



Rapport

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

MAHADALI Neil

DUFOSSE Jacob

DITTOO Farhan

PIGNOLET Matthieu

Sommaire

Introduction.....	4
1. Introduction.....	4
Contexte et Problématique.....	4
Objectif du Projet.....	4
2. Analyse des Besoins.....	5
Détection et Extraction des Emails Suspects.....	5
Analyse et Classification des Emails.....	5
Notification et Suivi.....	5
3. Conception du Workflow.....	6
1. Récupération des Emails avec Gmail API.....	6
2. Prétraitement des Emails avec un Script Python.....	6
3. Analyse des Menaces avec un Modèle LLM et Cortex.....	7
a) Analyse du Contenu Textuel (LLM).....	7
b) Vérification des Indicateurs de Compromission (IOC) avec Cortex.....	7
4. Classification des Risques.....	7
5. Notification sur Discord.....	8
6. Archivage et Marquage des Emails.....	8
4. Mise en Œuvre.....	8
Implémentation Technique.....	8
Problèmes et Solutions.....	9
5. Résultats et Fonctionnement.....	10
Tests et Validation.....	10
Améliorations possibles.....	10
6. Conclusion et Perspectives.....	11
7. PARTIE 2 : implémentation d'une solution professionnelle avec TheHive, Cortex et n8n.....	11
7.1 Introduction à l'écosystème professionnel de réponse aux incidents.....	11
7.2 Objectifs et portée de cette phase avancée.....	12
7.3 Architecture et composants de la solution.....	13
7.4 Problématiques et défis opérationnels rencontrés.....	14
7.4.1 Complexité de l'installation et dépendances système.....	14
7.4.2 Exigences matérielles substantielles.....	14
7.4.3 Courbe d'apprentissage et documentation lacunaire.....	15
7.5 Workflow spécifique pour le phishing.....	15

7.5.1 Workflow très avancé théorique pour réponse à incident : liste.....	15
7.5.2 Workflow très avancé **théorique** pour réponse à incident : schéma.....	20
7.5.3 Workflow de découverte pour l'évaluation des fonctionnalités principales.....	26
7.5.3.1 Architecture simplifiée pour l'évaluation des outils.....	26
7.5.3.2 Processus détaillé de traitement : liste.....	26
7.5.3.3 Processus détaillé de traitement : schéma.....	28
7.5.3.4 Objectifs pédagogiques de cette implémentation.....	29
7.6 Installation et configuration des outils.....	29
7.6.1 Installation thehive.....	29
7.6.1.1 script d'installation automatique.....	29
7.6.1.2 Configurer les permissions.....	29
7.6.1.3 Démarrage et vérification.....	30
7.6.1.4 Lancement de l'interface web.....	30
7.6.2 Installation cortex.....	31
7.6.2.1 Démarrage et vérification.....	32
7.6.2.2 Lancement de l'interface web.....	32
7.6.3 Interconnexion cortex et thehive.....	34
7.6.3.1 Ajouter un serveur cortex.....	34
7.6.4 Déblocage des fonctionnalités thehive "create case".....	35
7.6.4.1 créer un nouveau compte sur thehive.....	36
7.6.5 Interconnecter des analyseurs dans cortex.....	38
7.6.5.1 créer un nouveau compte sur cortex.....	38
7.6.5.2 Ajouter des analyseurs: virus total.....	39
7.6.5.3 Vérifiez l'intégration de virustotal sur cortex:.....	42
7.6.6 Installer n8n localement avec docker.....	43
7.6.7 Ajouter des connecteurs et déclencheurs dans n8n.....	44
7.7 Orchestration complète.....	51
7.7.1 Bloc de traitement initial : une branche qui sépare les pièces jointes, du contenu.....	51
7.7.2 Bloc de traitement cortex : analyse de chaque pièce jointe via cortex (et virus total).....	52
7.7.3 Bloc de traitement LLM IA : la branche qui analyse du contenu textuel pour verdict, phishing ou non.....	53
7.7.4 Bloc de regroupement des informations décisionnelles :.....	53
une zone qui décide si oui ou non il y a action. Si rien de suspect, aucune action....	53
7.7.5 Bloc d'actions:.....	54
7.8 Conclusion.....	61
7.9 Axes d'amélioration pour une seconde phase.....	61

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 issu 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

