

DUFOSSE Jacob

DITTOO Farhan

PIGNOLET Matthieu

Sommaire

Introduction

1. Introduction

Contexte et Problématique

Les attaques de phishing représentent l'une des menaces les plus courantes en cybersécurité, exploitant l'ingénierie sociale pour tromper les utilisateurs et voler des informations sensibles. Le traitement manuel des emails suspects est une tâche chronophage et sujette aux erreurs humaines. Pour améliorer l'efficacité de la détection et de la réponse aux incidents, une **automatisation du processus** est nécessaire.

Objectif du Projet

L'objectif de ce projet est de **concevoir un workflow automatisé** permettant :

- L'identification des emails suspects à partir d'une boîte Gmail.
- L'analyse approfondie des emails grâce à un moteur d'intelligence artificielle (LLM) et à Cortex.
- La classification des emails en fonction de leur dangerosité.
- La notification des analystes SOC (Security Operations Center) via Discord.
- L'archivage et le suivi des incidents pour une gestion efficace.

Cette automatisation permet de **réduire le temps de réponse**, d'améliorer l'efficacité du traitement et de minimiser le risque d'erreurs.

2. Analyse des Besoins

Détection et Extraction des Emails Suspects

Le workflow doit récupérer automatiquement les emails signalés comme suspects. Cela peut inclure :

- Les emails marqués par les utilisateurs.
- Les emails contenant des liens ou des pièces jointes douteuses.
- Les messages provenant d'expéditeurs inconnus.

Analyse et Classification des Emails

Une analyse en plusieurs étapes est nécessaire pour évaluer le niveau de menace d'un email :

1. **Extraction des données** (expéditeur, objet, corps du message, liens, pièces jointes).
2. **Analyse des indicateurs de compromission (IOC)** avec Cortex.
3. **Évaluation du contenu textuel** avec un modèle LLM pour identifier les tentatives de social engineering.

Notification et Suivi

Une fois l'email classifié, il est important d'automatiser la **notification** aux analystes via Discord et d'archiver l'email pour un suivi ultérieur.

3. Conception du Workflow

Le workflow est conçu de manière modulaire avec plusieurs étapes interdépendantes.

1. Récupération des Emails avec Gmail API

- **Technologie :** Gmail API
- **Objectif :** Récupérer les emails suspects en fonction des critères définis.
- **Avantages :** Intégration directe avec Gmail, accès sécurisé aux emails.
- **Inconvénients :** Dépendance aux quotas d'API de Google, nécessité d'une authentification OAuth 2.0.

2. Prétraitement des Emails avec un Script Python

- **Technologie :** Python (Parsing & Extraction)
- **Objectif :** Extraire les éléments critiques des emails :
    - Expéditeur
    - Contenu textuel
    - URLs et pièces jointes
- **Avantages :** Flexibilité et possibilité d'extension avec d'autres modules de sécurité.
- **Inconvénients :** Risque d'erreurs si les emails sont mal formatés.

3. Analyse des Menaces avec un Modèle LLM et Cortex

a) Analyse du Contenu Textuel (LLM)

- **Technologie :** LangChain / Ollama Model
- **Objectif :** Détecter des indices de phishing en analysant la structure et le vocabulaire du message.
- **Avantages :** Détection avancée du social engineering.
- **Inconvénients :** Faux positifs possibles, consommation élevée de ressources.

b) Vérification des Indicateurs de Compromission (IOC) avec Cortex

- **Technologie :** Cortex Analyzer
- **Objectif :** Vérifier les URLs, adresses IP et fichiers joints en les comparant aux bases de données de Threat Intelligence.
- **Avantages :** Rapidité et intégration avec des bases de données d'attaques connues.
- **Inconvénients :** Dépendance aux services externes, risque de faux négatifs si l'IOC n'est pas encore référencé.

4. Classification des Risques

- **Technologie :** Condition If + Sommarisation
- **Objectif :** Prendre une décision sur la menace en fonction des résultats d'analyse.
- **Critères de classification :**
    - **Faible** ⟶ Aucun élément suspect détecté.
    - **Moyen** ⟶ Contenu suspect mais sans preuve tangible d'attaque.
    - **Élevé** ⟶ IOC confirmé, contenu trompeur détecté.

5. Notification sur Discord

- **Technologie :** Webhook Discord
- **Objectif :** Envoyer un message aux analystes SOC avec les détails de l'email suspect.
- **Avantages :** Réception immédiate des alertes et possibilité d'interaction rapide.
- **Inconvénients :** Ne remplace pas un système SIEM plus avancé.

6. Archivage et Marquage des Emails

- **Technologie :** Gmail API (Ajout de labels)
- **Objectif :** Classer les emails analysés pour suivi et audit.
- **Avantages :** Traçabilité des incidents sans stockage externe.
- **Inconvénients :** Nécessite une configuration des labels Gmail.

4. Mise en Œuvre

Implémentation Technique

- **Connexion à l'API Gmail** pour extraire les emails suspects.
- **Utilisation de Regex et de bibliothèques Python** (BeautifulSoup, PyPDF2) pour l'analyse du texte et des pièces jointes.
- **Intégration de Cortex** pour vérifier la présence d'IOC.
- **Déploiement d'un modèle LLM** pour analyser le contenu textuel des emails.
- **Définition des règles conditionnelles** pour classifier les menaces.
- **Configuration d'un webhook Discord** pour alerter les analystes en cas de phishing confirmé.
- **Ajout de labels Gmail** pour suivre l'évolution des emails traités.

Problèmes et Solutions

Problème	Solution
Faux positifs élevés	Ajustement des seuils de détection LLM et Cortex
Limites d'API Gmail	Mise en cache des requêtes pour réduire l'utilisation excessive
Temps de réponse du modèle LLM	Optimisation du pipeline d'analyse pour accélérer l'exécution

5. Résultats et Fonctionnement

Tests et Validation

Plusieurs scénarios de test ont été effectués :

1. **Email légitime** ⟶ Pas d'alerte générée, l'email est archivé.
2. **Email avec lien suspect** ⟶ Analyse approfondie par Cortex, alerte Discord si nécessaire.
3. **Email avec pièce jointe malveillante** ⟶ Vérification avec une sandbox, classification du niveau de risque.

Améliorations possibles

- Ajout d'une **sandbox pour l'analyse des pièces jointes**.
- Intégration avec un **SIEM** pour une gestion avancée des incidents.
- Mise en place d'un **modèle d'apprentissage supervisé** pour affiner la classification des emails.

6. Conclusion et Perspectives

Ce projet a permis de **mettre en place un système automatisé de réponse aux incidents de phishing**, améliorant la rapidité et la précision de la détection. En intégrant plusieurs technologies complémentaires (Gmail API, LLM, Cortex, Discord), ce workflow optimise le traitement des menaces tout en réduisant la charge de travail des analystes.

Perspectives :

- Amélioration des algorithmes de détection avec du **Machine Learning**.
- Intégration à une **solution SOAR** pour automatiser encore plus la réponse aux incidents.
- **Extension à d'autres types de cybermenaces** (malwares, fraudes, etc.).

7. PARTIE 2 : implémentation d'une solution professionnelle avec TheHive, Cortex et n8n

7.1 Introduction à l'écosystème professionnel de réponse aux incidents

Suite à notre première implémentation qui a démontré la faisabilité d'un workflow automatisé pour la détection et la réponse aux incidents de phishing, nous avons souhaité explorer une approche plus robuste et industrielle. Cette seconde phase vise à intégrer des outils reconnus dans l'industrie de la cybersécurité pour construire une plateforme complète et évolutive.

Nous nous sommes tournés vers trois technologies complémentaires qui constituent l'épine dorsale des SOC (Security Operations Centers) modernes :

- **TheHive** - Plateforme de réponse aux incidents conçue spécifiquement pour les équipes de sécurité, offrant des capacités avancées de gestion de cas, de collaboration et de suivi des incidents.
- **Cortex** - Moteur puissant d'orchestration et d'analyse qui permet l'automatisation des recherches d'indicateurs de compromission (IOC) via de nombreuses sources externes.
- **n8n** - Plateforme open-source d'automatisation des flux de travail qui se présente comme une alternative performante à Zapier ou Microsoft Power Automate, et que nous avons installé localement avec la version community.

7.2 Objectifs et portée de cette phase avancée

Cette seconde itération poursuit plusieurs objectifs stratégiques :

1. **Acquérir une expertise technique** sur des outils de référence utilisés par les professionnels de la cybersécurité
2. **Comprendre les exigences infrastructurelles** nécessaires au déploiement de solutions robustes
3. **Explorer l'interopérabilité** entre ces différentes technologies
4. **Développer des compétences valorisables** pour notre parcours professionnel

Le marché de l'emploi en cybersécurité valorise particulièrement la maîtrise de ces outils, comme en témoigne leur présence récurrente dans les offres d'emploi pour les postes d'analystes SOC, d'ingénieurs en sécurité, ou de responsables de la réponse aux incidents.

Notre démarche ne vise pas l'exhaustivité — les contraintes temporelles du projet ne nous permettent pas d'explorer toutes les fonctionnalités offertes par cet écosystème — mais plutôt une familiarisation pratique avec ces technologies et leurs possibilités d'intégration.

7.3 Architecture et composants de la solution

L'architecture que nous allons mettre en place repose sur l'intégration de ces trois composants principaux :

- **TheHive** constitue le cœur opérationnel du système, servant de plateforme centralisée pour :
    - La gestion structurée des incidents
    - La documentation des cas
    - La collaboration entre analystes
    - Le suivi des actions entreprises

- **Cortex** joue le rôle de moteur d'analyse avec :
    - Des analyseurs pour évaluer différents types d'indicateurs
    - Des connecteurs vers les bases de threat intelligence externes
    - Des capacités d'enrichissement des données collectées
- **n8n** orchestre les flux de travail en :
    - Automatisant le transfert d'informations entre systèmes
    - Gérant les déclencheurs et les réponses conditionnelles
    - Offrant une interface visuelle pour concevoir les processus

Cette approche modulaire nous permettra d'établir une base solide qui pourrait ultérieurement être étendue avec d'autres composants comme MISP (pour le partage d'indicateurs de menaces) ou des solutions SIEM plus avancées.

Dans les sections suivantes, nous détaillerons l'installation, la configuration et l'intégration de ces différentes briques technologiques, ainsi que leur adaptation à notre scénario de réponse aux incidents de phishing.

7.4 Problématiques et défis opérationnels rencontrés

L'implémentation d'une solution professionnelle de réponse aux incidents présente des défis techniques. Notre expérience a mis en lumière plusieurs obstacles significatifs qui méritent d'être documentés pour les déploiements futurs.

7.4.1 Complexité de l'installation et dépendances système

La phase d'installation s'est avérée laborieuse en raison de :

- **Incompatibilités entre versions** : Les différentes versions d'OS mentionnées dans la documentation officielle n'étaient pas toujours pleinement compatibles avec TheHive, nécessitant des ajustements constants et des recherches complémentaires.

7.4.2 Exigences matérielles substantielles

Les besoins en ressources système se sont révélés considérables :

- **Mémoire vive** : Un minimum de 16 Go de RAM par machine est nécessaire pour un fonctionnement fluide, particulièrement pour les environnements exécutant Elasticsearch et Cassandra simultanément.
- **Capacité de stockage** : Les bases de données utilisées par TheHive et Cortex nécessitent un espace de stockage important, surtout en considérant la croissance des données au fil du temps.
- **Ressources CPU** : L'analyse en temps réel des artefacts par Cortex demande une puissance de calcul significative, particulièrement lors de l'utilisation de multiples analyseurs en parallèle.

7.4.3 Courbe d'apprentissage et documentation lacunaire

L'adoption de ces outils est freinée par plusieurs facteurs liés à la documentation et à l'apprentissage :

- **Documentation fragmentée** : Si les guides d'installation sont généralement bien détaillés, la documentation concernant l'utilisation avancée, l'intégration entre composants et la résolution de problèmes est souvent dispersée ou incomplète.
- **Exemples limités** : Les cas d'usage complexes et les configurations avancées manquent d'exemples concrets, obligeant à procéder par tâtonnements.

Ces problématiques soulignent l'importance d'allouer des ressources adéquates (temps, infrastructure, expertise) lors de la planification d'un déploiement à l'échelle d'entreprise.

Elles expliquent également pourquoi ces compétences sont particulièrement valorisées sur le marché du travail en cybersécurité.

7.5 Workflow spécifique pour le phishing

Pour cette partie nous nous inspirons entre autres du document processus issus du CERT de la société générale, ainsi que des conseils du NIST en matière de réponse à incident, et avec un scénario de phishing.

Mais ce workflow détaillé ci-bas est si complet qu'il peut être utilisé sur tous types d'incident (à quelques modifications près évidemment liées aux types d'incident en question). Ceci nous servira donc de référence pour nos prochains travaux personnels et professionnels.

7.5.1 Workflow très avancé théorique pour réponse à incident : liste

https://github.com/cert-advens/IRM/blob/main/FR/IRM-16-Phishing.pdf

En pratique l'ordre indiqué ne fonctionne pas tel que cela, et en réalité nous avons beaucoup simplifié ce workflow lors de la réalisation, dû aux contraintes exprimées plus haut (temps et objectifs d'utilisation de ces outils avancés).

Toutefois avec plus de temps c'est ce workflow que nous souhaitons mettre en place via ces outils d'automatisation (et incluant des modifications issus de notre compréhension pratique).

PHASE DE DÉTECTION INITIALE

A. Réception du signalement

- Création automatique d'un ticket dans TheHive
- Collecte des informations du rapporteur :
  - Informations de contact complètes
  - Rôle et département
  - Localisation
  - Horodatage de la détection
- Application d'un template de collecte standardisé pour l'email suspect :
  - En-têtes complets
  - Corps du message
  - Pièces jointes
  - URLs identifiées

B. Qualification de l'incident

(Cette étape est cruciale selon le NIST)

- Vérification des critères d'incident **(via N8N ou via cortex, ou les deux)**:
  - L'email correspond-il aux patterns de phishing connus ?
  - Viole-t-il les politiques de sécurité de l'organisation ?
  - Est-ce une campagne ciblée ou générique ?
  - Quel est le niveau de sophistication ?
- Analyse préliminaire automatisée **(via Cortex)** :
  - Scan des URLs et pièces jointes
  - Vérification des domaines émetteurs
  - Recherche d'indicateurs de compromission
  - Consultation des bases de phishing connus
- Décision de qualification :
  - Si qualifié comme incident ⟶ poursuite du processus
  - Si non qualifié ⟶ documentation et clôture **(dans thehive)**

PHASE D'ANALYSE ET PRIORISATION

A. Évaluation de l'impact

- Impact fonctionnel :
  - Systèmes potentiellement touchés
  - Services critiques menacés
  - Nombre d'utilisateurs concernés
- Impact informationnel :
  - Type de données visées
  - Sensibilité des informations
  - Obligations réglementaires associées
- Effort de récupération :
  - Ressources nécessaires
  - Temps estimé
  - Complexité technique

B. Détermination du niveau de criticité

- Score basé sur :

- Urgence (nécessité d'action immédiate)
- Impact (gravité des conséquences)
- Propagation (potentiel d'extension)

PHASE DE RÉPONSE INITIALE

A. Si l'utilisateur n'a PAS cliqué :

- Actions automatisées :
  - Extraction des IOCs
  - Enrichissement via MISP
  - Mise à jour des filtres de sécurité
  - Recherche d'emails similaires
  - Blocage préventif des sources
  - Documentation technique complète

B. Si l'utilisateur A cliqué :

- Actions immédiates automatisées :
  - Isolation réseau du poste (via EDR)
  - Désactivation du compte (via API Active Directory)
  - Révocation des sessions actives
  - Collecte des logs système et réseau
  - Capture mémoire si nécessaire

PHASE D'INVESTIGATION APPROFONDIE (si clic confirmé)

A. Analyse technique

- Investigation forensique :
  - Analyse chronologique complète
  - Recherche d'artefacts malveillants
  - Identification des actions effectuées
  - Recherche de persistance

B. Analyse de propagation

- Cartographie de l'exposition :
  - Recherche d'activités suspectes sur le réseau

- Vérification des systèmes connectés
- Analyse des accès aux ressources sensibles
- Identification d'autres victimes potentielles

PHASE DE CONFINEMENT ET REMÉDIATION

A. Actions de confinement

- Mise en place des blocages :
  - Blocage des IOCs au niveau réseau
  - Blocage des domaines malveillants
  - Mise à jour des règles de filtrage email
  - Déploiement des signatures de détection

B. Actions de remédiation

- Nettoyage des systèmes :
  - Suppression des composants malveillants
  - Réinitialisation des accès compromis
  - Restauration des systèmes affectés
  - Vérification de l'intégrité

PHASE DE RETOUR À LA NORMALE

A. Validation

- Tests de fonctionnement :
  - Vérification des systèmes restaurés
  - Confirmation des accès légitimes
  - Validation des communications
  - Tests de sécurité

B. Surveillance renforcée

- Mise en place de contrôles spécifiques :
  - Surveillance accrue des systèmes affectés
  - Monitoring des indicateurs identifiés
  - Alertes sur comportements similaires

PHASE POST-INCIDENT

A. Documentation

- Rapport complet incluant :
  - Chronologie détaillée
  - Actions effectuées
  - Preuves collectées
  - Indicateurs techniques
  - Impact final évalué
  - Coûts engagés

B. Retour d'expérience

- Organisation d'une réunion formelle
- Analyse des points d'amélioration :
  - Processus de détection
  - Procédures de réponse
  - Outils utilisés
  - Formation des utilisateurs