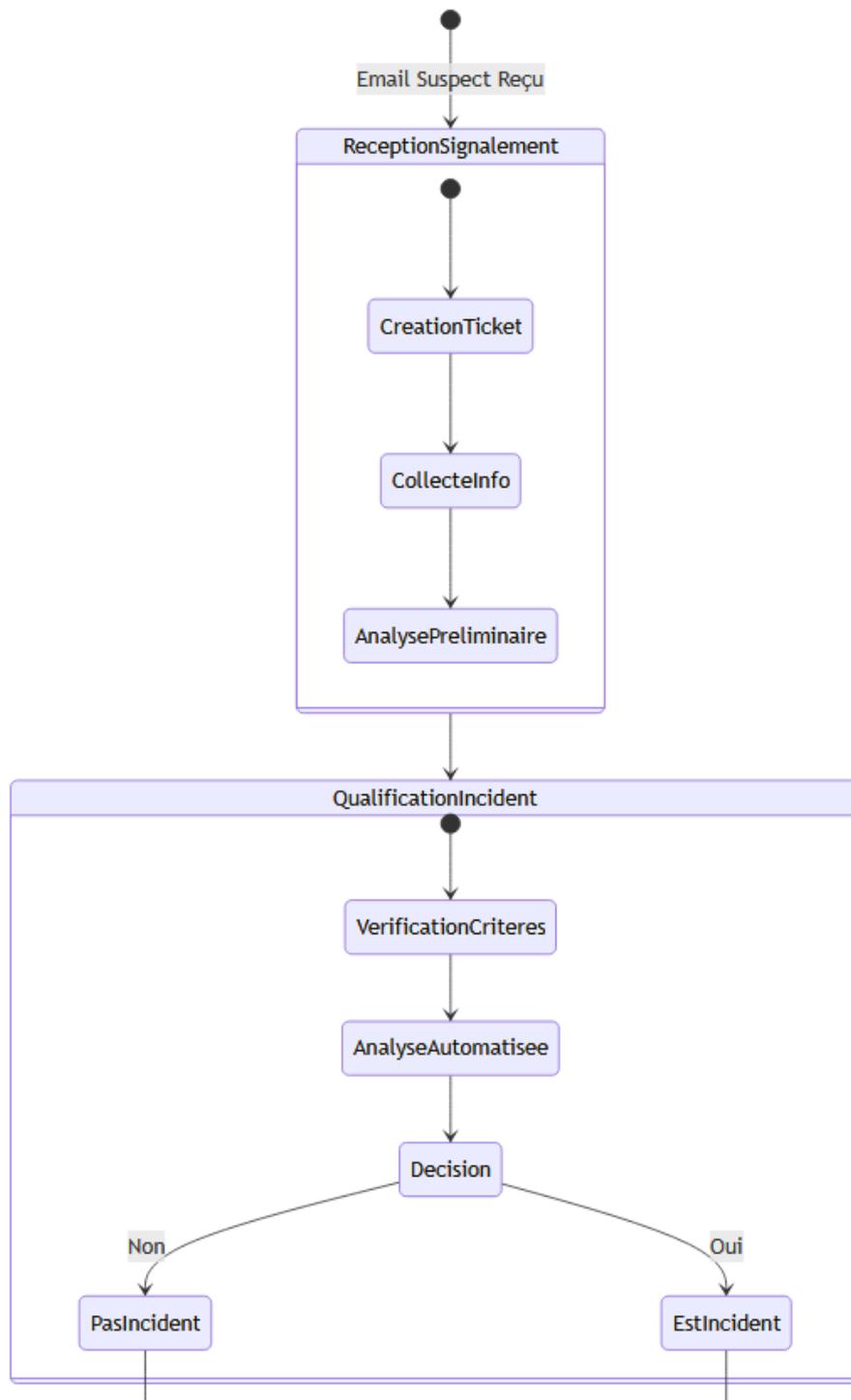
C. Actions d'amélioration

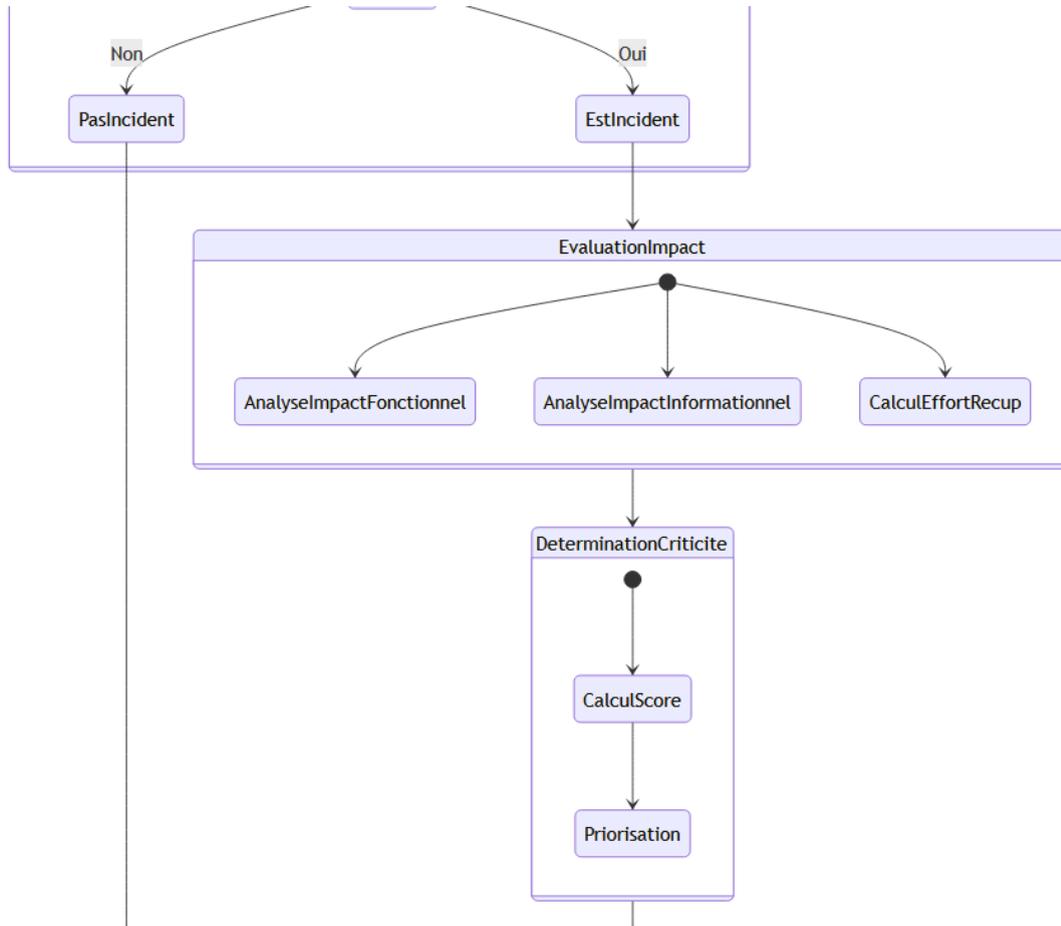
- Mise à jour des procédures
- Renforcement des contrôles
- Adaptation des formations
- Évolution des outils