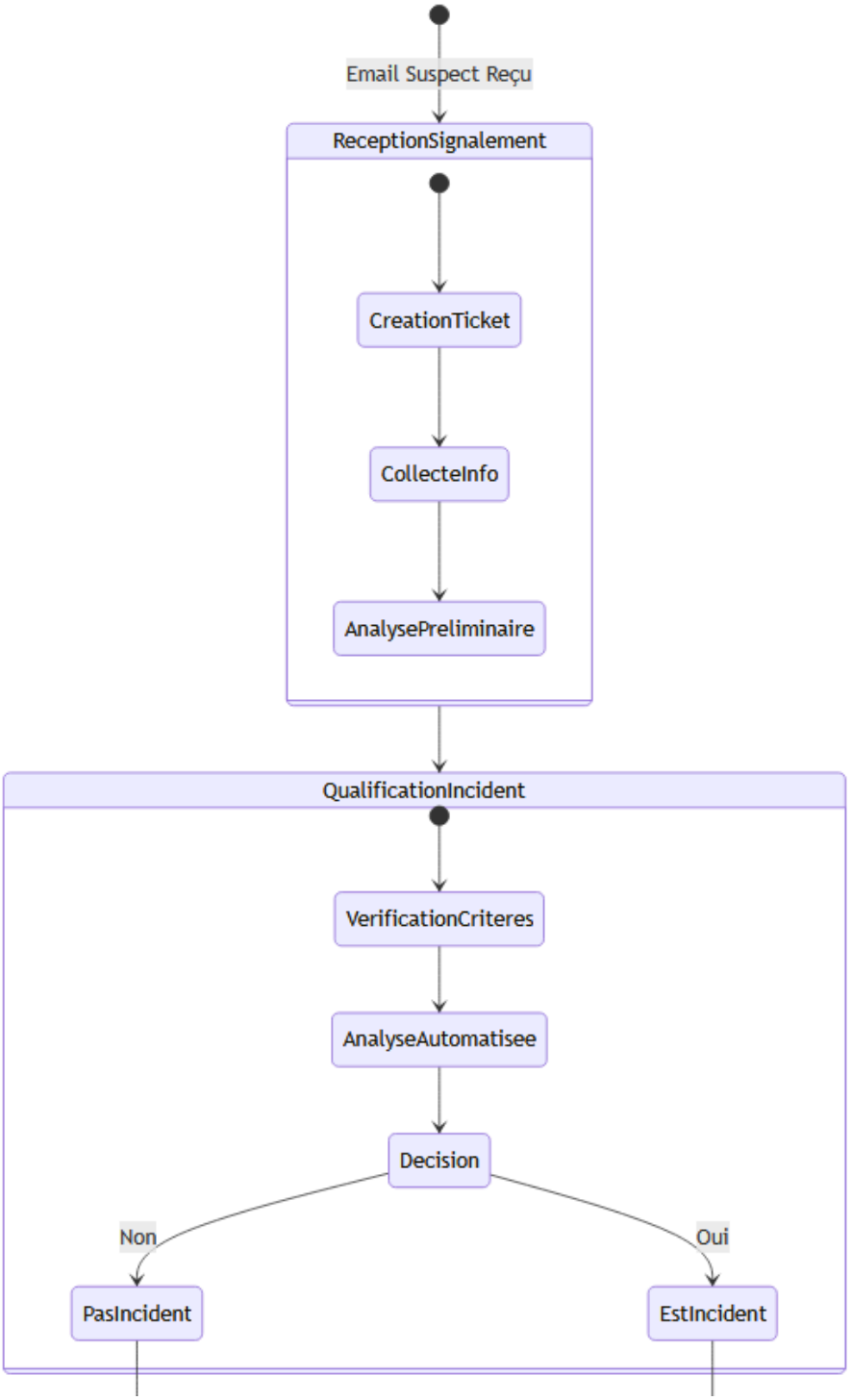
C. Actions d'amélioration

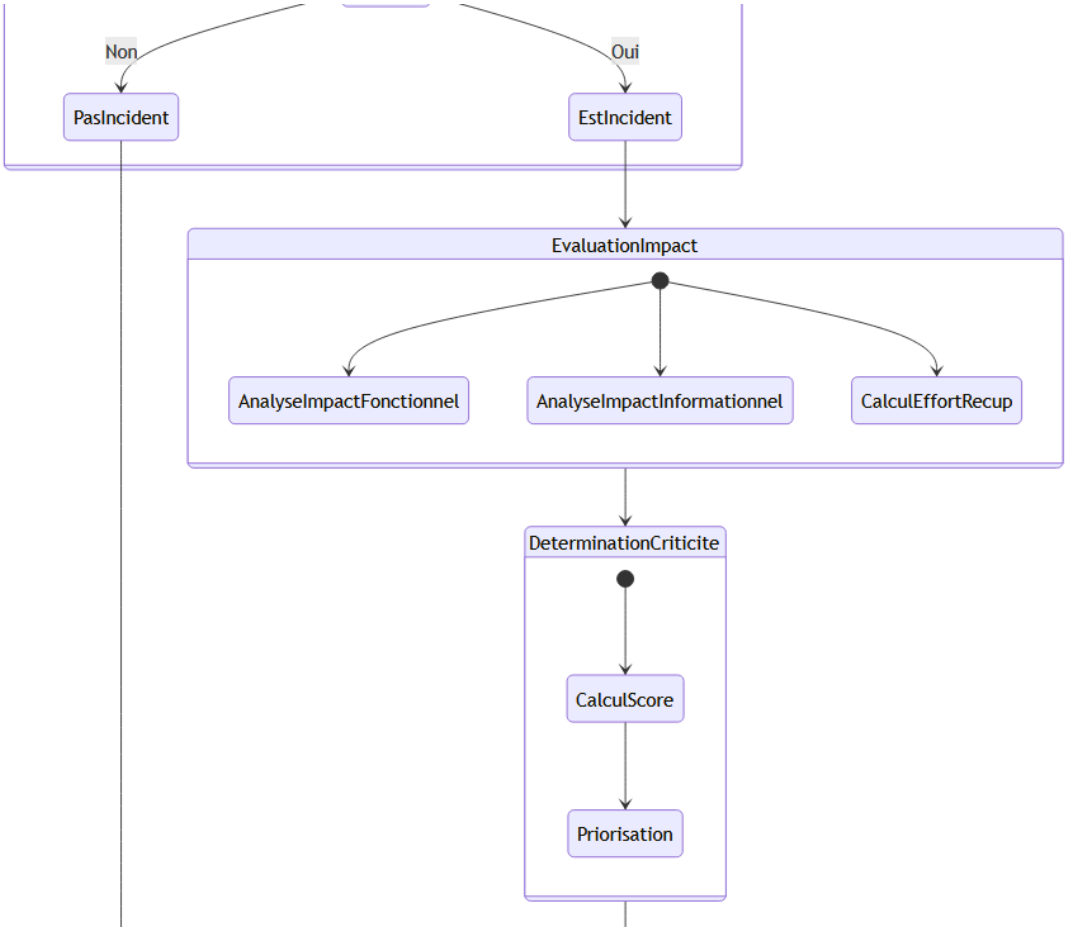
- Mise à jour des procédures
- Renforcement des contrôles
- Adaptation des formations
- Évolution des outils

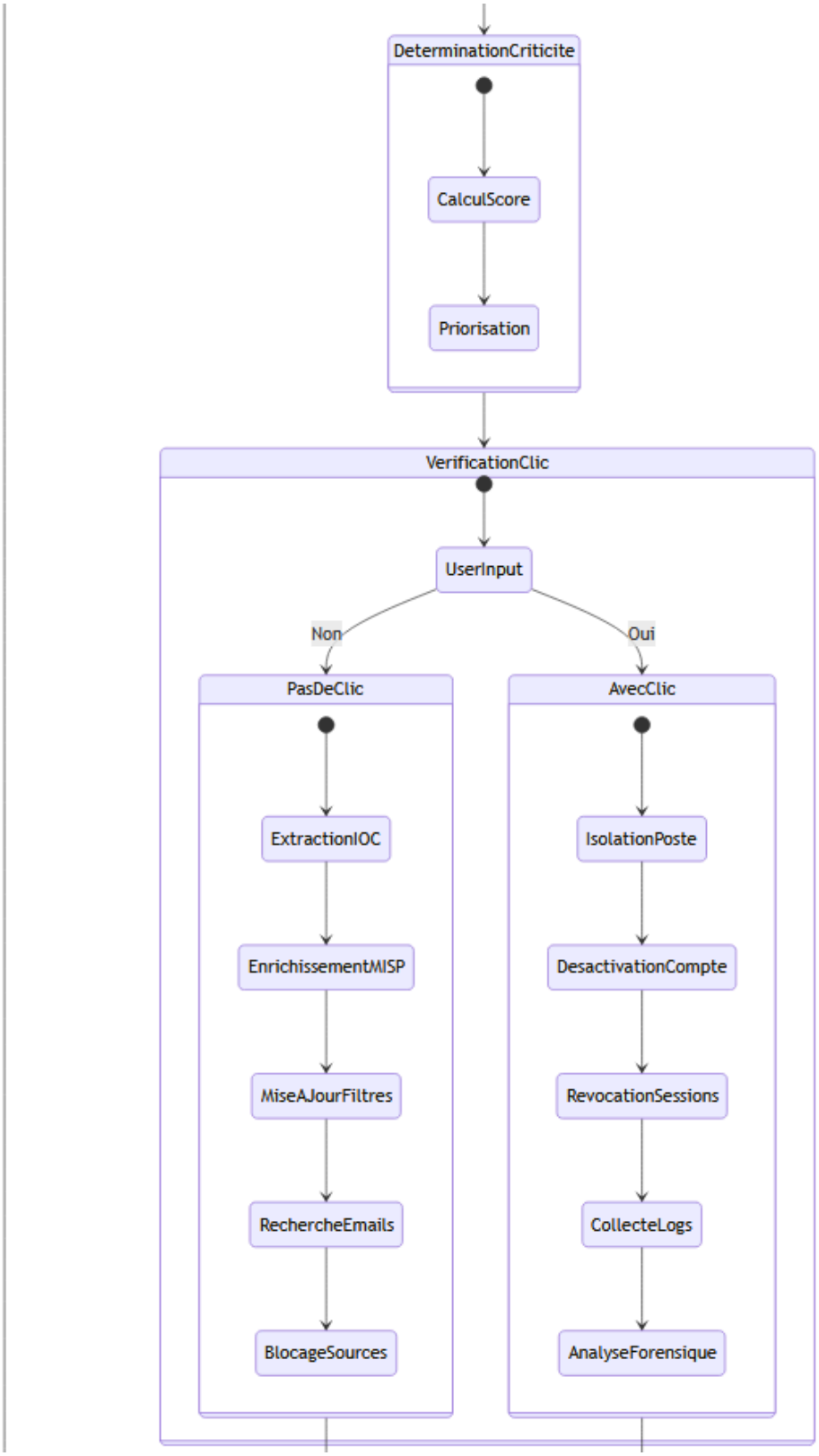
*7.5.2 Workflow très avancé **théorique** pour réponse à incident : schéma*

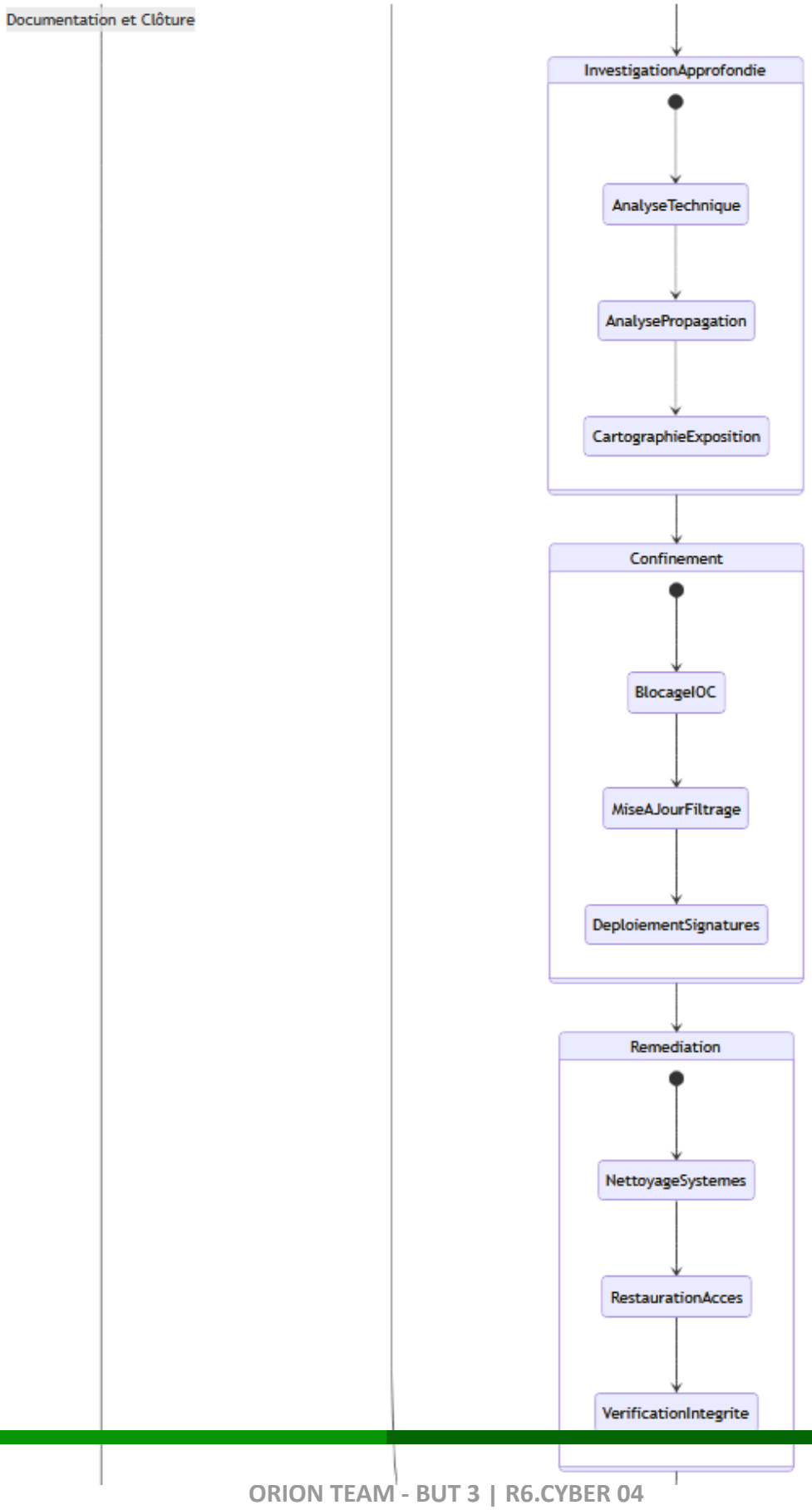
→ Pour voir le schéma au complet en ligne cliquez ici : Voir le schéma.

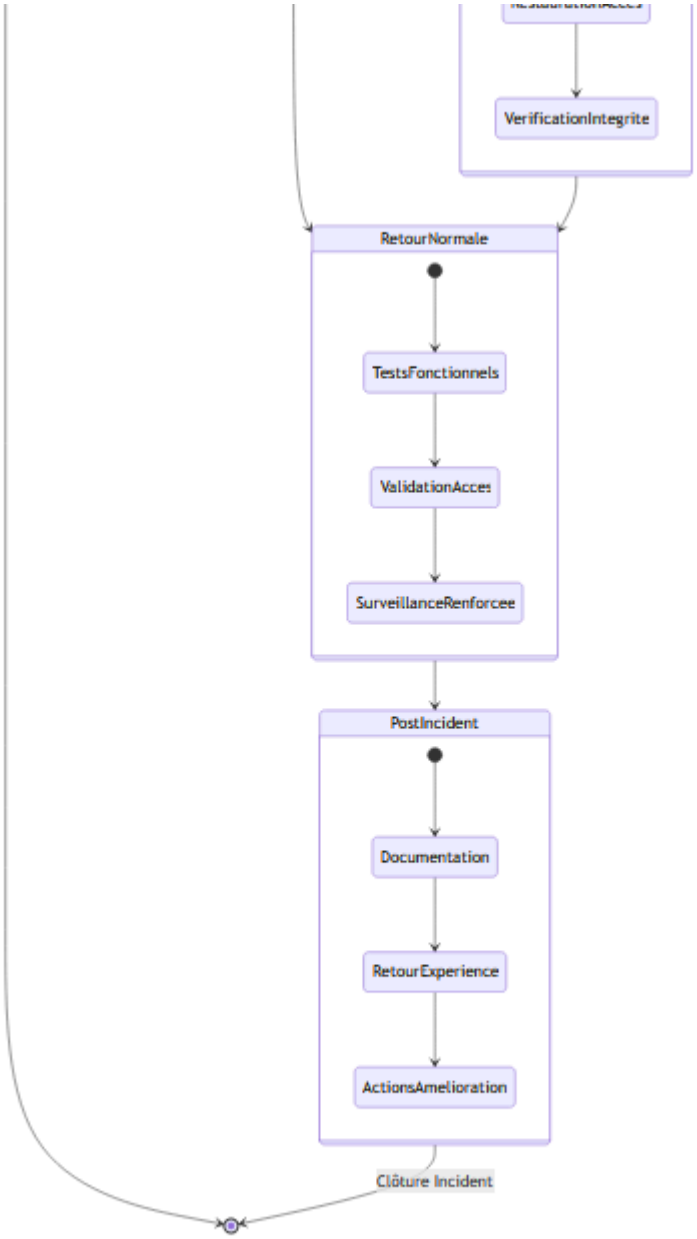
Nous avons tenté de recoller les différentes pièces du schéma, mais comme il est un long, il est plus facile d'aller voir sur le lien donné ci haut (ceci n'est pas un phishing).


Email Suspect Reçu
ReceptionSignalement
CreationTicket
CollecteInfo
AnalysePreliminaire
QualificationIncident
VerificationCriteres
AnalyseAutomatisee
Decision
Non
Oui
PasIncident
EstIncident


Non
Oui
PasIncident
EstIncident
EvaluationImpact
AnalyseImpactFonctionnel
AnalyseImpactInformationnel
CalculEffortRecup
DeterminationCriticite
CalculScore
Priorisation


DeterminationCriticite
CalculScore
Priorisation
VerificationClic
UserInput
Non
Oui
PasDeClic
AvecClic
ExtractionIOC
EnrichissementMISP
MiseAJourFiltres
RechercheEmails
BlocageSources
IsolationPoste
DesactivationCompte
RevocationSessions
CollecteLogs
AnalyseForensique


Documentation et Clôture
InvestigationApprofondie
AnalyseTechnique
AnalysePropagation
CartographieExposition
Confinement
BlocageIOC
MiseAJourFiltrage
DeploiementSignatures
Remediation
NettoyageSystemes
RestaurationAcces
VerificationIntegrite


VerificationIntegrite
RetourNormale
TestsFonctionnels
ValidationAcces
SurveillanceRenforcee
PostIncident
Documentation
RetourExperience
ActionsAmelioration
Clôture Incident

7.5.3 Workflow de découverte pour l'évaluation des fonctionnalités principales

Notre approche de découverte vise à évaluer rapidement les capacités fondamentales de TheHive et Cortex, en établissant un workflow simplifié mais fonctionnel.

Bien que ces plateformes disposent de nombreuses intégrations natives, nous avons opté pour l'utilisation de n8n comme orchestrateur intermédiaire afin d'accélérer cette phase d'apprentissage et contourner certaines limitations d'intégration rencontrées.