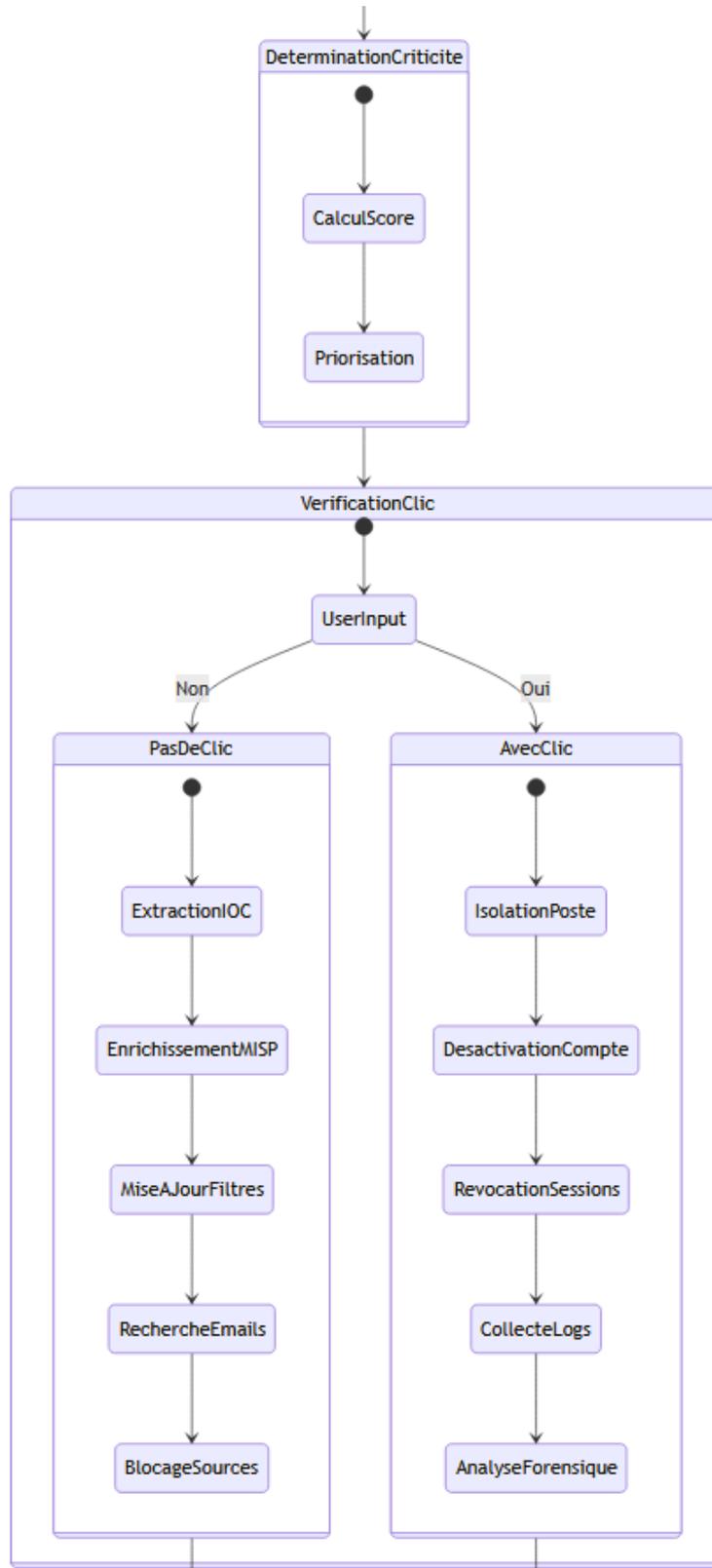
7.5.2 Workflow très avancé *théorique*** pour réponse à incident : schéma**

→ Pour voir le schéma au complet en ligne cliquez ici : [Voir le schéma](#).

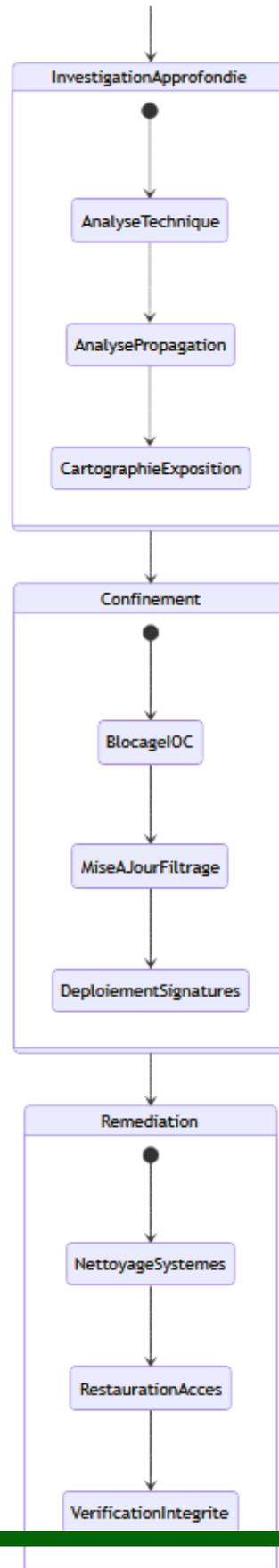
Nous avons tenté de recoller les différentes pièces du schéma, mais comme il est un long, il est plus facile d'aller voir sur le lien donné ci haut (ceci n'est pas un phishing).

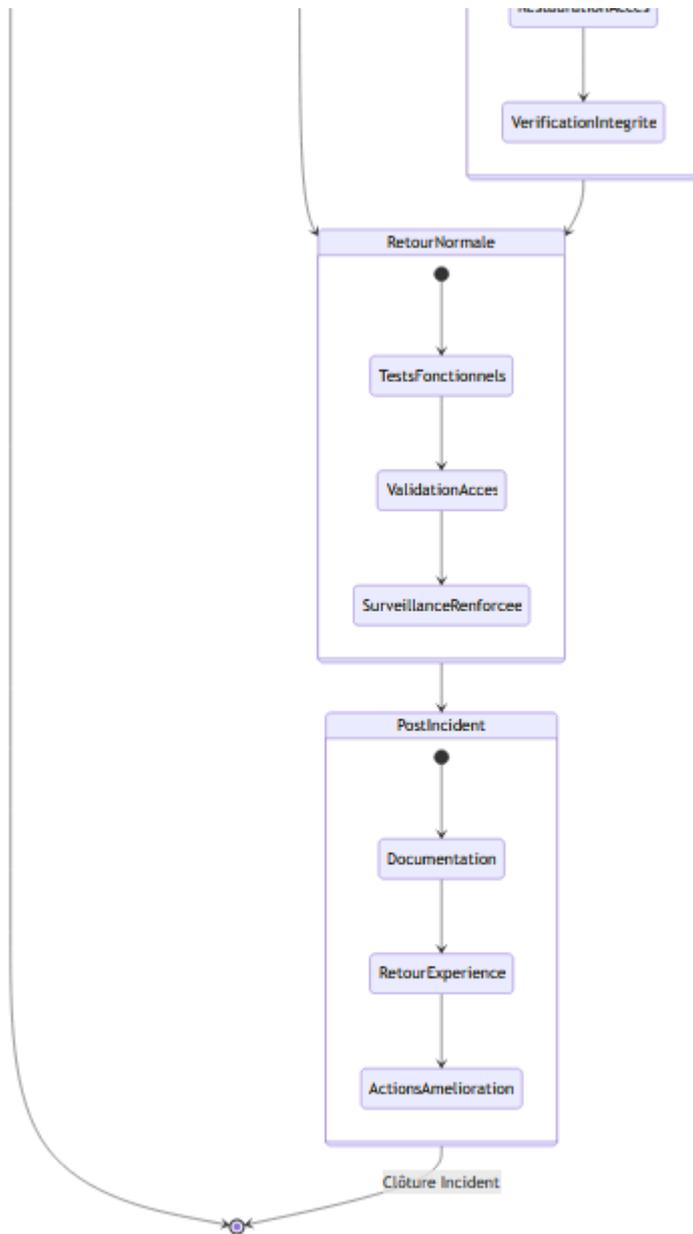






Documentation et Clôture





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

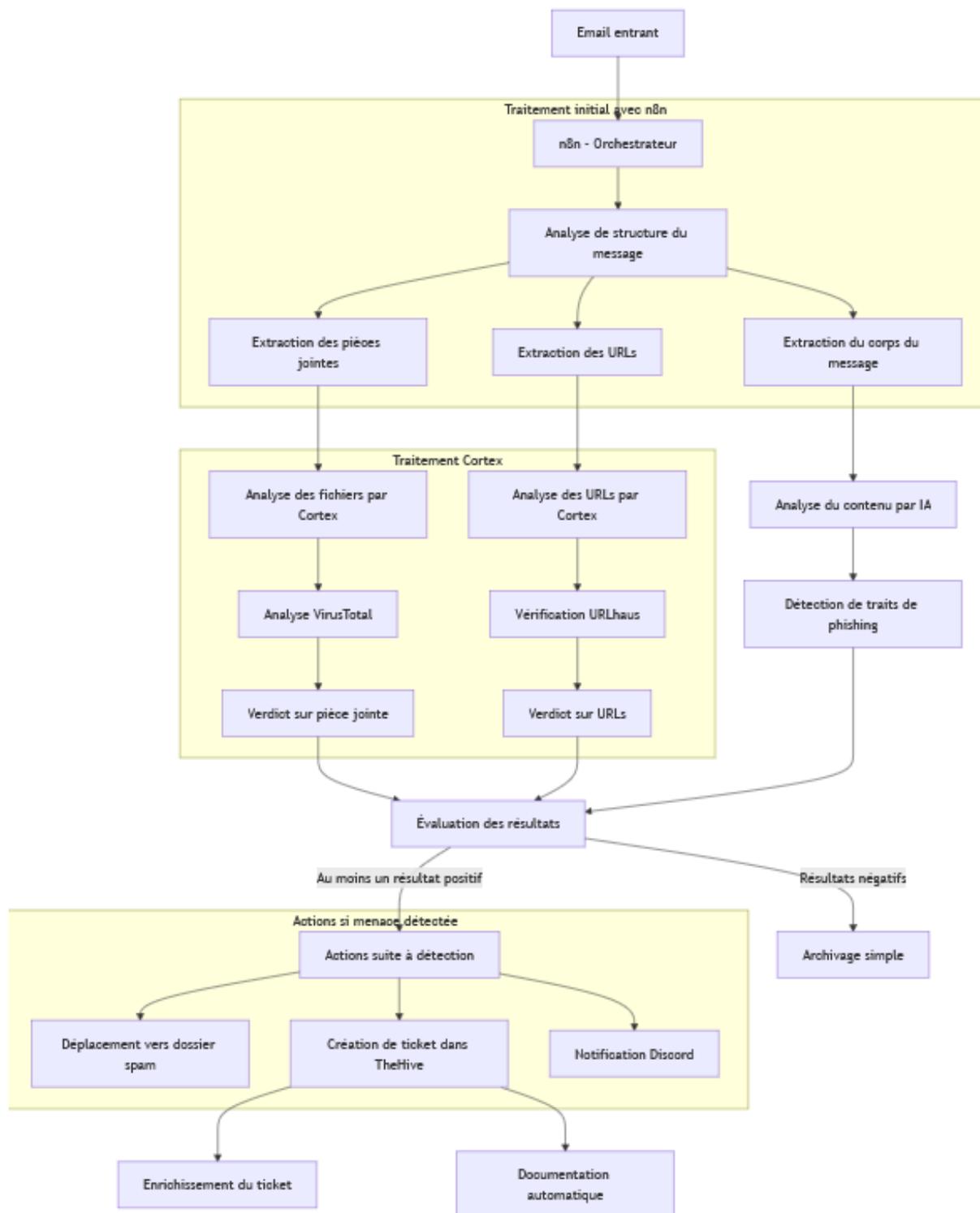
- Analyse du corps du message pour détecter des caractéristiques de phishing
- Identification des techniques de manipulation psychologique
- Production d'un rapport de raisonnement détaillé
- Transmission d'une conclusion binaire (phishing/légitime) pour prise de décision

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 ikb@ikb-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