7.5.3.1 Architecture simplifiée pour l'évaluation des outils

Voici un workflow opérationnel que nous avons conçu pour tester efficacement ces technologies, en reprenant le scénario de détection de phishing présenté dans la première partie de notre rapport :

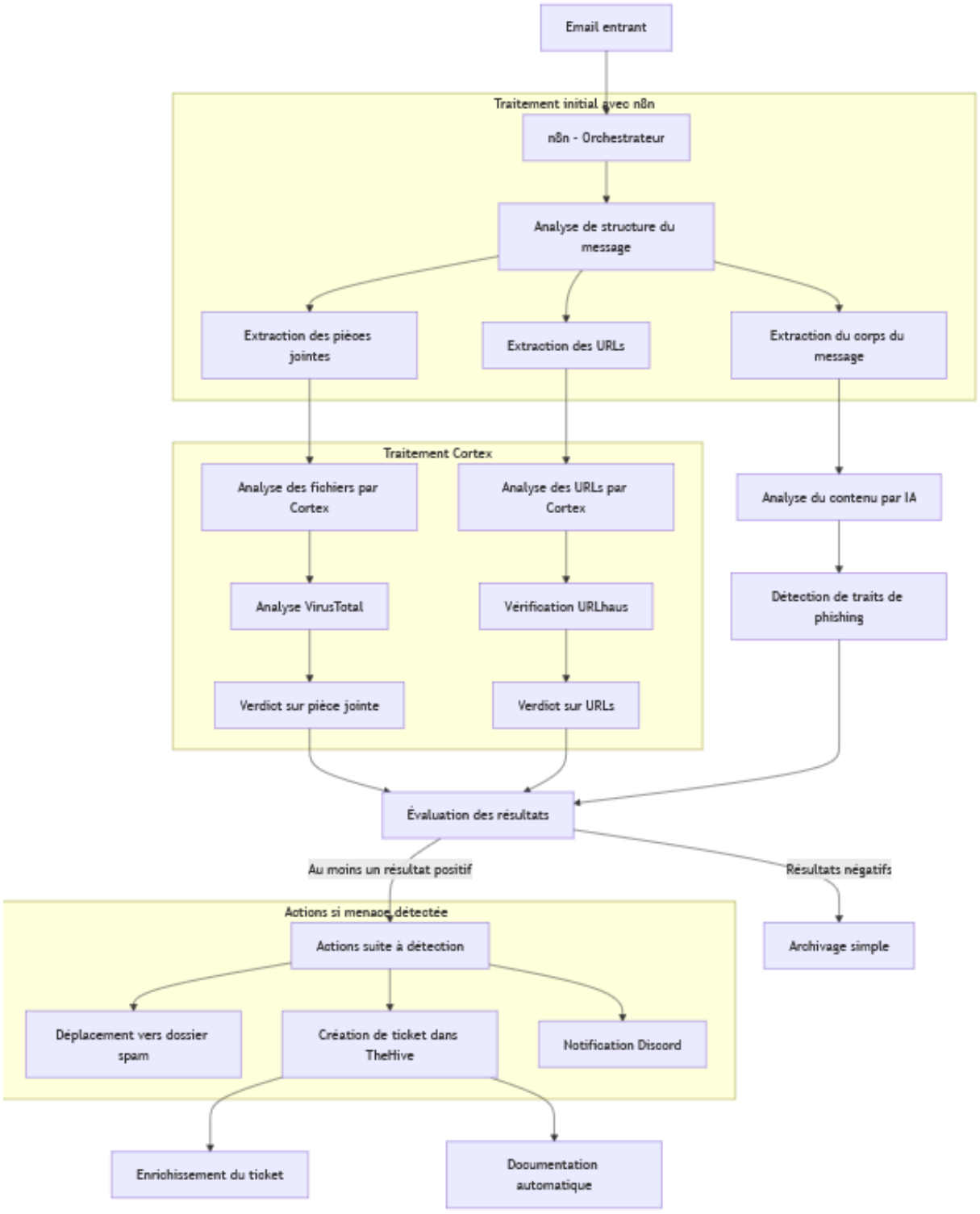
7.5.3.2 Processus détaillé de traitement : liste

1. **Réception et prétraitement via n8n**
    - Interception des emails entrants via webhooks/connecteurs IMAP/connecteur gmail natif
    - Décomposition structurelle du message (corps, pièces jointes, URLs)
    - Acheminement des différents éléments vers les moteurs d'analyse appropriés
2. **Analyse des composants suspects par Cortex**
    - Soumission des pièces jointes à l'analyseur VirusTotal pour détection de malware **(implémentation d'un connecteur virustotal dans cortex)**
    - Vérification des URLs extraites via les connecteurs URLhaus et PhishTank **(non réalisé)**
    - Génération de scores de menace et extraction d'indicateurs de compromission
    - Transmission des verdicts à n8n pour centralisation des résultats

3. **Évaluation du contenu textuel par intelligence artificielle**
    - Analyse du corps du message pour détecter des caractéristiques de phishing
    - Identification des techniques de manipulation psychologique
    - Production d'un rapport de raisonnement détaillé
    - Transmission d'une conclusion binaire (phishing/légitime) pour prise de décision
4. **Orchestration des réponses basée sur les résultats**
    - **Scénario négatif**: Si tous les verdicts sont négatifs, aucune action n’est prise, le courriel va dans la boîte principale gmail.
    - **Scénario positif**: Si au moins un verdict est positif, déclenchement d'actions défensives:
        - Déplacement automatique du message vers le dossier spam
        - Création d'un cas documenté dans TheHive avec les IOCs extraits
        - Notification en temps réel via Discord, incluant le résumé de l'analyse et le raisonnement de l'IA

7.5.3.3 Processus détaillé de traitement : schéma

→ voir le schéma simplifié en ligne (ceci n'est pas un phishing)



7.5.3.4 Objectifs pédagogiques de cette implémentation

Cette configuration nous permet d'explorer plusieurs aspects essentiels:

- La capacité de TheHive à centraliser les informations d'incidents
- Les fonctionnalités d'analyse de Cortex via ses différents connecteurs
- L'orchestration de flux de travail automatisés entre plusieurs systèmes
- L'enrichissement progressif des tickets d'incident

Bien que simplifiée par rapport au workflow complet décrit précédemment, cette implémentation constitue une base solide pour notre familiarisation avec ces outils professionnels et permet d'en évaluer rapidement la pertinence pour nos besoins futurs.

7.6 Installation et configuration des outils

7.6.1 Installation thehive

- debian 11
- 16g de RAM, 4 processeurs
- gourmand en ressource (elasticsearch, cassandra and thehive)
- ssh jkb@jkb-vm.pantheon.lab.mpgn.dev
- passphrase [redacted]
- mdp sudo : [redacted]

7.6.1.1 script d'installation automatique

```
sudo apt update && sudo apt upgrade -y

wget -q -O /tmp/install.sh
https://archives.strangebee.com/scripts/install.sh ; sudo -v ;
bash /tmp/install.sh
```

7.6.1.2 Configurer les permissions

```
sudo chown -R thehive:thehive /etc/thehive
```

7.6.1.3 Démarrage et vérification

```
sudo systemctl start thehive

sudo systemctl enable thehive

sudo systemctl status thehive
```

Vérifier aussi le statut ses dépendances essentielles

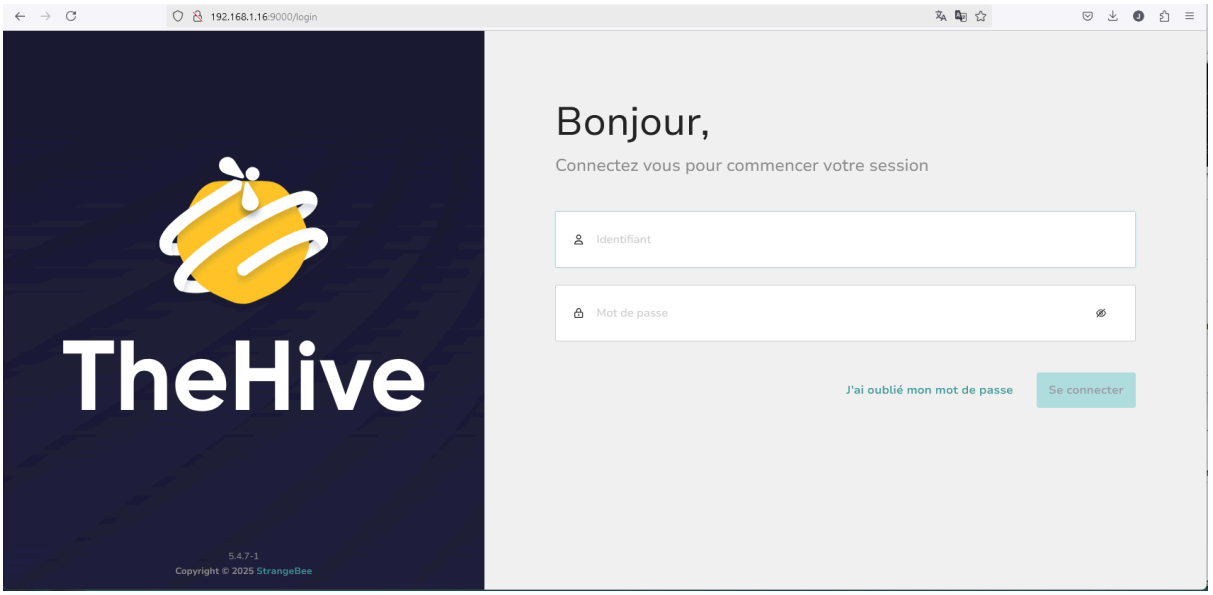
```
thehive@thehive:~$ sudo systemctl status thehive
● thehive.service - Scalable, Open Source and Free Security Incident Response Solutions
     Loaded: loaded (/lib/systemd/system/thehive.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-02-05 05:04:13 UTC; 2h 19min ago
       Docs: https://thehive-project.org
   Main PID: 20995 (java)
      Tasks: 163 (limit: 11803)
     Memory: 1.3G
        CPU: 2h 6min 14.746s
     CGroup: /system.slice/thehive.service
             └─20995 java -Dfile.encoding=UTF-8 -Dconfig.file=/etc/thehive/application.conf -Dlogge
```

```
thehive@thehive:~$ sudo systemctl status cassandra
● cassandra.service - LSB: distributed storage system for structured data
     Loaded: loaded (/etc/init.d/cassandra; generated)
     Active: active (running) since Wed 2025-02-05 05:00:09 UTC; 2h 23min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 111 (limit: 11803)
     Memory: 2.8G
        CPU: 45min 33.456s
     CGroup: /system.slice/cassandra.service
             └─20374 /usr/bin/java -ea -da:net.openhft... -XX:+UseThreadPriorities -XX:+HeapDumpOnO
```

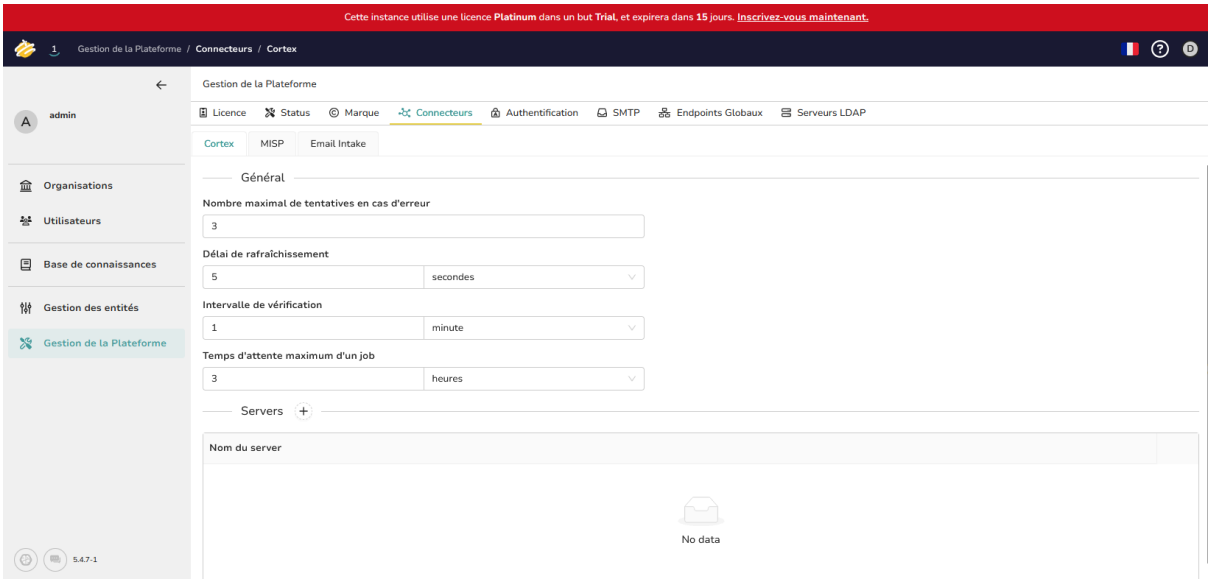
```
thehive@thehive:~$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-02-05 05:03:50 UTC; 2h 20min ago
       Docs: https://www.elastic.co
   Main PID: 20640 (java)
      Tasks: 109 (limit: 11803)
     Memory: 4.4G
        CPU: 31min 41.121s
     CGroup: /system.slice/elasticsearch.service
             ├─20640 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.t
             └─20838 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
```

7.6.1.4 Lancement de l'interface web

```
http://IP_ADDRESS:9000
```



L'utilisateur par défaut est "admin@thehive.local" et le mot de passe est "**secret**".



7.6.2 Installation cortex

→ Utilisez le même script installation automatique que précédemment mais choisir installation de cortex

- debian 11
- 16g de RAM, 4 processeurs

- gourmand en ressource (elasticsearch, cassandra)
- ssh jkb@jkb2-vm.pantheon.lab.mpgn.dev
- passphrase [redacted]
- mdp sudo : [redacted]

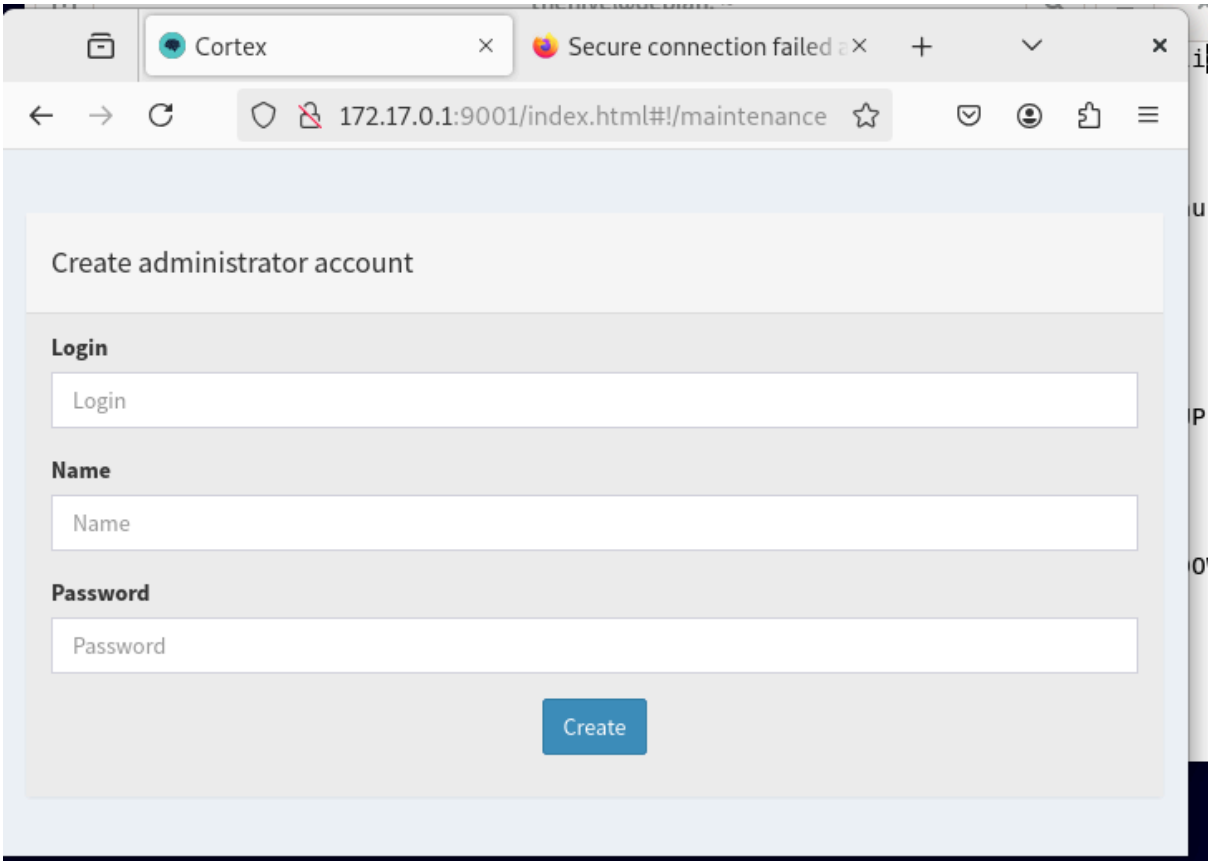
7.6.2.1 Démarrage et vérification

```
sudo systemctl start cortex.service

sudo systemctl enable cortex.service

sudo systemctl status cortex.service
```

```
thehive@debian:~$ sudo systemctl status cortex.service
● cortex.service - cortex
     Loaded: loaded (/etc/systemd/system/cortex.service; enabled; vendo
     Active: active (running) since Wed 2025-02-19 13:12:37 CET; 1min 1
       Docs: https://thehive-project.org
   Main PID: 14679 (java)
      Tasks: 46 (limit: 12272)
     Memory: 490.3M
        CPU: 15.652s
     CGroup: /system.slice/cortex.service
             └─14679 java -Duser.dir=/opt/cortex -Dconfig.file=/etc/cor
```

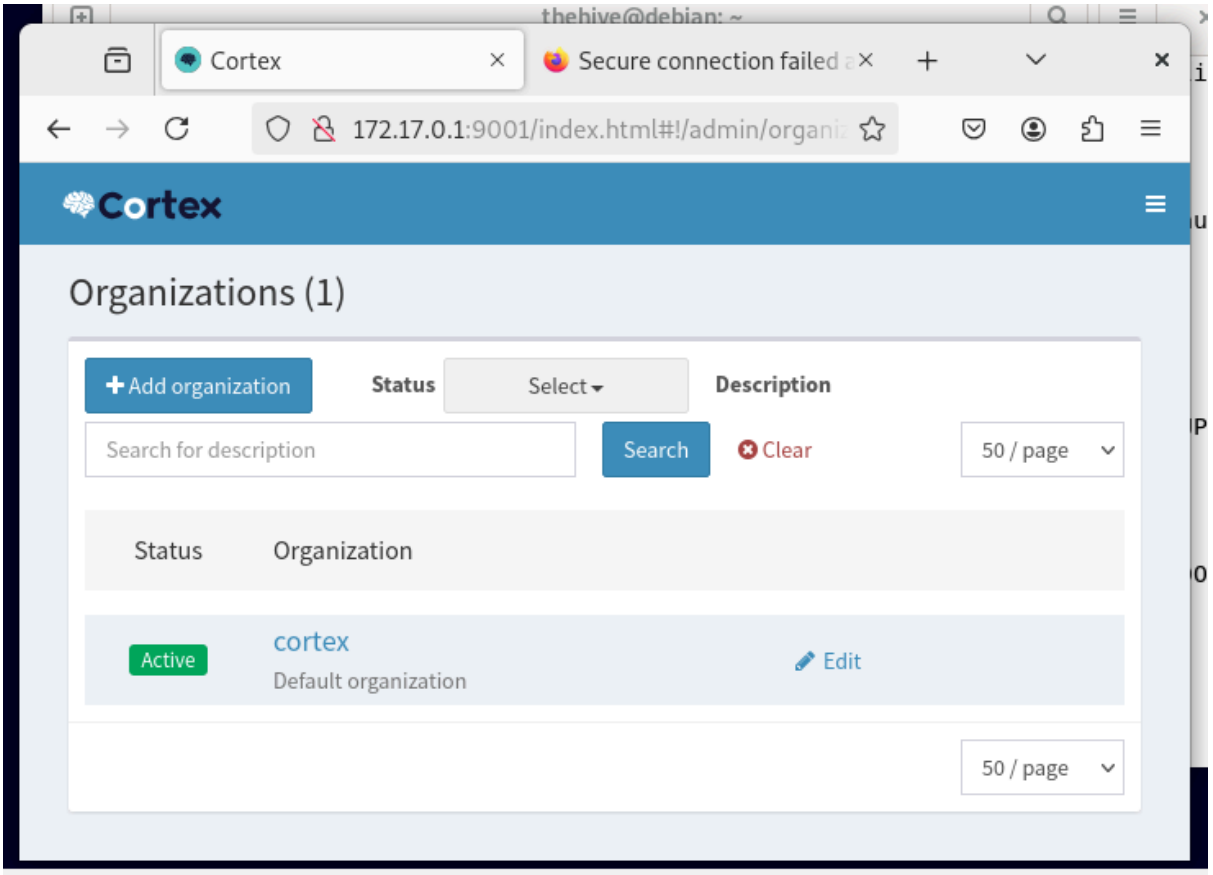
7.6.2.2 Lancement de l'interface web

```
http://IP_ADDRESS:9001
```