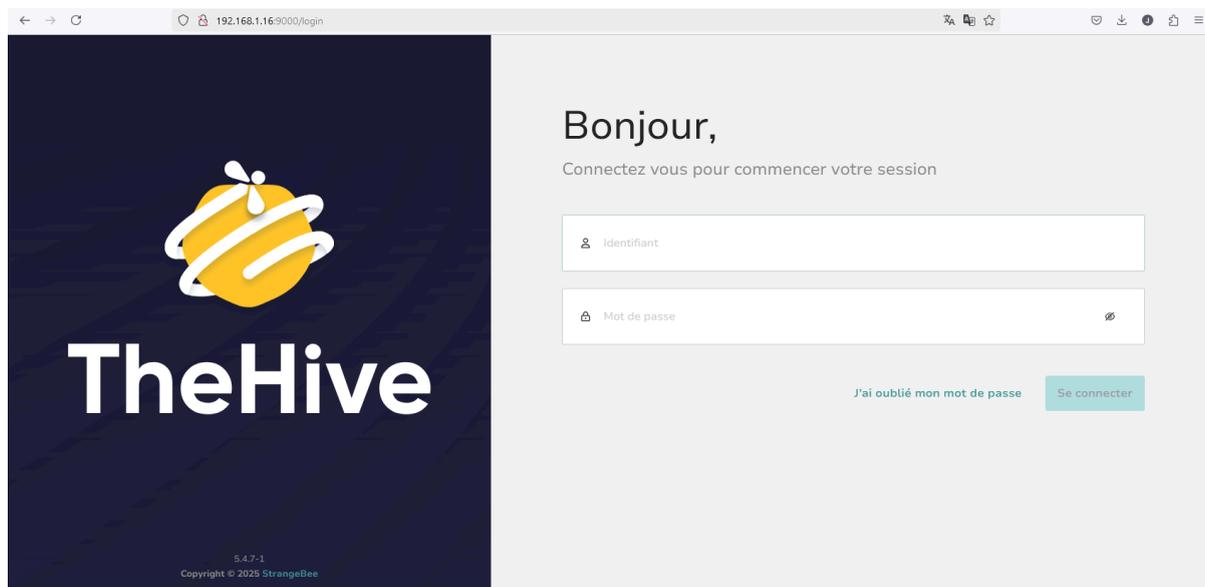
```
thehive@thehive:~$ sudo systemctl status thehive
• thehive.service - Scalable, Open Source and Free Security Incident Response Solutions
  Loaded: loaded (/lib/systemd/system/thehive.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2025-02-05 05:04:13 UTC; 2h 19min ago
  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
```

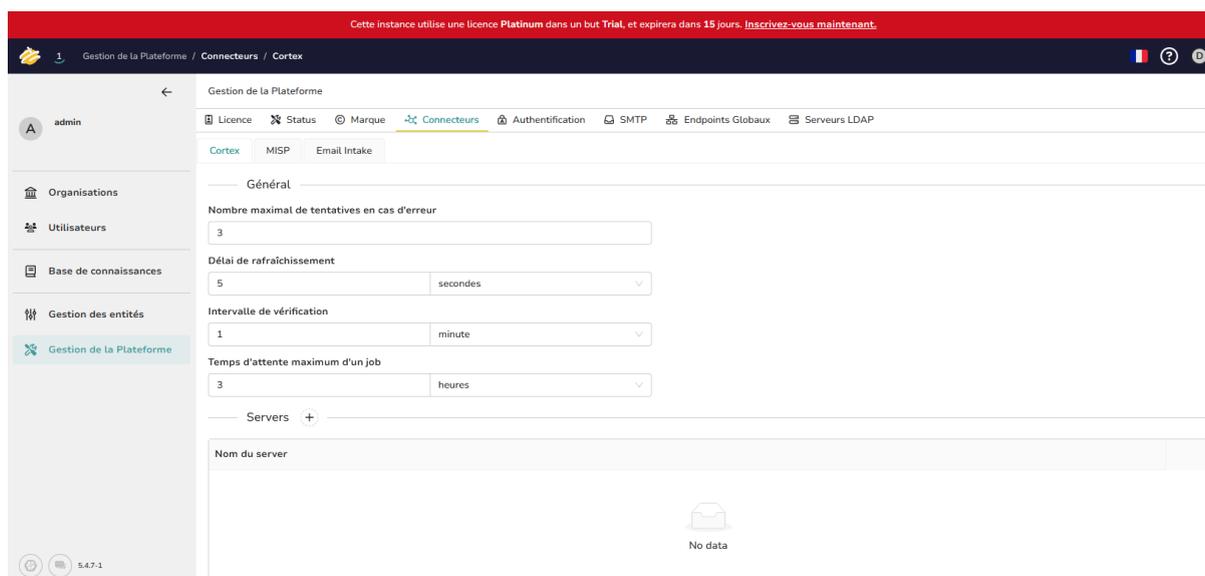
```
thehive@thehive:~$ sudo systemctl status elasticsearch.service
• elasticsearch.service - Elasticsearch
  Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2025-02-05 05:03:50 UTC; 2h 20min ago
  Docs: https://www.elastic.co
  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-m1/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](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
```