Créer un premier utilisateur admin

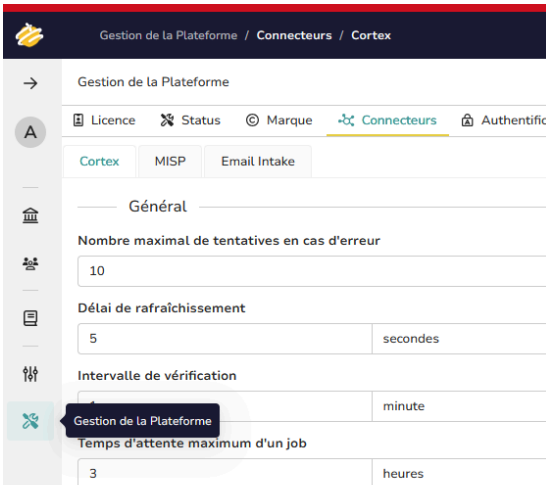
- user : admin
- name: jacob
- pwd: [redacted]



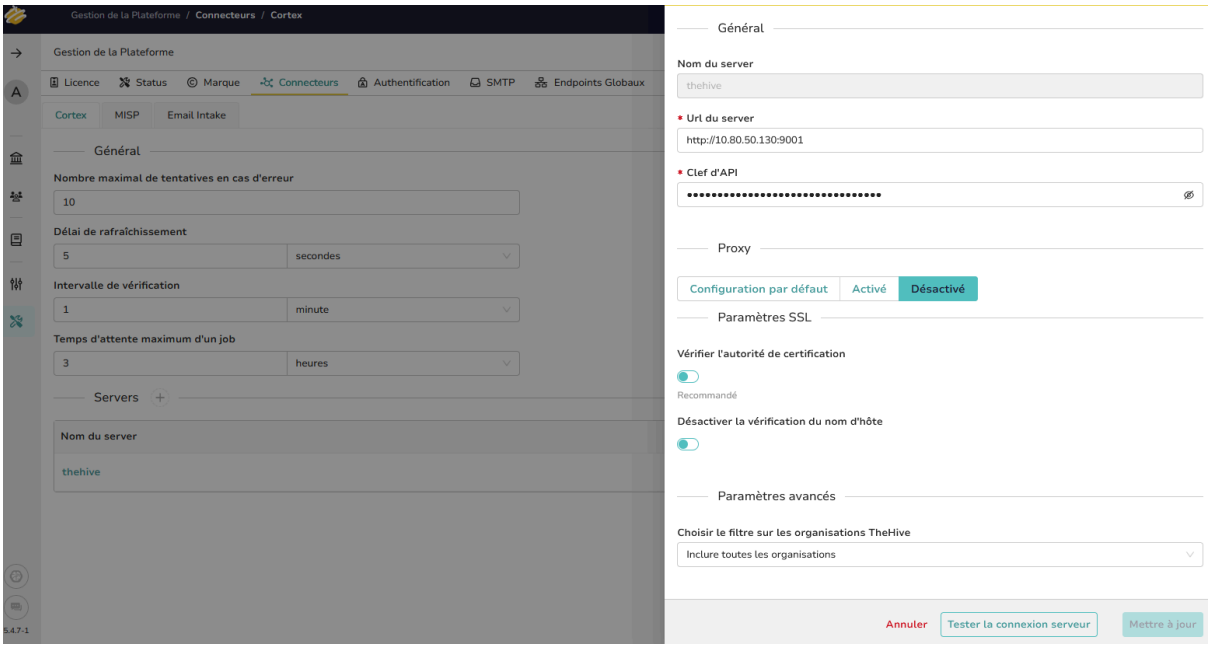
7.6.3 Interconnexion cortex et thehive

7.6.3.1 Ajouter un serveur cortex

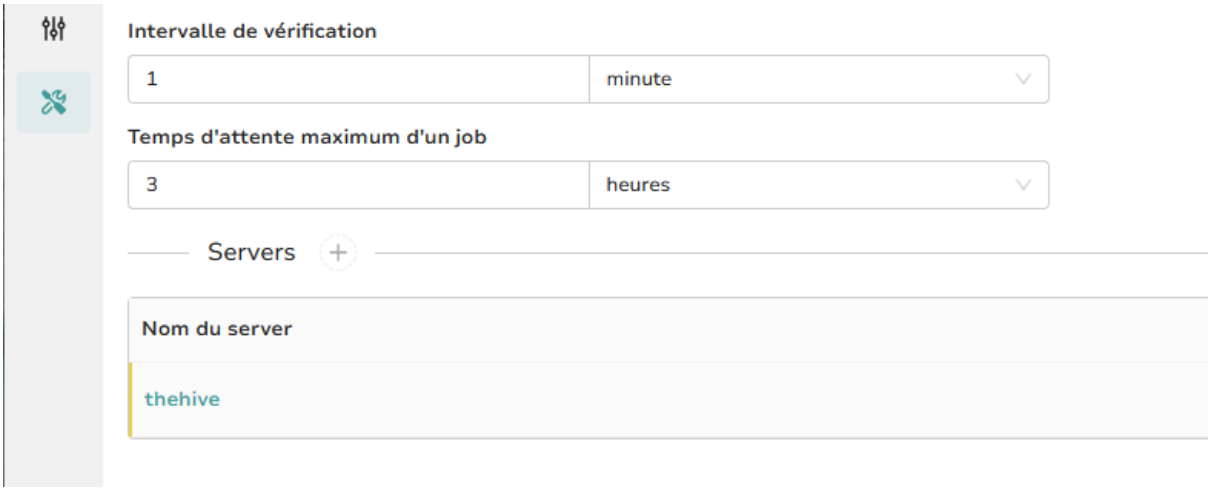
Dans le compte admin rendez vous dans le menu à gauche gestion de la plateforme



Cliquez sur ajouter un serveur et remplissez les informations clé API et URL du serveur cortex.



Le serveur si correctement connecté apparaîtra en bas à gauche de la fenêtre.



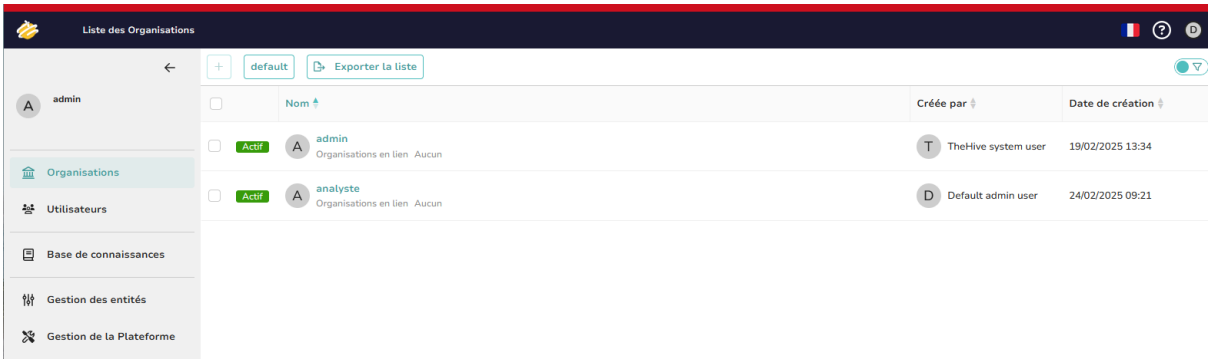
7.6.4 Déblocage des fonctionnalités thehive "create case"

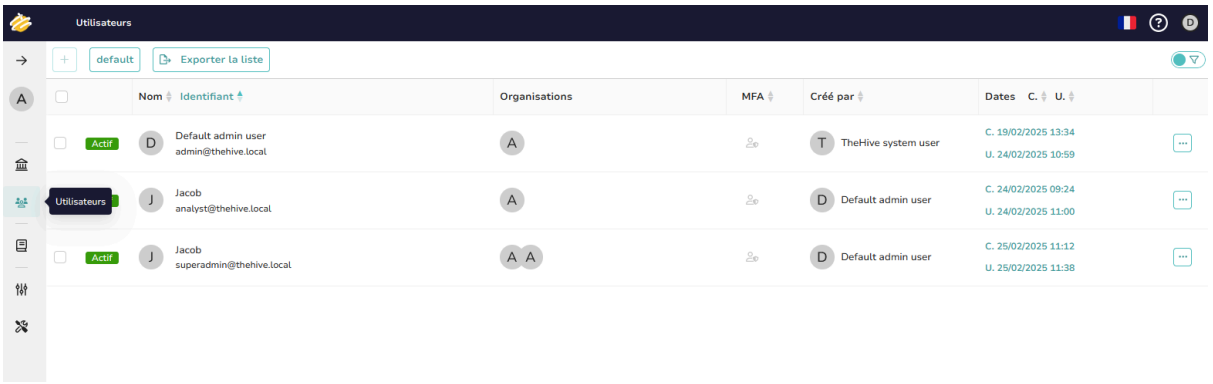
ATTENTION !

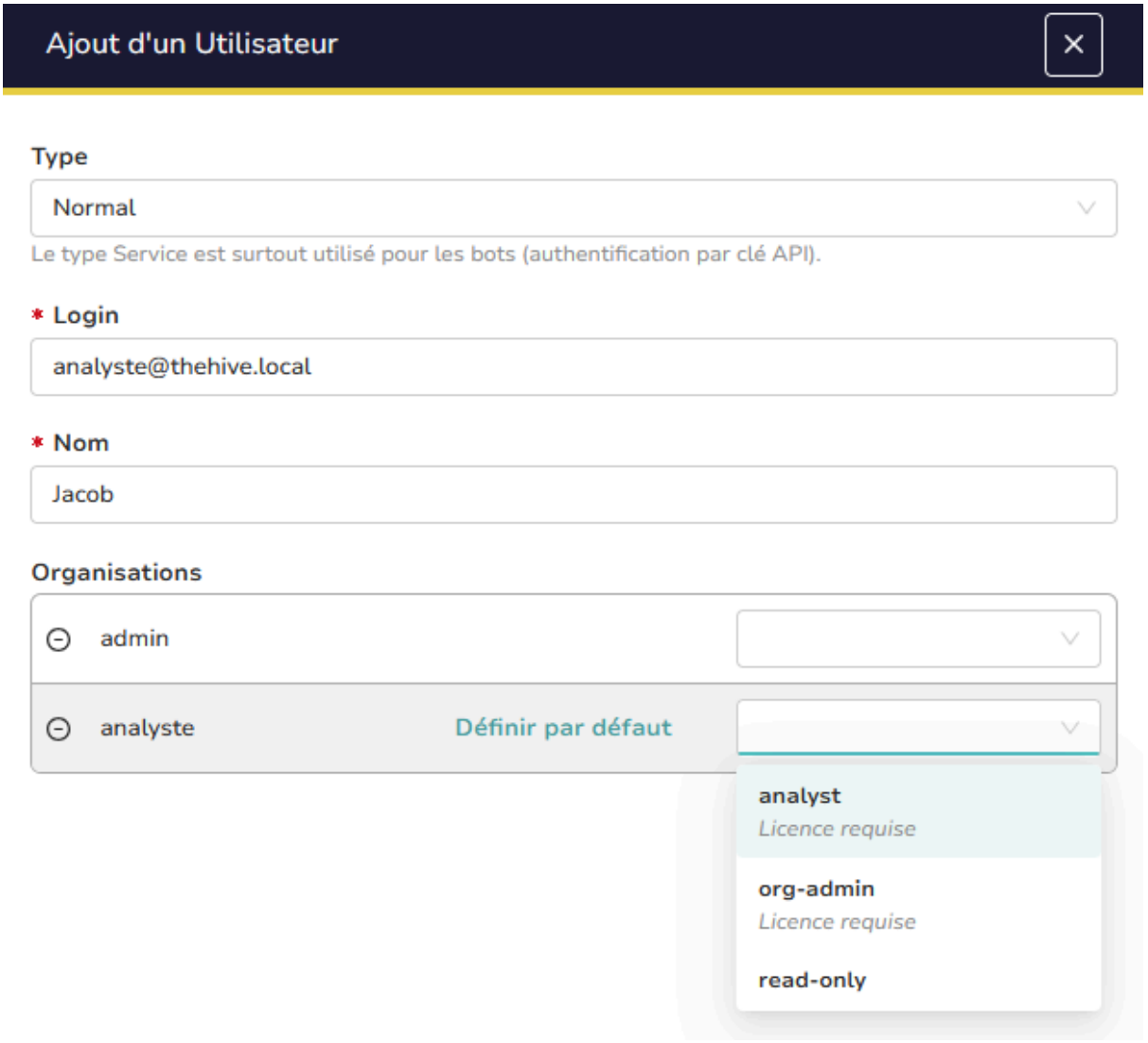
C’est la partie qui m’a semblé le moins bien expliquée dans la documentation officielle. En effet, pour pouvoir accéder au menu afin d’interconnecter les outils ou encore créer des case avec thehive il faut tout d’abord créer des comptes supplémentaires sur chaque plateforme. Les comptes admin n’ont pas tous les droits de création.

7.6.4.1 créer un nouveau compte sur thehive

Vous devez créer un compte supplémentaire en plus de l’administrateur et avec des droits différents afin de débloquer cette fonctionnalité. Cliquez sur utilisateur dans le menu de gauche de l’interface thehive, puis ajoutez un utilisateur avec les droits d’analyse, lecture et organisation.



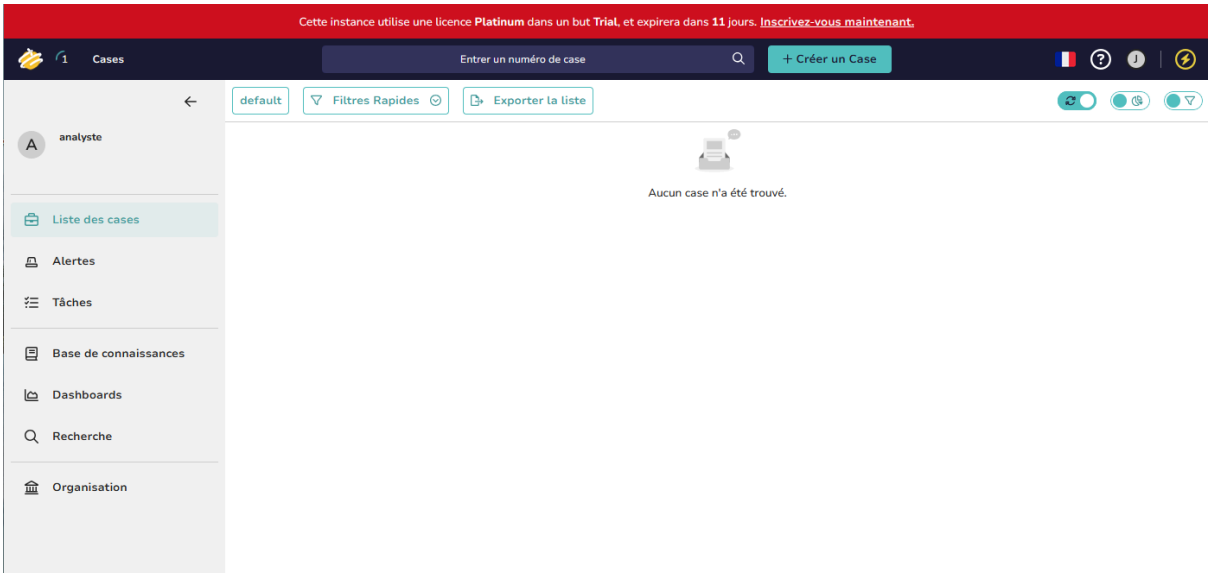



Ajout d'un Utilisateur
Type
Normal
Le type Service est surtout utilisé pour les bots (authentification par clé API).
* Login
analyste@thehive.local
* Nom
Jacob
Organisations
admin
analyste
Définir par défaut
analyst
Licence requise
org-admin
Licence requise
read-only


Bonjour,
Connectez vous pour commencer votre session
analyst
J'ai oublié mon mot de passe
Se connecter

7.6.4.2 créer un case dans thehive

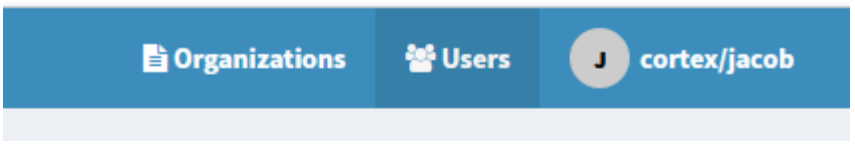
A présent vous verrez apparaître créer un case, qui n'était pas disponible précédemment. Grâce à cela nous pourrons continuer l'automatisation.

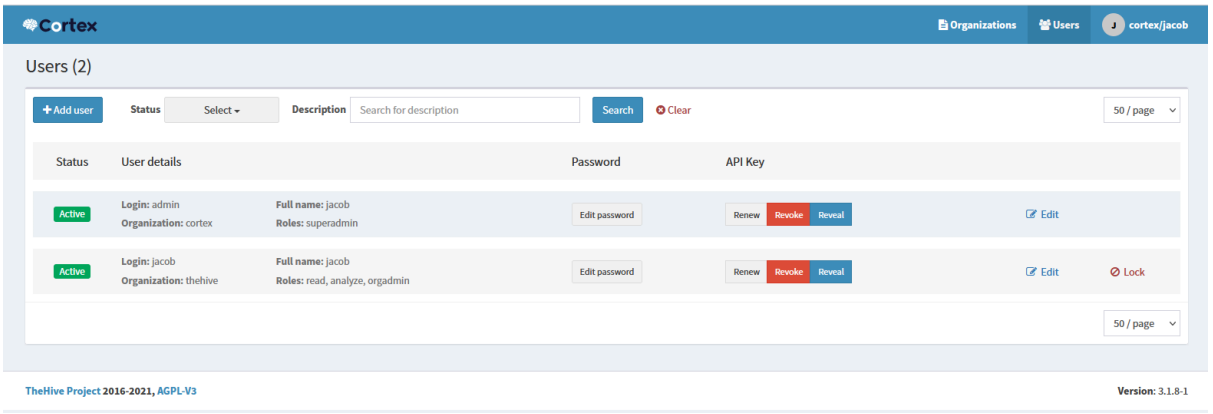


7.6.5 Interconnecter des analyseurs dans cortex

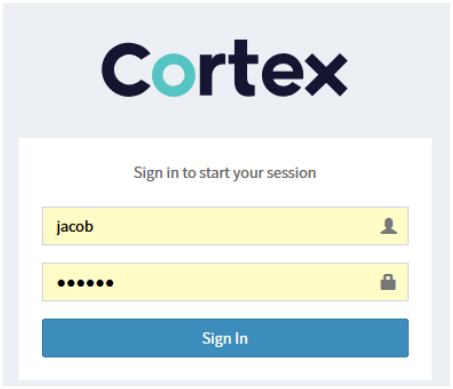
7.6.5.1 créer un nouveau compte sur cortex

Vous devez créer un compte supplémentaire en plus de l'administrateur et avec des droits différents afin de débloquer cette fonctionnalité. Cliquez sur user en haut à droite de l'interface cortex, puis ajoutez un utilisateur avec les droits d'analyse, lecture et organisation.



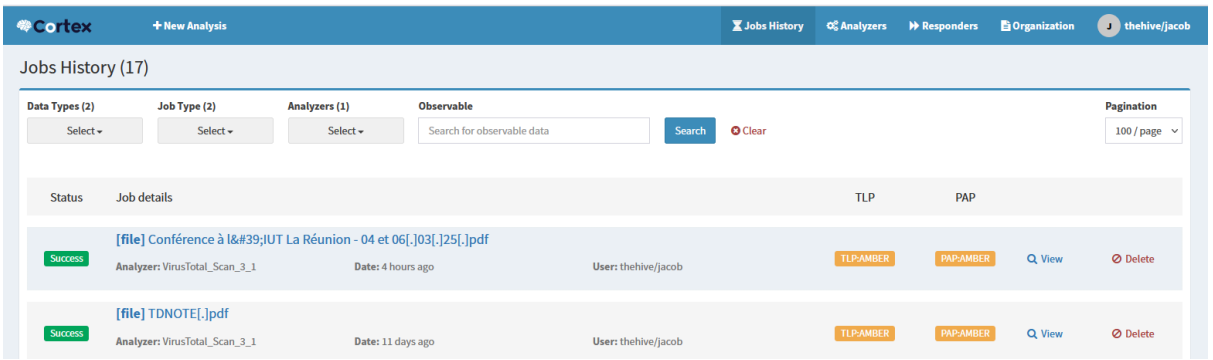


Une fois créée, vous devez sortir du compte administrateur et vous connecter avec le nouveau compte.

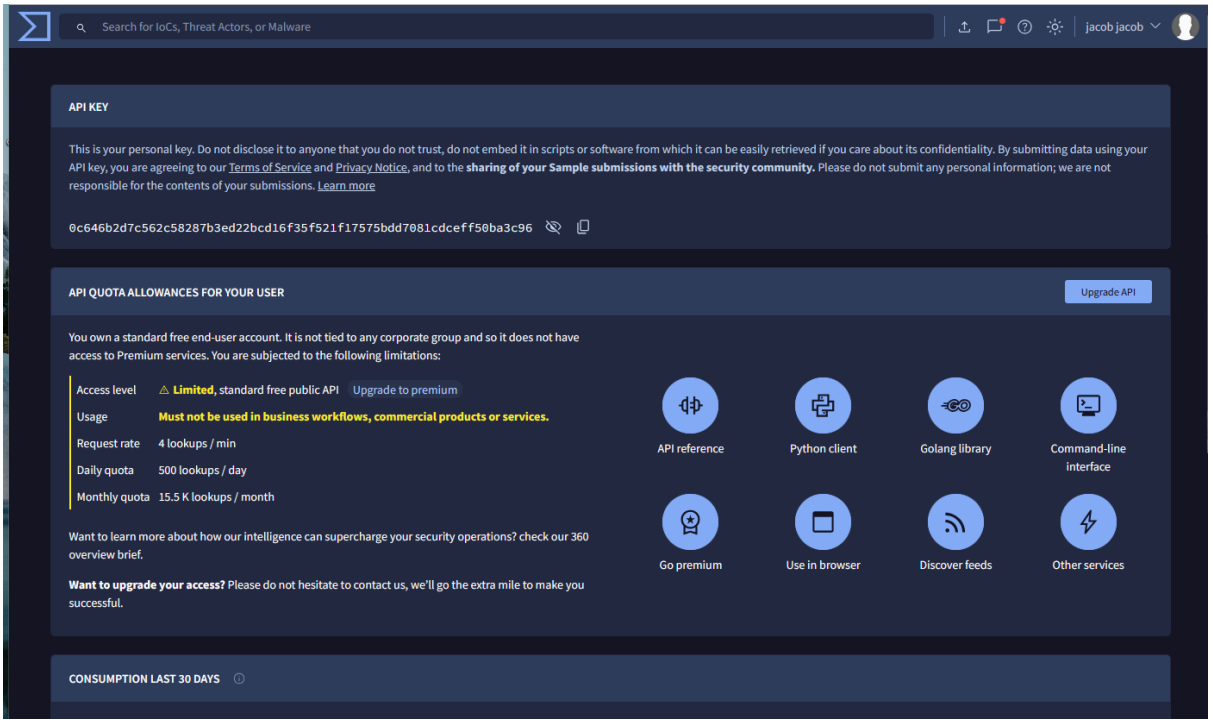


7.6.5.2 Ajouter des analyseurs: virus total

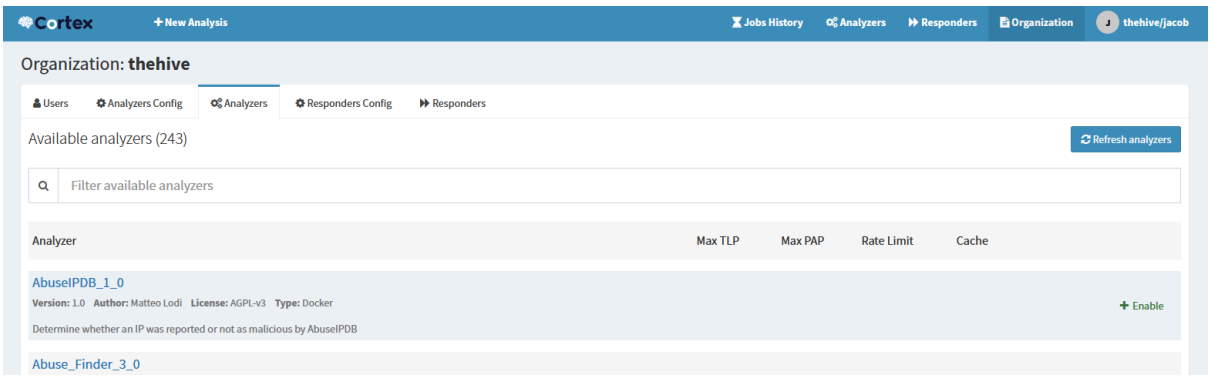
De nouvelles fonctionnalités apparaissent dans le menu en haut à droite et à gauche. Vous pouvez désormais ajouter un analyseur.

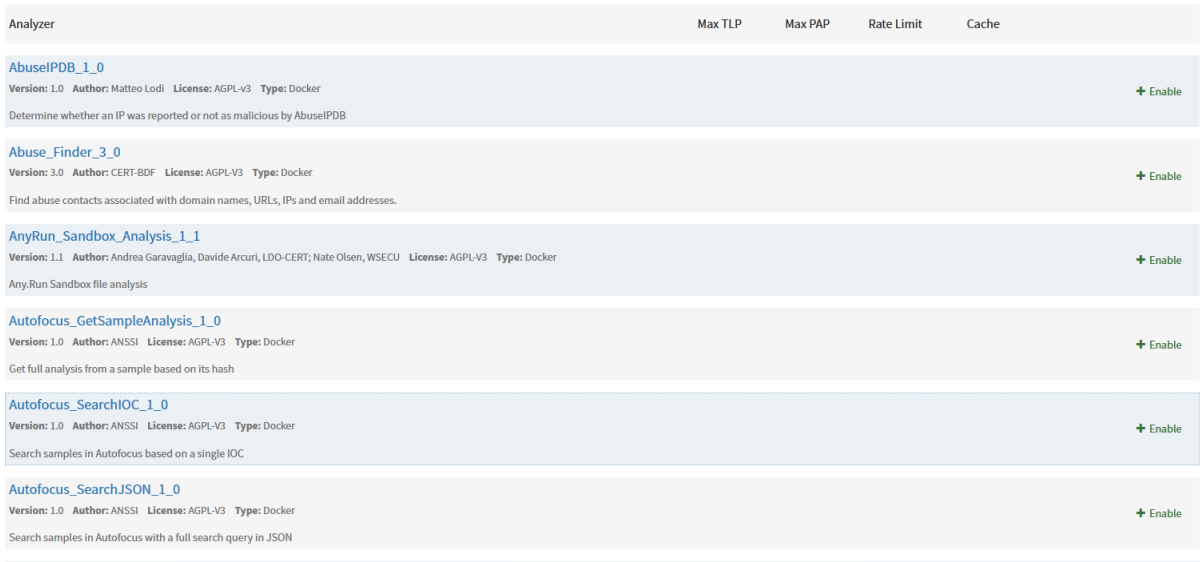


Créez d'abord un compte virutotal et récupérez une clé API.

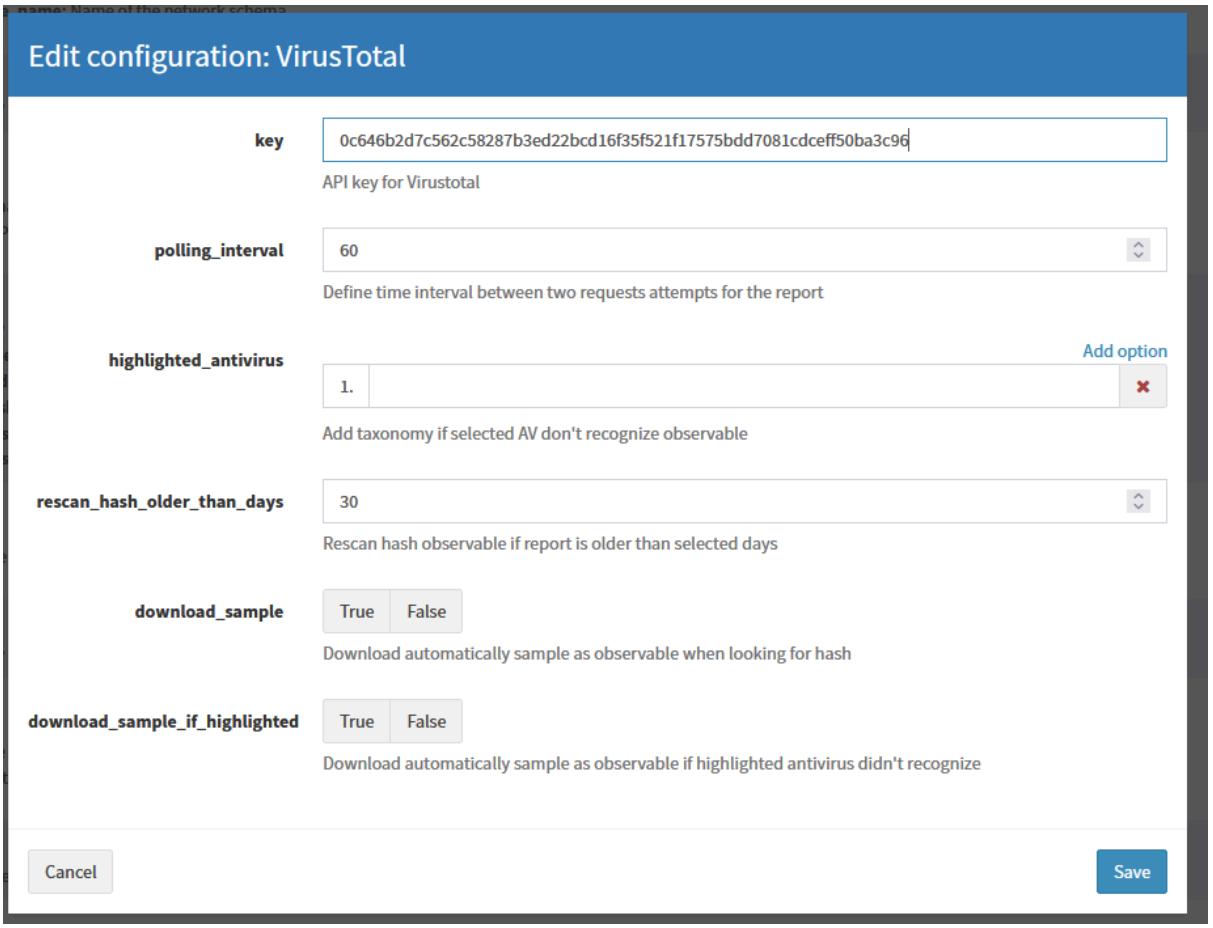


Revenez à cortex et cliquez sur organisation et sur analyseur. Une liste apparaîtra. Choisissez ceux à ajouter. Ici nous prenons l'exemple de virus total.





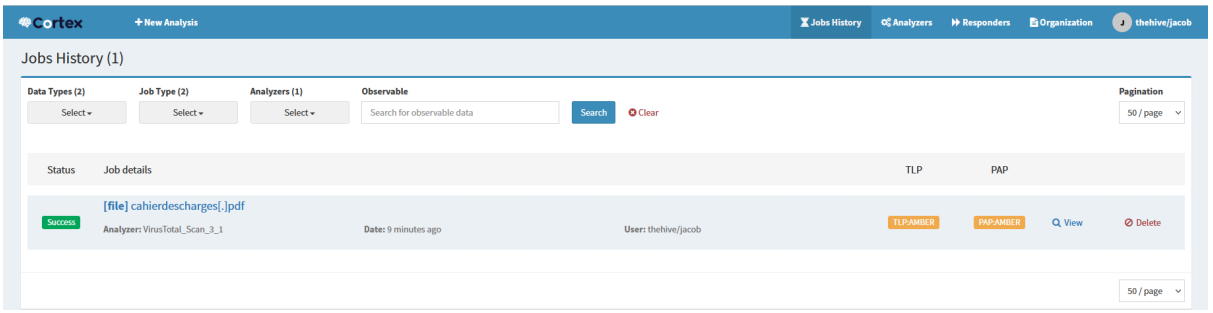
Autorisez virustotal et ajoutez les informations dans la fenêtre qui apparaît.



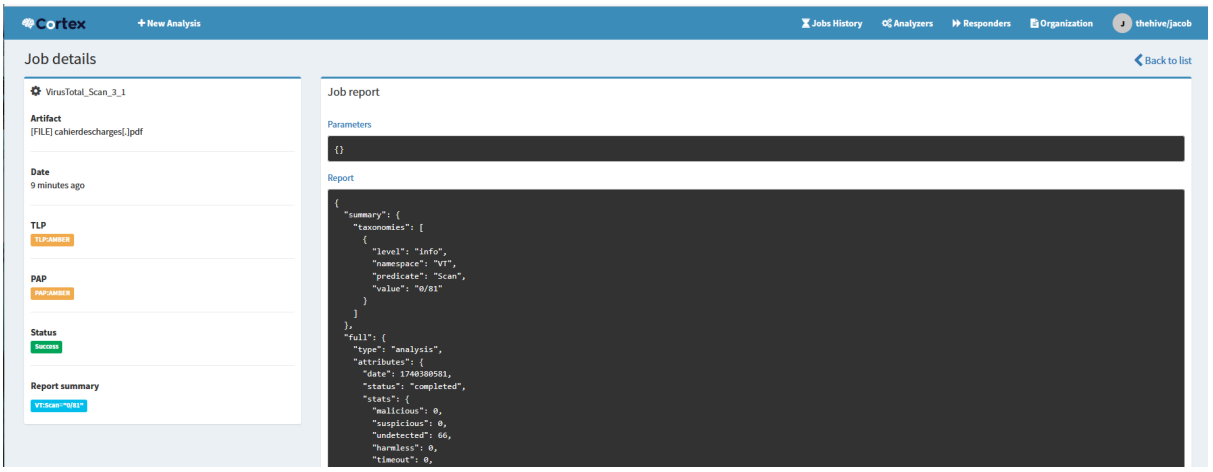
7.6.5.3 Vérifiez l'intégration de virustotal sur cortex:

En haut à gauche cliquez sur créer une nouvelle analyse, insérer un fichier manuellement.

Dans job history vous constatez que le travail est en cours.



Une fois l'analyse complétée vous pourrez la consulter.



7.6.6 Installer n8n localement avec docker

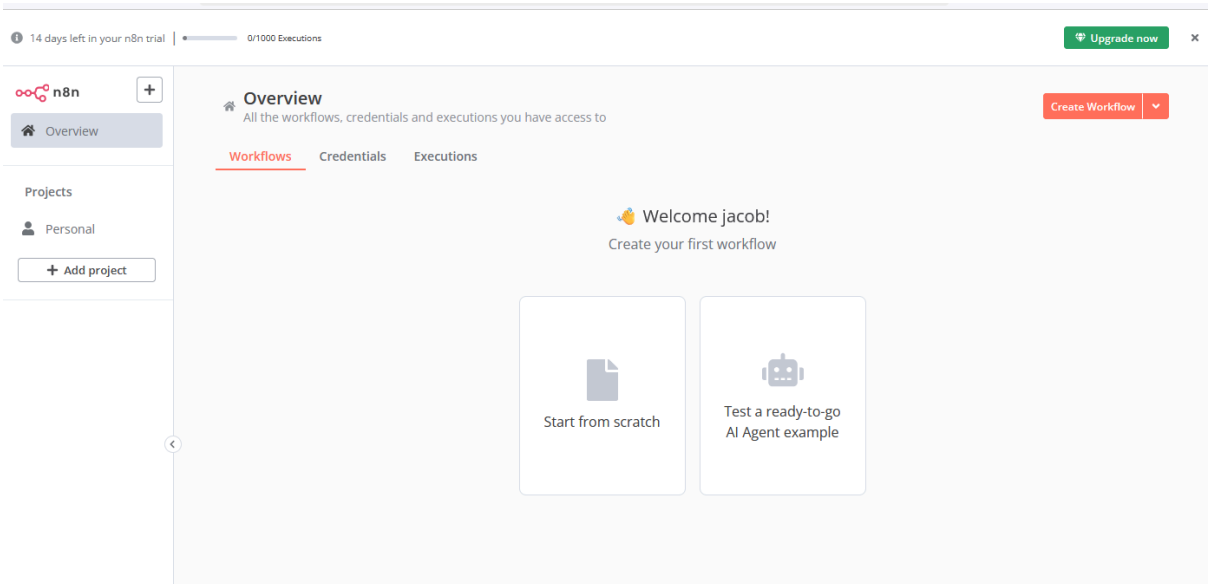
https://docs.n8n.io/hosting/installation/docker/

Installez docker puis suivez simplement le script automatique pour lancer n8n.

```
docker volume create n8n_data

docker run -it --rm --name n8n -p 5678:5678 -v
n8n_data:/home/node/.n8n docker.n8n.io/n8nio/n8n
```

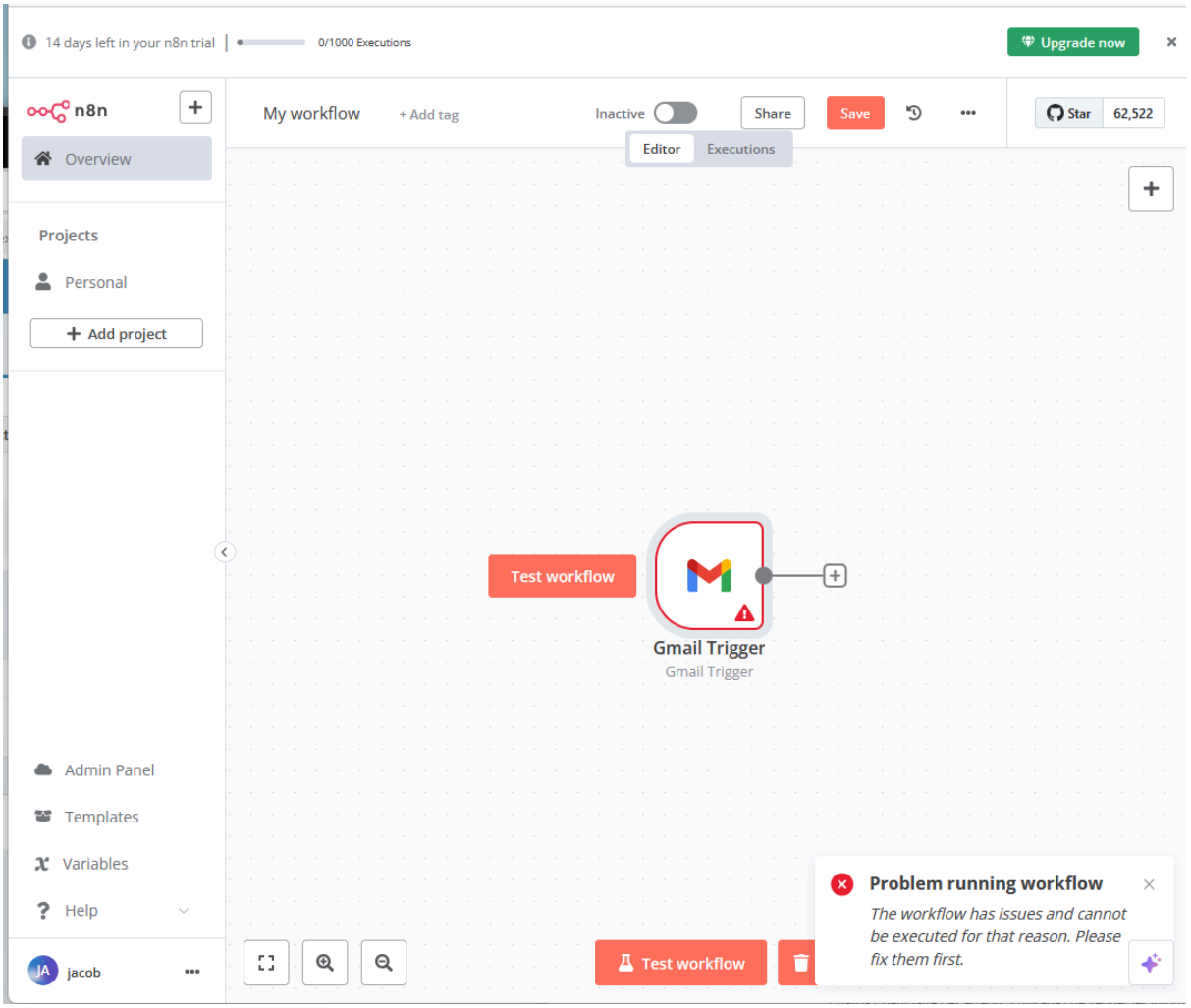
```
eceived SIGINT. Shutting down...

topping n8n...
kb@jkb2-vm:~$ sudo docker run -it --rm --name n8n -e N8N_SECURE_COOKIE=false -p 5678:5678 -v n8n_data:/home/node/.n8n d
cker.n8n.io/n8nio/n8n
ermissions 0644 for n8n settings file /home/node/.n8n/config are too wide. This is ignored for now, but in the future n
n will attempt to change the permissions automatically. To automatically enforce correct permissions now set N8N_ENFORC
_SETTINGS_FILE_PERMISSIONS=true (recommended), or turn this check off set N8N_ENFORCE_SETTINGS_FILE_PERMISSIONS=false.
ser settings loaded from: /home/node/.n8n/config
nitializing n8n process
8n ready on 0.0.0.0, port 5678
ersion: 1.79.3

ditor is now accessible via:
ttp://localhost:5678/

ress "o" to open in Browser.
wner was set up successfully
ser survey updated successfully
```

Une fois connecté à n8n, découvrez la plateforme. Elle est facile d'utilisation, très intuitive, le UI est très bien fait, et le visuel agréable.