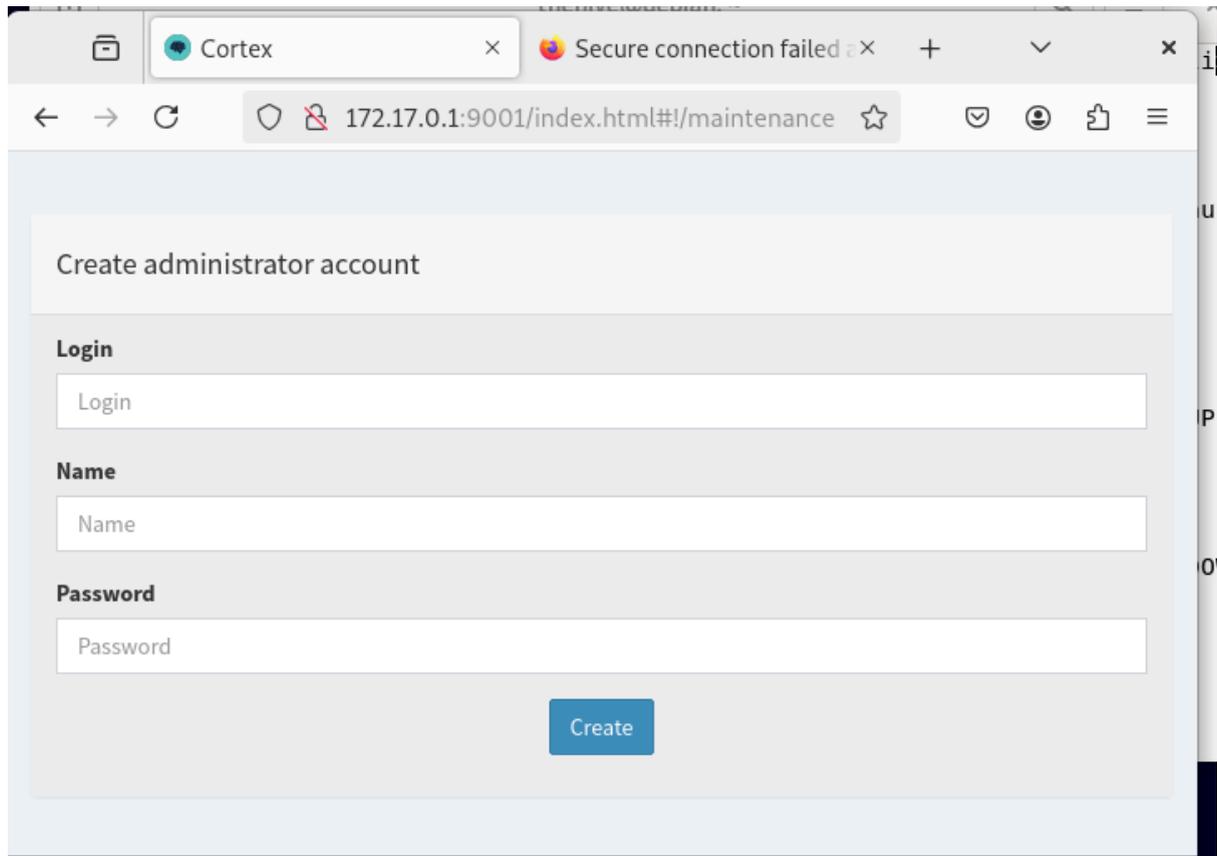
```
sudo systemctl enable cortex.service
```

```
sudo systemctl status cortex.service
```

```
thehive@debian:~$ sudo systemctl status cortex.service
● cortex.service - cortex
   Loaded: loaded (/etc/systemd/system/cortex.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-02-19 13:12:37 CET; 1min 1s ago
     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
```

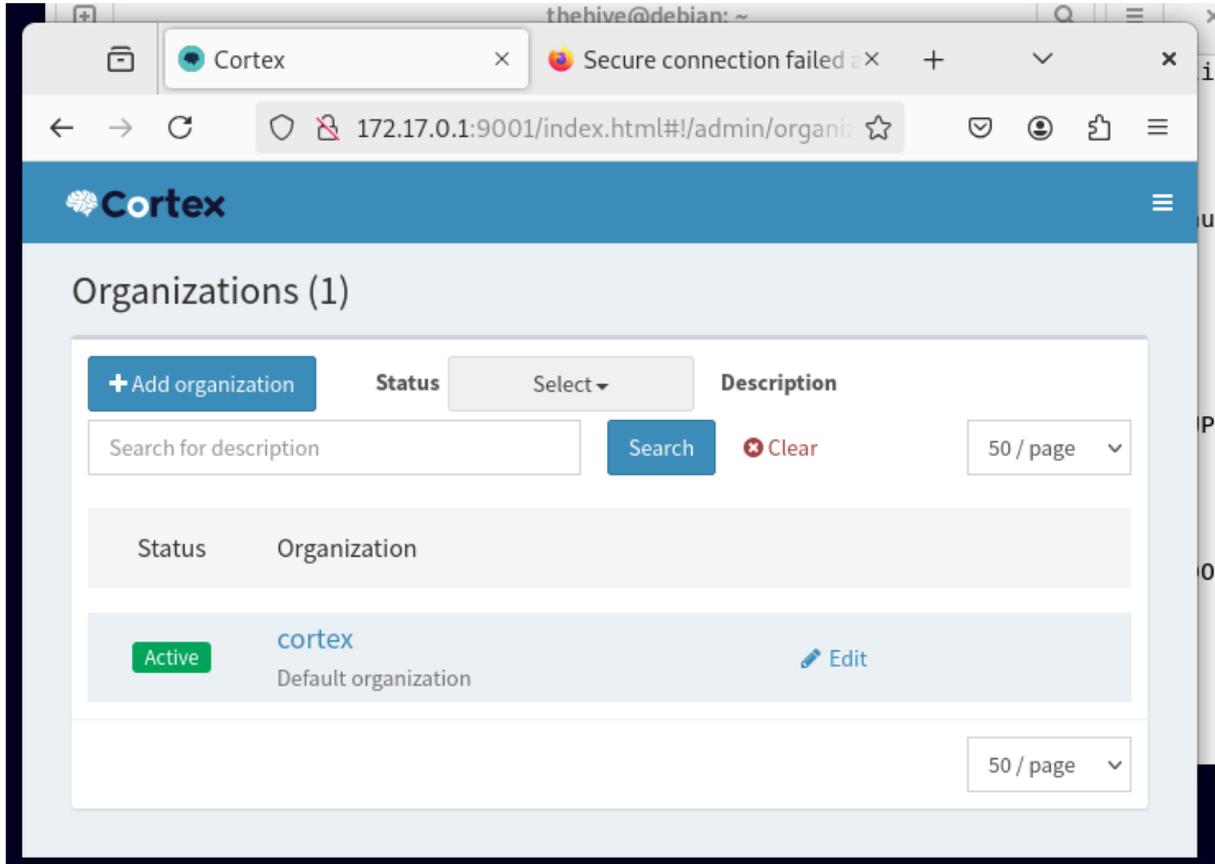
7.6.2.2 Lancement de l'interface web

```
http://IP\_ADDRESS:9001
```



Créer un premier utilisateur admin

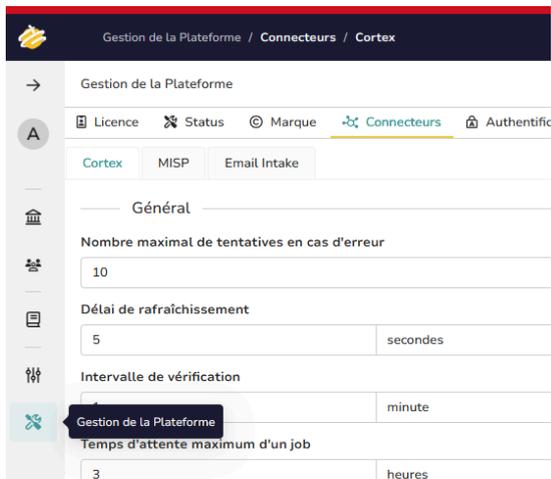
- user : admin
- name: jacob
- pwd: XXXXXXXXXX