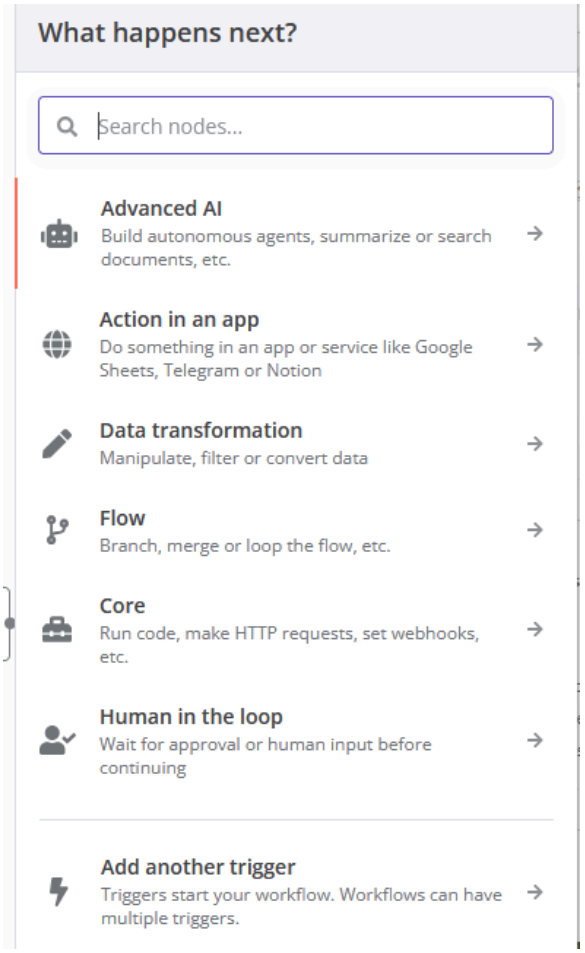


7.6.7 Ajouter des connecteurs et déclencheurs dans n8n

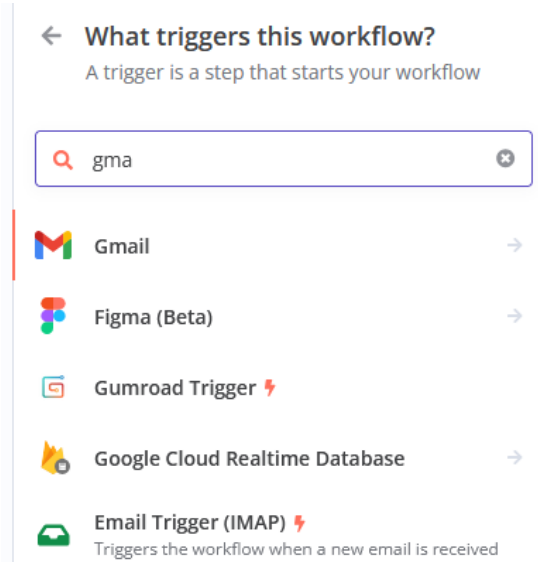
Prenons l'exemple de gmail. Dans notre workflow nous déclenchons le processus à réception d'un email. Nous ajoutons un module, en cliquant sur le bouton plus en haut à droite de la fenêtre.



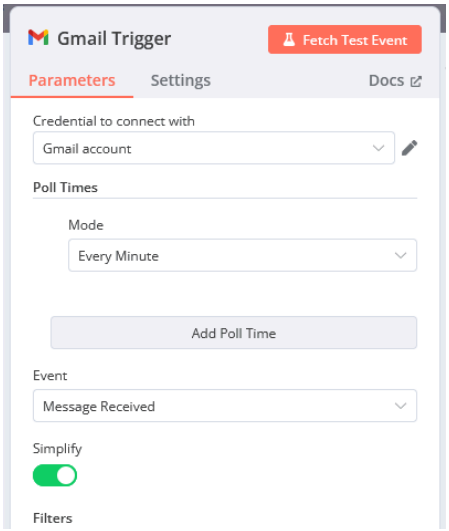
Une fenêtre s'ouvre et offre différentes options



Vous pouvez ajouter votre recherche

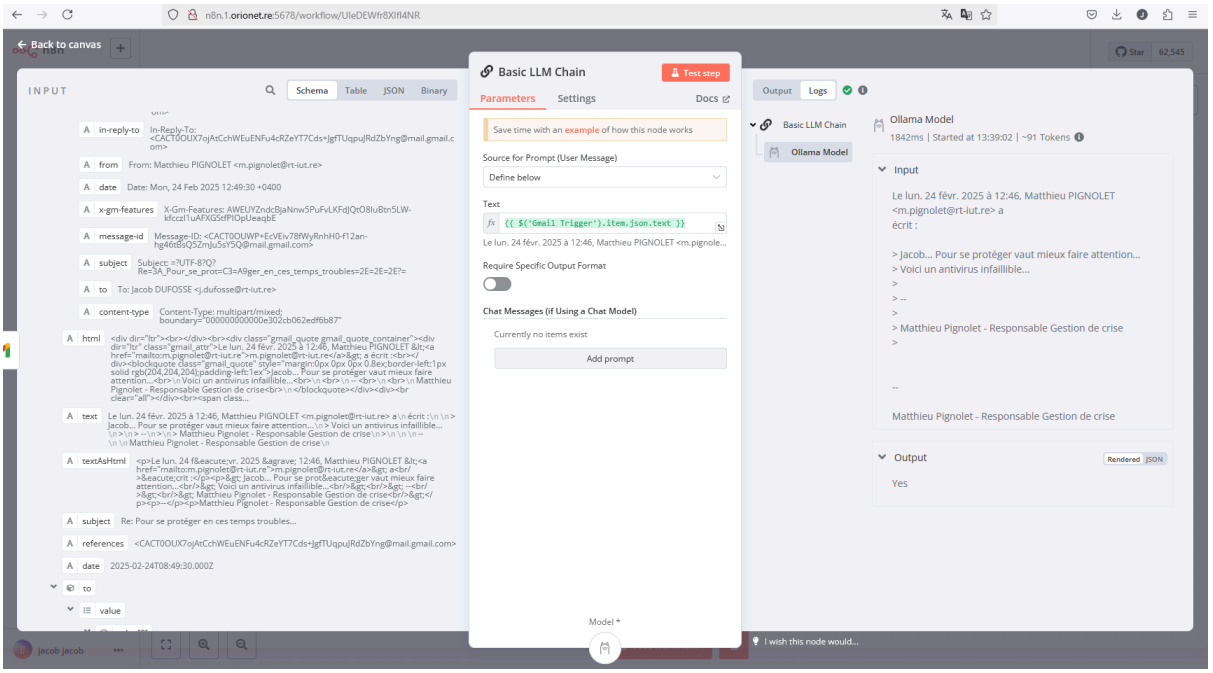


Les menus d'option sont assez simples et intuitif pour être rapidement compris.

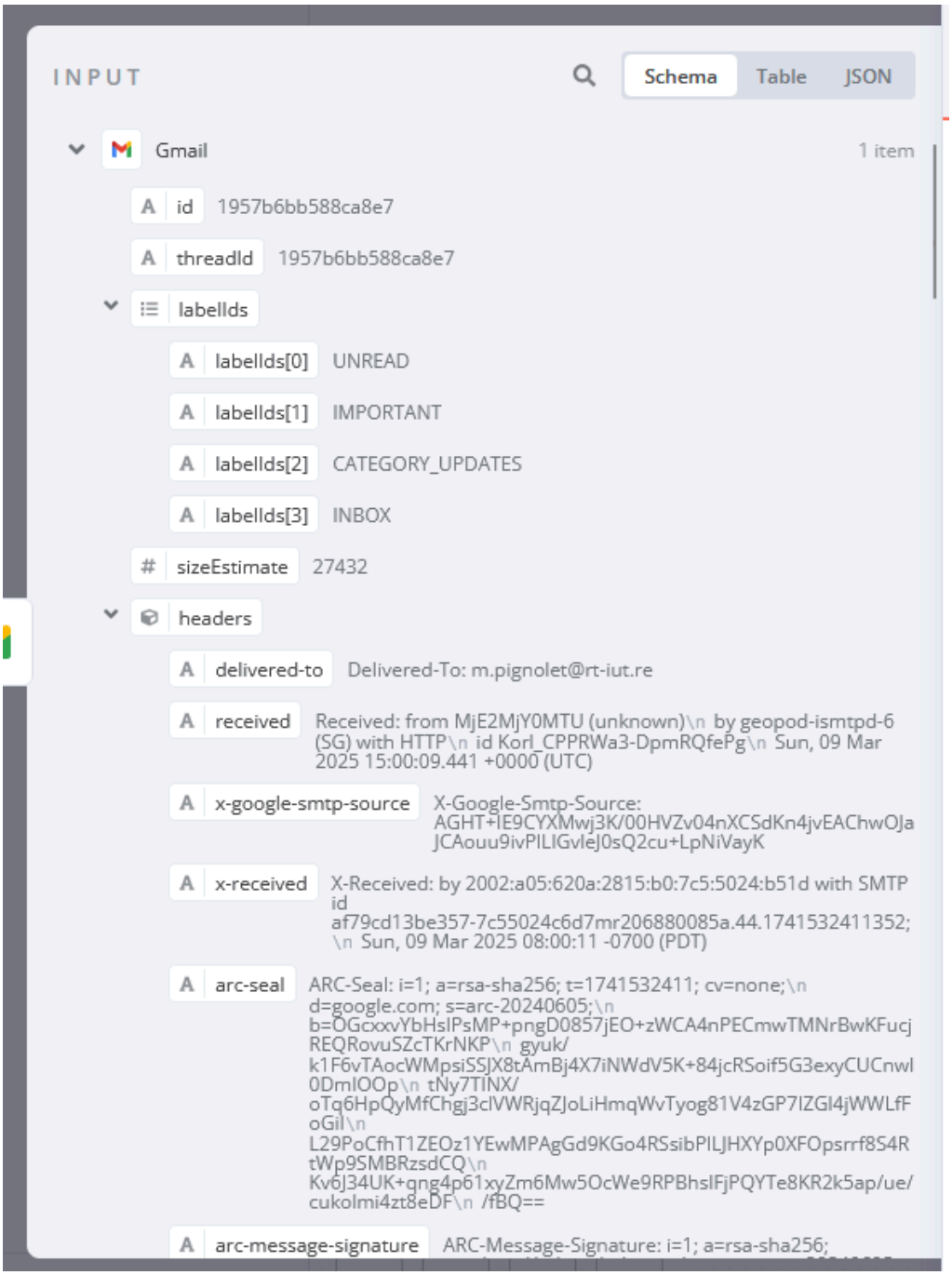


L'intérêt principal réside dans l'utilisation rapide et facile des données provenant des précédents modules. Par exemple, à la suite de la réception d'un courriel, nous pouvons immédiatement ajouter les différents éléments directement dans les champs d'un module suivant.

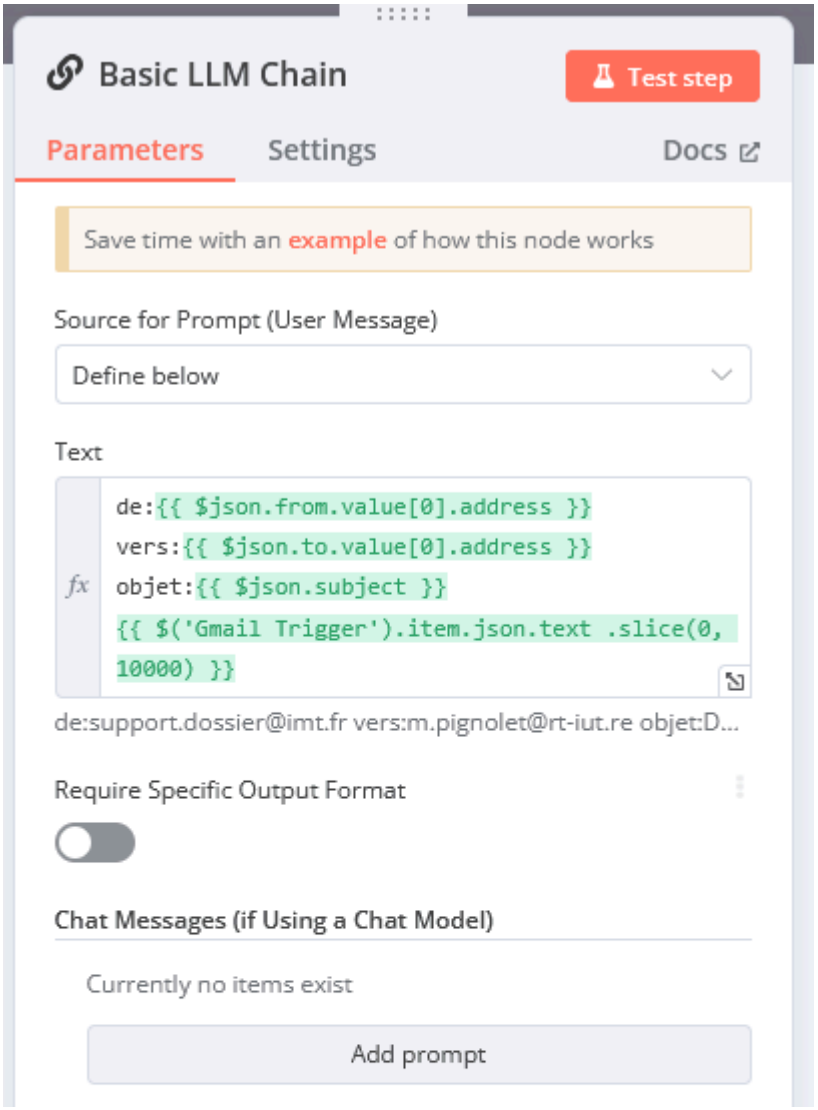
Exemple avec notre IA qui vérifie le contenu d'un courriel.



Dans la partie de gauche nous avons à disposition tous les éléments en provenance du courriel que nous pouvons glisser dans la fenêtre de configuration de notre module LLM AI. Les données sont disponibles en table, schéma et JSON format.



Dans la partie centrale, nous pouvons simplement les glisser dans la fenêtre et constituer par exemple l'entrant principal à analyser par notre LLM. Ici **de: …. , vers:…., object:… et contenu… Ce contenu est désormais dynamiquement rempli et à chaque nouvel email, les informations seront remplacées.**



Dans la partie de droite on peut observer l'analyse du LLM IA sur le contenu du message. Elle nous donne son analyse, opinion et nous indique une décision, YES or NO. Dans ce cas, c'est non, ce n'est pas un spam.

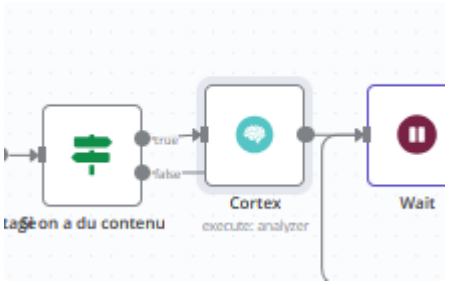
Output Logs Table JSON Schema

1 item

text

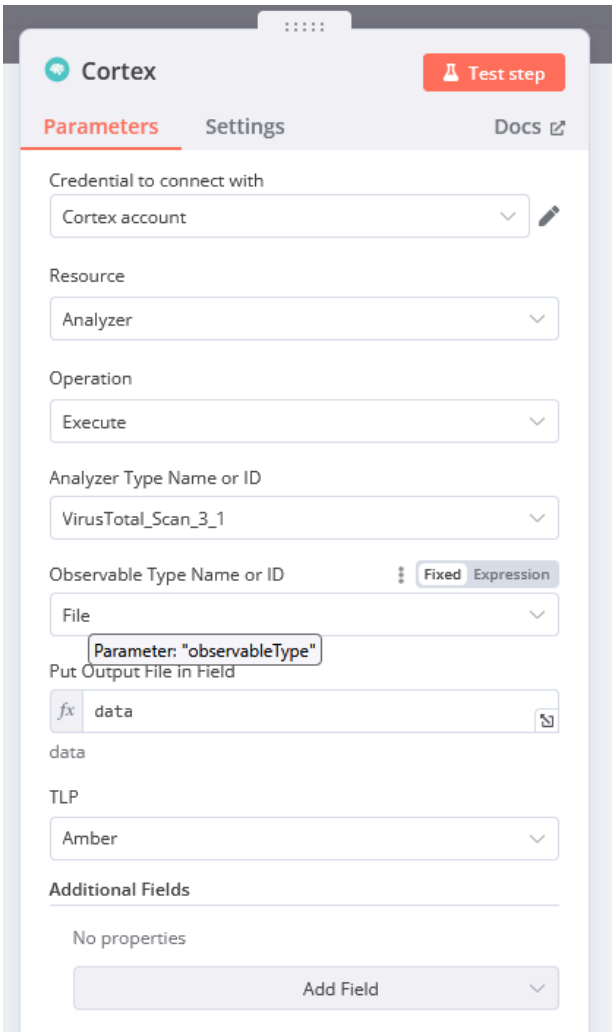
<think>\n Okay, I need to determine whether the given email is spam or not. Let me go through it step by step. \n \n The email is addressed from support.dossier@imt.fr to Matthieu Pignolet. The subject line mentions "Derniers jours pour candidater..." which translates to "Last days to apply for...". This seems related to a job opportunity or application, possibly for an educational program given the context of Ecoles de l'IMT.\n \n Looking at the content, it's informing Matthieu that he has started a candidate dossier and is reminding him about the last date for submission until March 11, 2025. It also provides a link to access the candidacy space and includes instructions on how to submit his application. \n \n The email seems official, coming from an institution's support address, and it's clearly related to a job application process. There's no indication of unsolicited nature or promotional content; instead, it's a notification about a pending application and deadlines.\n \n No clear signs of phishing, malicious links, or deceptive content are present. The tone is professional and informative, without any typical traits of spam such as excessive exclamation marks, urgent but irrelevant information, or requests for personal data beyond the provided link.\n \n Therefore, this email doesn't meet the criteria of unsolicited spam. It serves a legitimate purpose related to an ongoing application process.\n </think>\n \n no

Un dernier exemple de module facile à implémenter c'est la connexion avec cortex

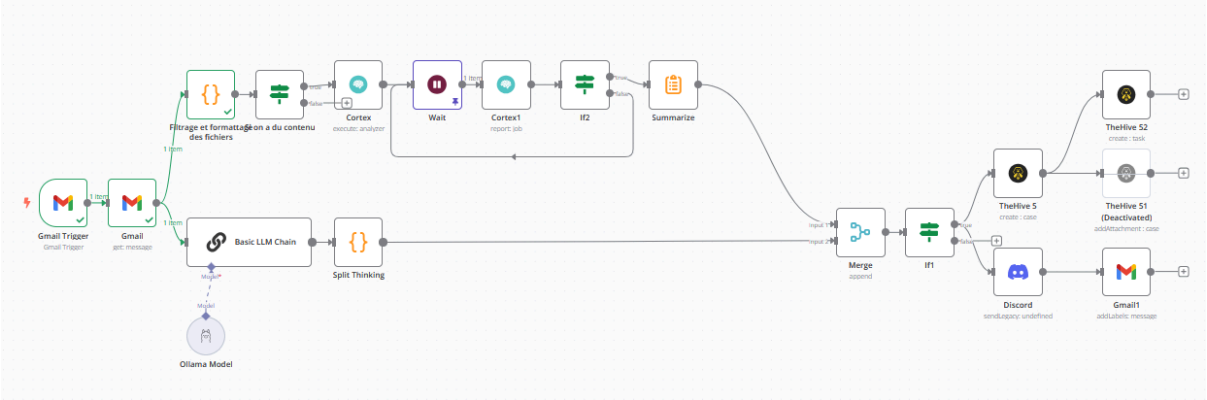


En connectant le compte cortex (cliquez sur le stylo et rentrez API et adresse URL du serveur), vous obtiendrez immédiatement des informations comme les analyseurs à

disposition dans cortex, et que vous pouvez utiliser ici avec les données que vous choisissez comme vu précédemment.

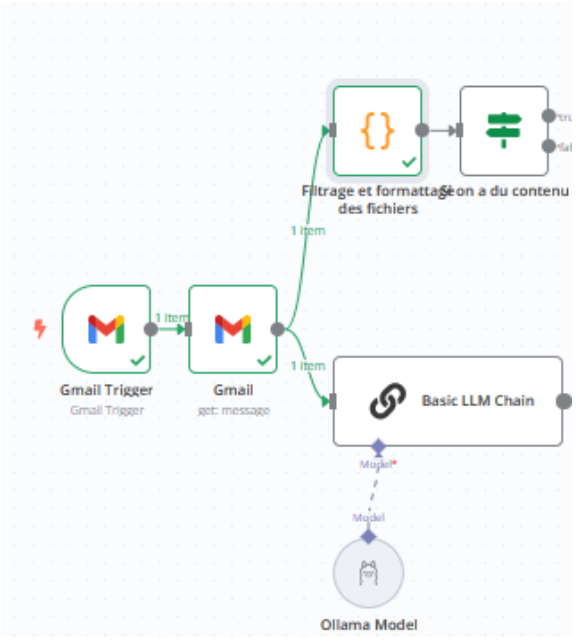


7.7 Orchestration complète

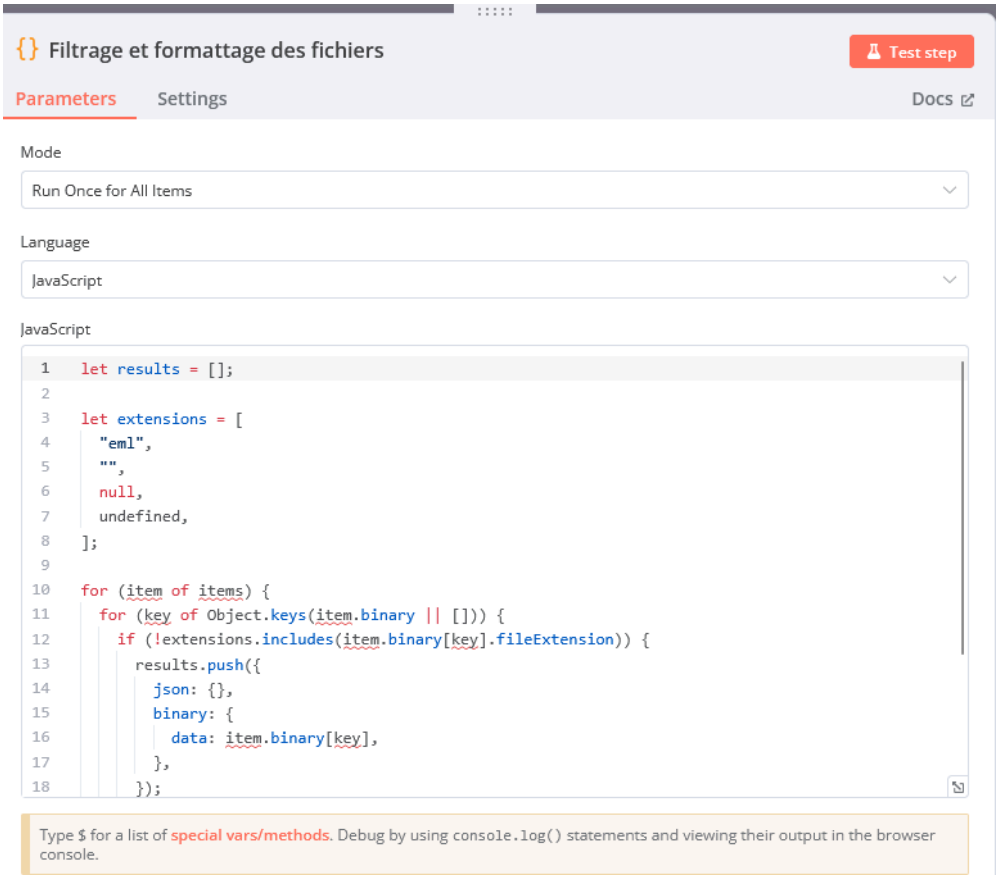


Nous pouvons voir visuellement sur ce schéma ci haut qu'il y a deux branches comme nous l'avons modélisé dans notre section 7.5.3.3 Processus détaillé de traitement : schéma / page 28

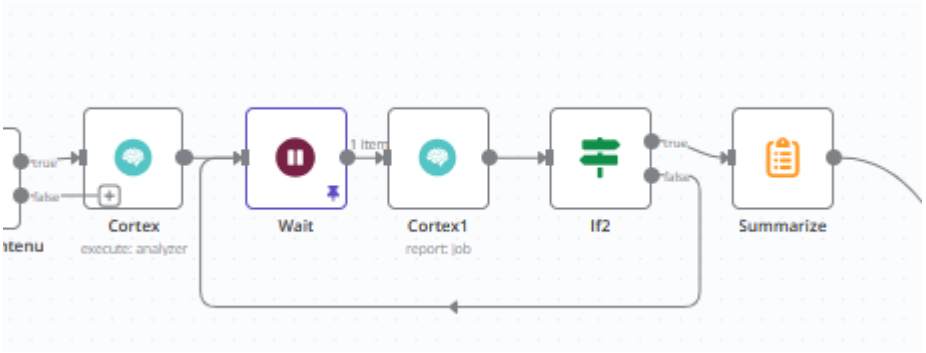
7.7.1 Bloc de traitement initial : une branche qui sépare les pièces jointes, du contenu



Le module filtrage utilise un script permettant de rejeter les éléments de contenu et de ne retenir que les fichiers binaires (les attachements que nous analysons).



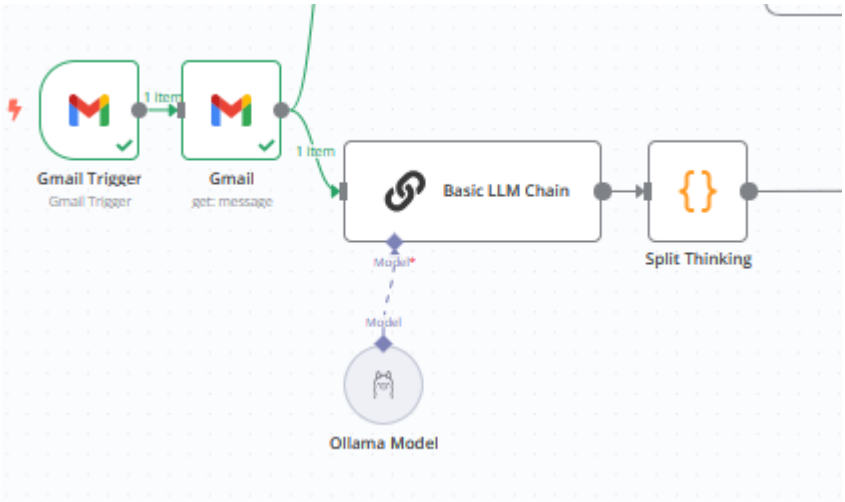
7.7.2 Bloc de traitement cortex : analyse de chaque pièce jointe via cortex (et virus total)



Cette branche ci haut permet d'itérer toutes les pièces jointes, et d'agréger les résultats de traitement (summarize) afin de transmettre à la branche suivante pour combiner le résultats avec la branche LLM AI (qui analyse le contenu textuel du courriel).

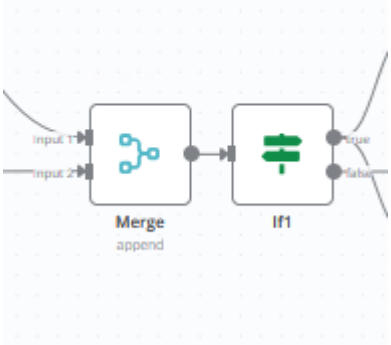
7.7.3 Bloc de traitement LLM IA : la branche qui analyse du contenu textuel pour verdict, phishing ou non.

Nous avons déjà donné des précisions précédemment sur le contenu traité et la sortie générée (voir page 46 à 49).

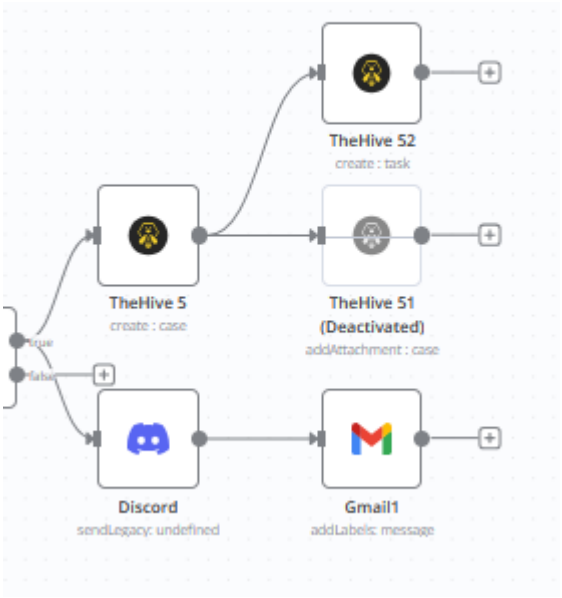


7.7.4 Bloc de regroupement des informations décisionnelles :

une zone qui décide si oui ou non il y a action. Si rien de suspect, aucune action.



7.7.5 Bloc d'actions:



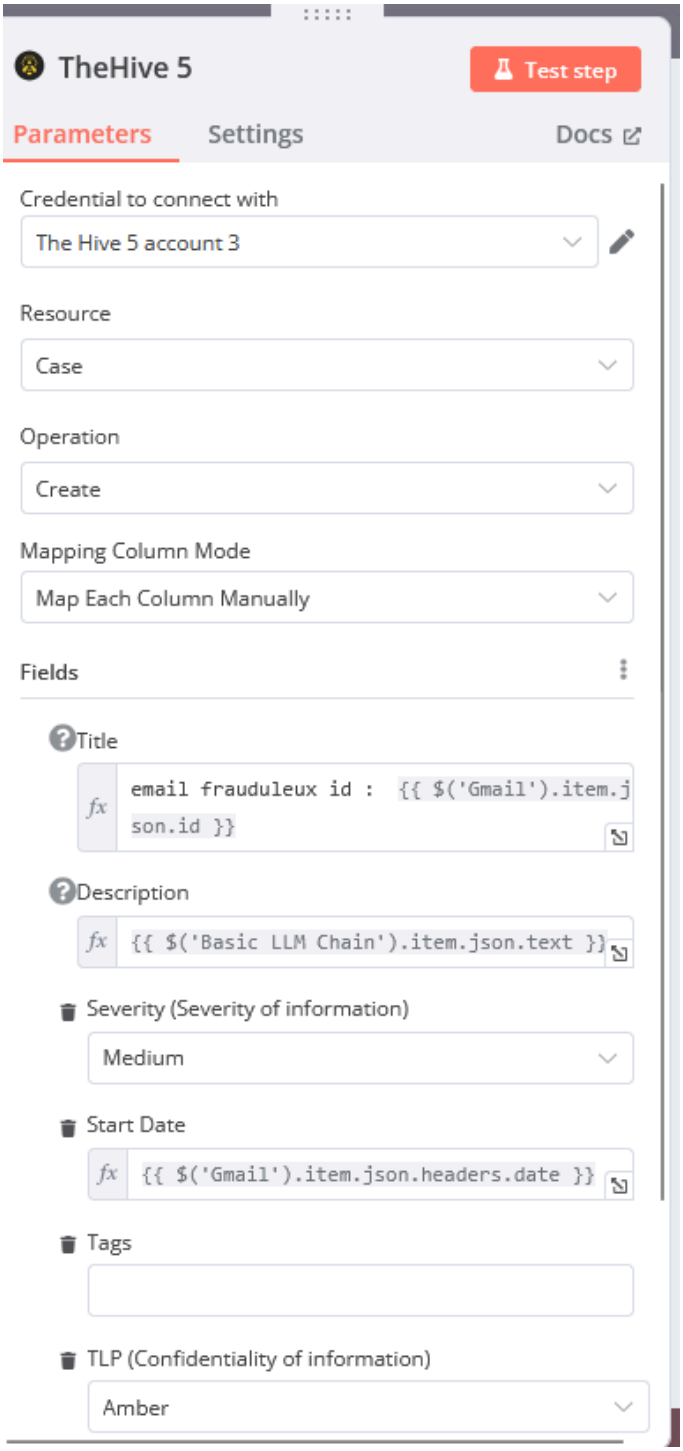
Exemple du module thehive, nous choisissons créer un case et nous pouvons pré remplir dynamiquement les informations qui vont peupler le case dans l'interface thehive.

Il faudra un module séparé pour transmettre la pièce joint et l'ajouter au dossier (nous n'avons pas terminé cette partie).

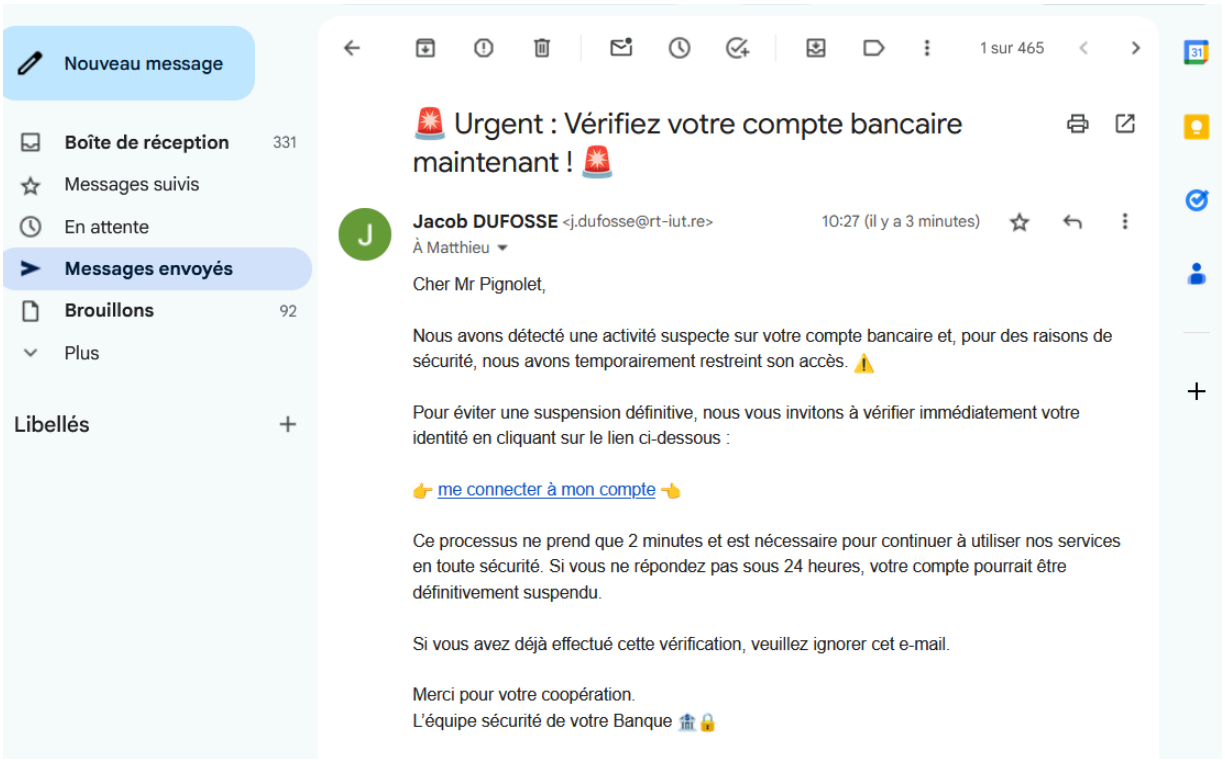
Nous utilisons, comme on peut le voir, les informations de schéma suivantes pour tester la création dynamique d'un case:

- texte d'analyse du LLM
- la date de démarrage du cas
- le nom de l'email

Sur la page suivante vous pouvez voir la configuration dynamique du module.