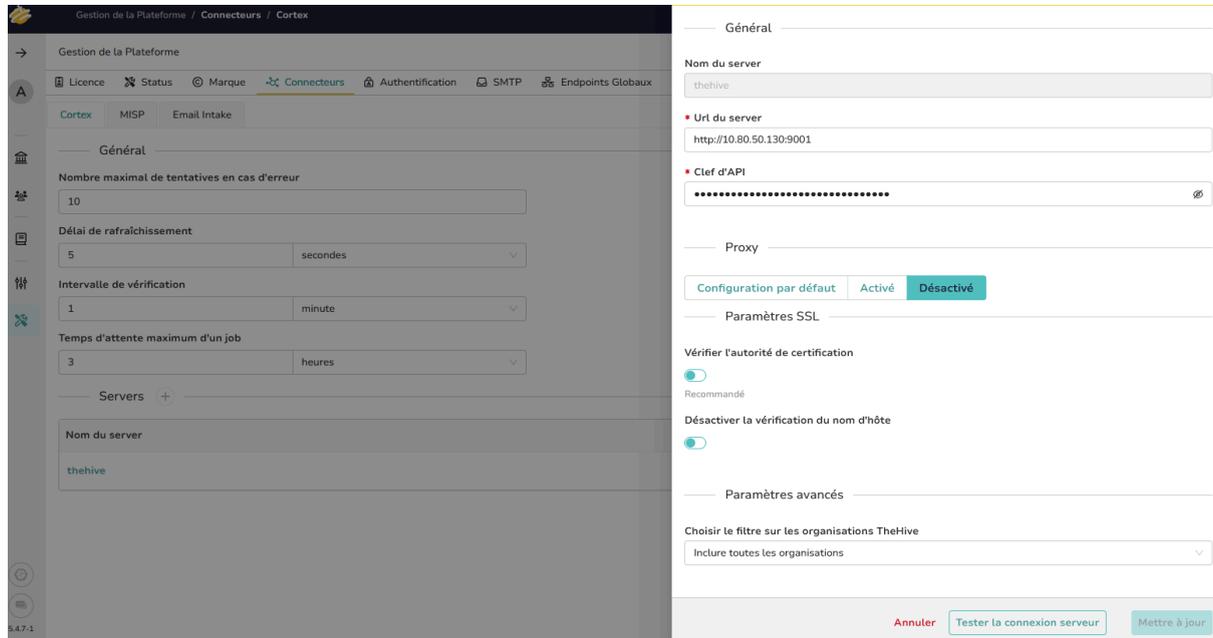
7.6.3 Interconnexion cortex et thehive

7.6.3.1 Ajouter un serveur cortex

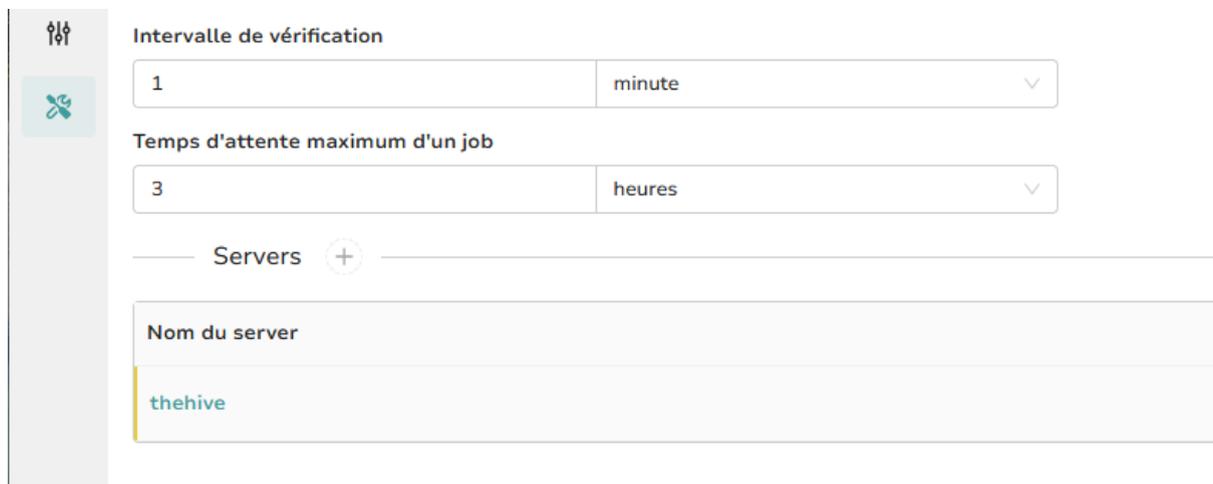
Dans le compte admin rendez vous dans le menu à gauche gestion de la plateforme



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.



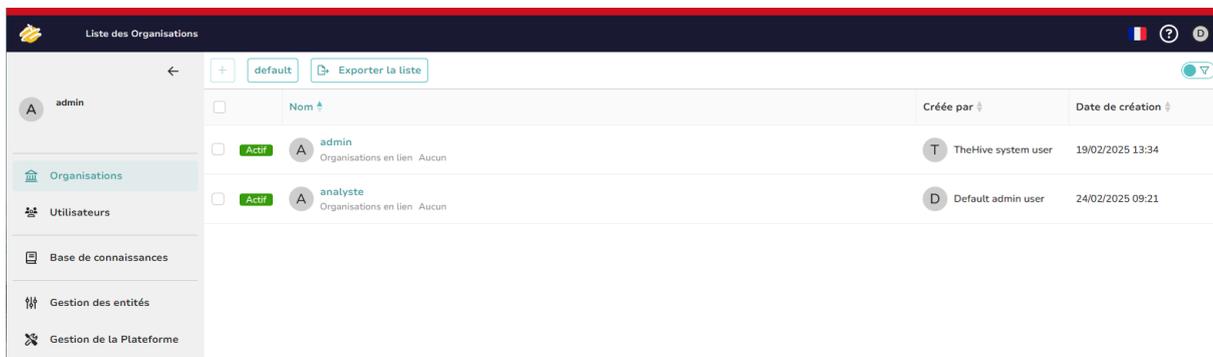
7.6.4 Déblocage des fonctionnalités thehive "create case"

ATTENTION !