Nous testons donc le module en réceptionnant un email frauduleux (phishing contenant une URL). “Cher Mr Pignolet…”

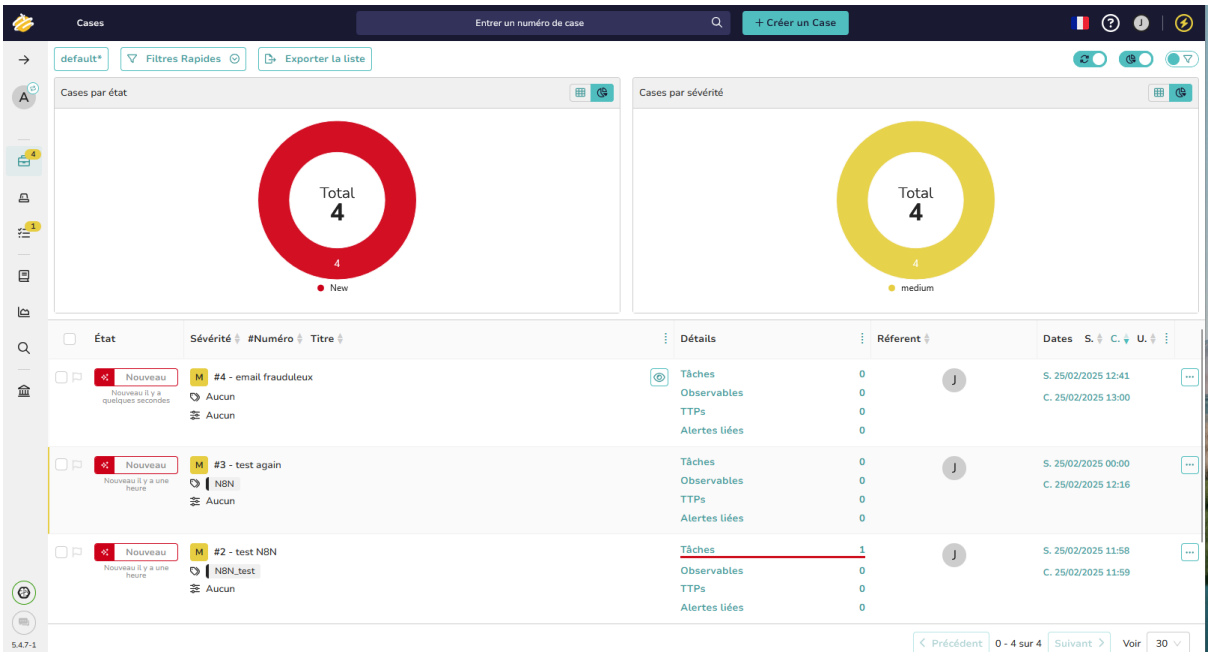


La détection est effective, le LLM juge que c'est un courriel de phishing. Le case est automatiquement créé dans la plateforme thehive comme on peut le voir sur la page suivante, sous le titre de cas email frauduleux. Les informations sont bien collectées comme souhaité (description et date).

Beaucoup de champs d'informations sont disponibles, mais nous ne les avons pas encore testés (ceci est attendu dans une deuxième partie, puisque celle-ci était dans un but de découverte et de prise en main).

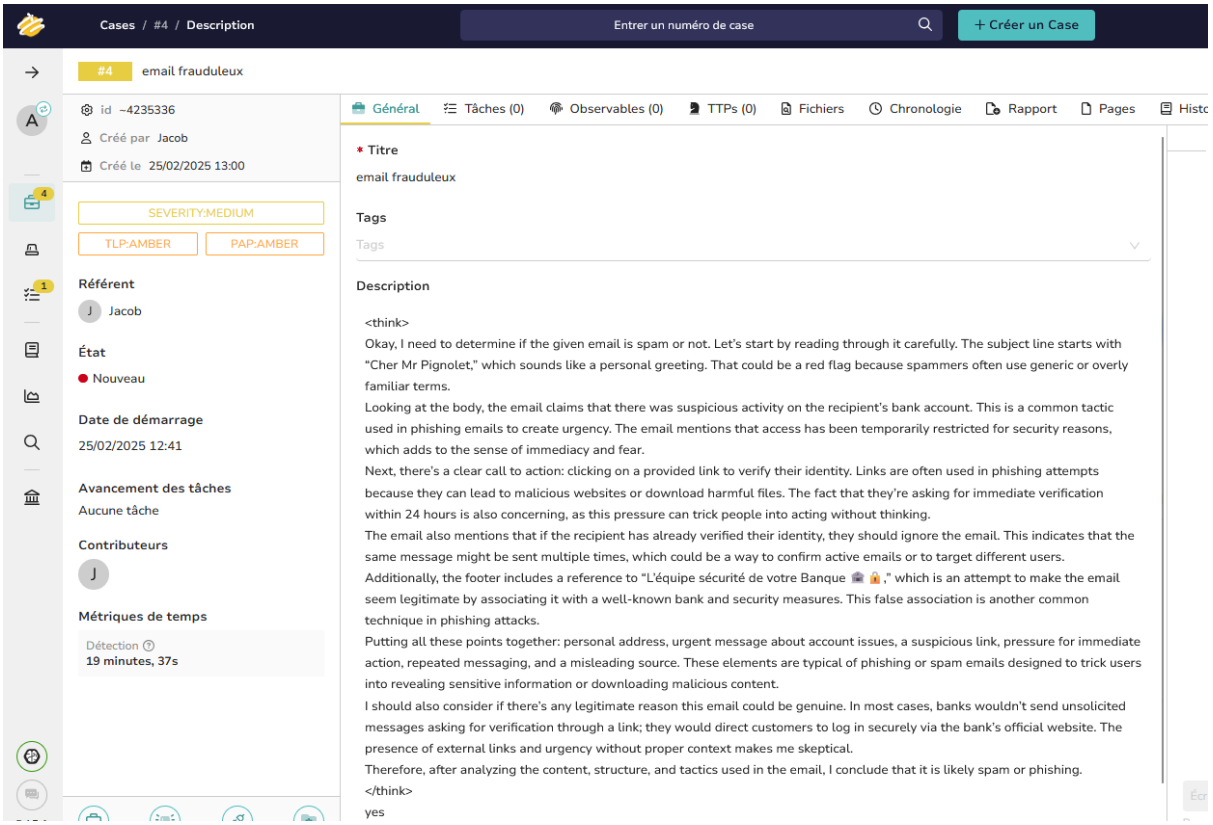
Nous pouvons aussi automatiser l'ajout de tâches, une fois le cas créé (par exemple des tâches pourraient être réparties automatiquement à chaque spécialiste impliqué).

Interface thehive qui résume les cas qui viennent d'être créés. En tête de liste on peut voir que notre cas email frauduleux vient bien d'être créé.

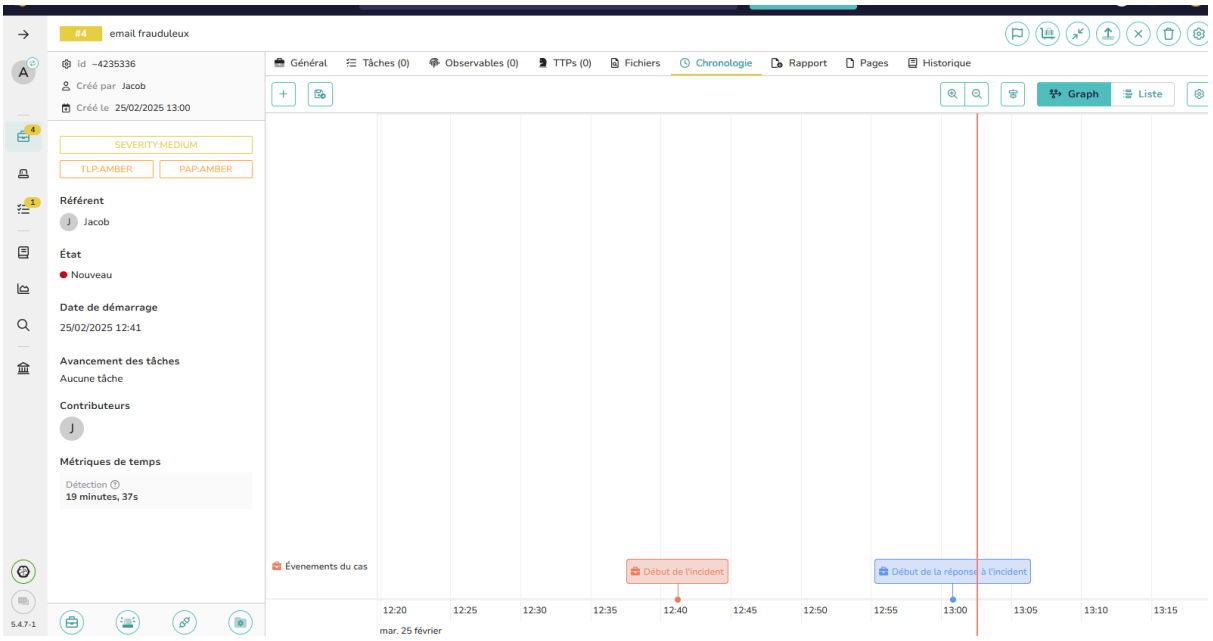


En cliquant sur le cas email frauduleux (en tête de liste), nous rentrons dans les détails du cas.

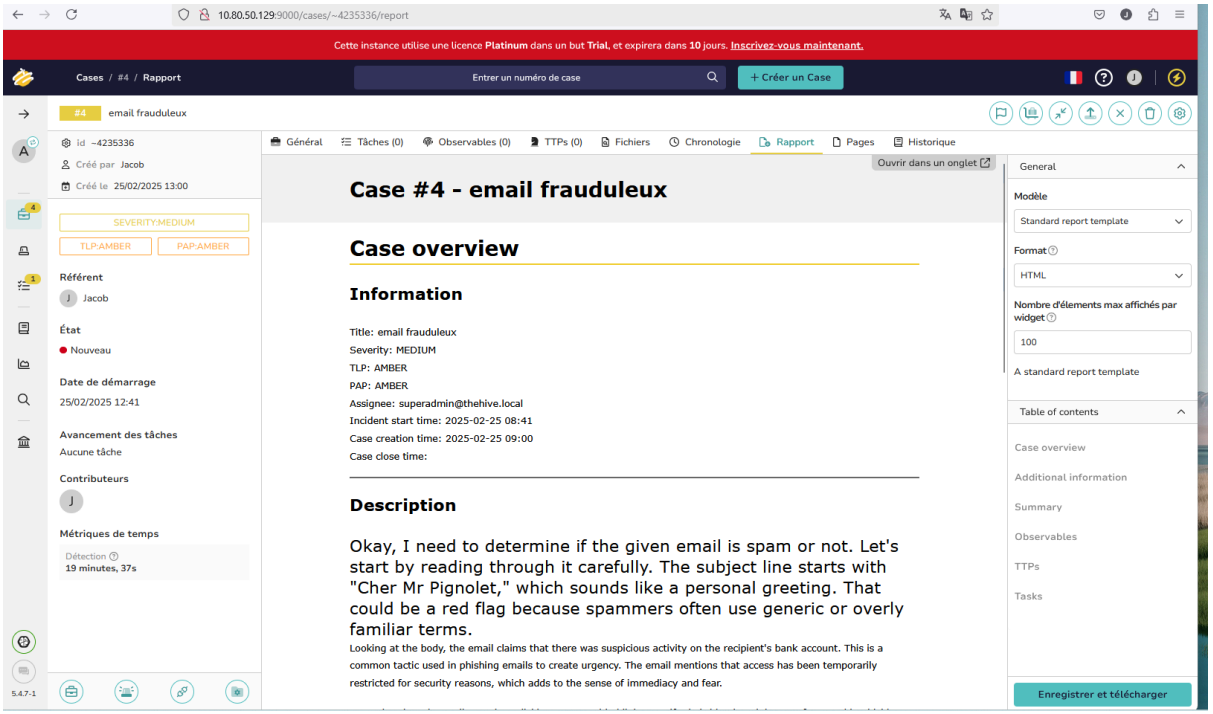
La description qui contient l'analyse LLM.

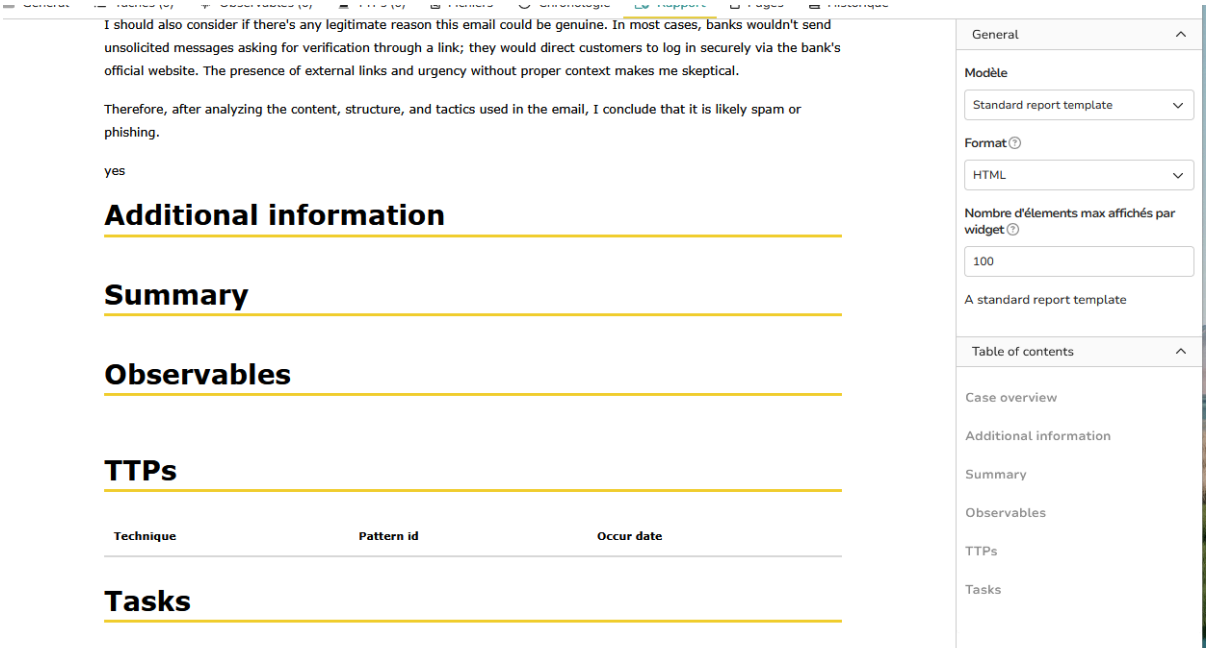


La timeline du cas :

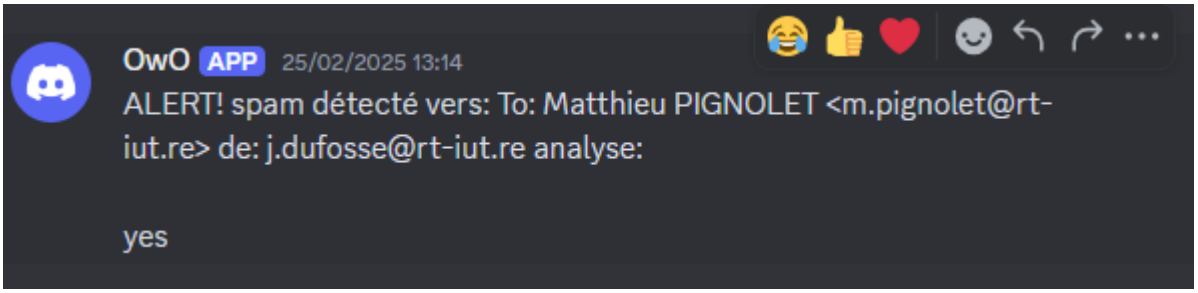


Le résumé du cas en question:

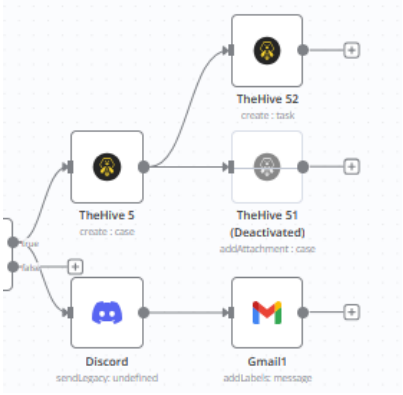


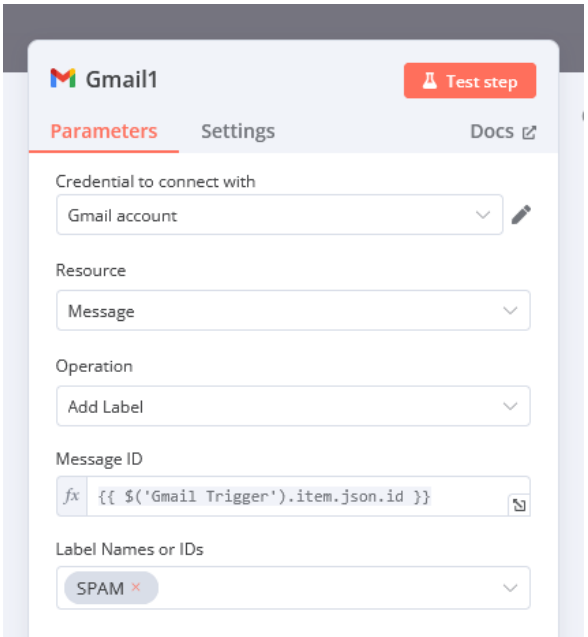


Les alertes sont bien envoyées sur discord automatiquement:



Enfin la dernière action c'est de placer ce courriel dans les spams.Et cela fonctionne correctement.





7.8 Conclusion

Notre projet d'implémentation d'une solution professionnelle de réponse à incident avec TheHive, Cortex et n8n représente une découverte significative pour notre boîte à outil de réponse à incident. Cette approche modulaire nous a permis de créer un workflow efficace qui:

1. Capte automatiquement les emails suspects via Gmail API
2. Sépare et analyse le contenu textuel (via LLM) et les pièces jointes (via Cortex/VirusTotal)
3. Prend une décision sur la nature malveillante du message
4. Déclenche des actions automatisées en cas de détection positive (création de cas dans TheHive, notification Discord, déplacement du message vers les spams)

Malgré des défis techniques (complexité d'installation, besoins en ressources, documentation lacunaire), notre équipe a réussi à mettre en place une preuve de concept fonctionnelle qui démontre la valeur ajoutée de ces outils professionnels pour la réponse à incident.

L'utilisation de n8n comme orchestrateur s'est révélée particulièrement judicieuse grâce à son interface intuitive et ses capacités d'intégration rapide.

La solution actuelle constitue une base qui prépare le terrain pour une implémentation plus complète du workflow théorique avancé que nous avons modélisé.

7.9 Axes d'amélioration pour une seconde phase

1. **Enrichissement des cas TheHive**:
    - Implémentation de l'ajout automatique des pièces jointes au dossier
    - Création et assignation automatique de tâches aux analystes selon leur expertise

- Exploitation des champs supplémentaires disponibles pour enrichir les métadonnées des cas

2. **Extension des capacités d'analyse**:
   - Intégration d'analyseurs Cortex supplémentaires (URLhaus, PhishTank)
   - Ajout d'un système de sandbox pour l'analyse dynamique des pièces jointes
   - Amélioration de l'extraction et de l'analyse des URLs embarquées dans les emails
3. **Automatisation avancée**:
   - Mise en œuvre des étapes d'investigation approfondie (analyse de propagation)
   - Implémentation des phases de confinement et remédiation automatisées
   - Intégration avec les systèmes de sécurité existants (EDR, Firewall, SIEM)
4. **Amélioration de la prise de décision**:
   - Développement d'un système de score combinant les résultats des différentes analyses
   - Implémentation d'un modèle d'apprentissage supervisé pour affiner la classification
   - Création de règles de détection plus granulaires basées sur le retour d'expérience
5. **Documentation et formation**:
   - Création d'une documentation détaillée sur l'architecture et les workflows
   - Développement de procédures opérationnelles standards pour l'équipe SOC
   - Mise en place d'un système de retour d'expérience et d'amélioration continue
6. **Intégration de MISP**:
   - Ajout de MISP (Malware Information Sharing Platform) pour le partage d'indicateurs

Cette seconde phase nous permettrait de transformer notre preuve de concept actuelle en une solution complète de réponse à incident, capable de suivre l'intégralité du cycle de vie d'un incident de sécurité, depuis la détection initiale jusqu'au retour à la normale et aux leçons apprises.