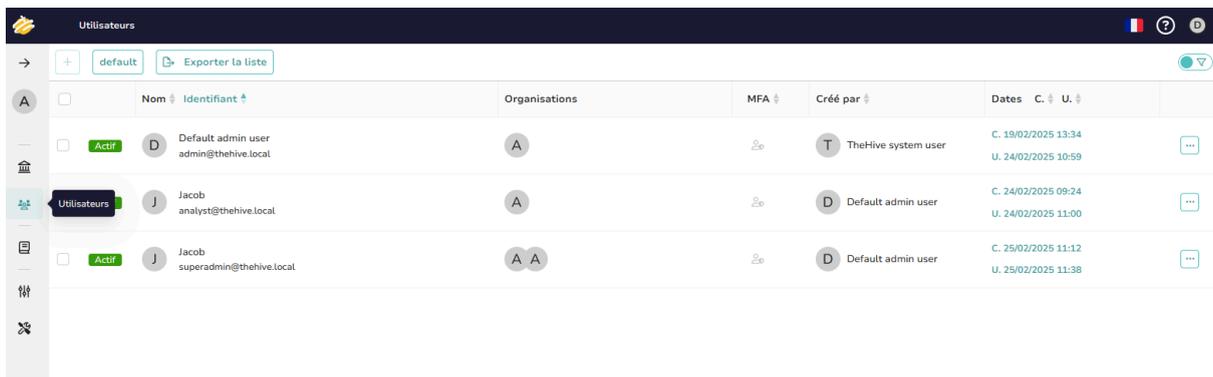
C'est la partie qui m'a semblé le moins bien expliquée dans la documentation officielle. En effet, pour pouvoir accéder au menu afin d'interconnecter les outils ou encore créer des case avec thehive il faut tout d'abord créer des comptes supplémentaires sur chaque plateforme. Les comptes admin n'ont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



	Nom ↑	Créé par ↓	Date de création ↓
<input type="checkbox"/>	admin Organisations en lien Aucun	TheHive system user	19/02/2025 13:34
<input type="checkbox"/>	analyste Organisations en lien Aucun	Default admin user	24/02/2025 09:21



	Nom ↓	Identifiant ↑	Organisations	MFA ↓	Créé par ↓	Dates C. ↓ U. ↓
<input type="checkbox"/>	Default admin user	admin@thehive.local	A	2e	TheHive system user	C. 19/02/2025 13:34 U. 24/02/2025 10:59
<input checked="" type="checkbox"/>	Jacob	analyst@thehive.local	A	2e	Default admin user	C. 24/02/2025 09:24 U. 24/02/2025 11:00
<input type="checkbox"/>	Jacob	superadmin@thehive.local	A A	2e	Default admin user	C. 25/02/2025 11:12 U. 25/02/2025 11:38

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

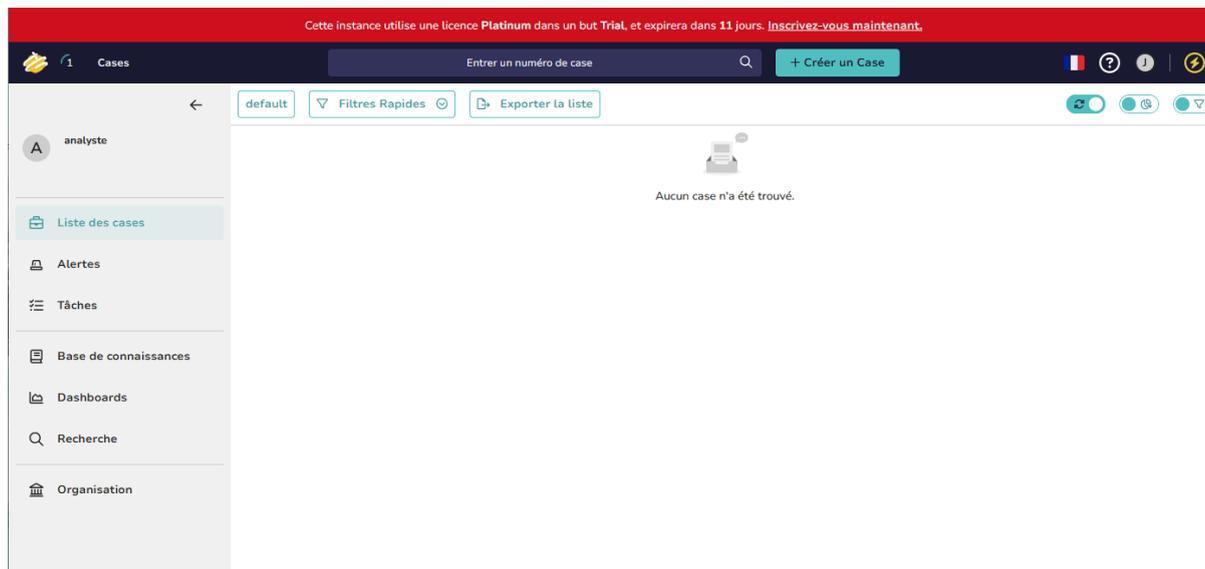
•••••

[J'ai oublié mon mot de passe](#)

[Se connecter](#)

7.6.4.2 créer un case dans thehive

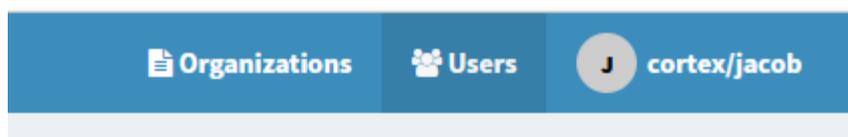
A présent vous verrez apparaître créer un case, qui n'était pas disponible précédemment. Grâce à cela nous pourrons continuer l'automatisation.

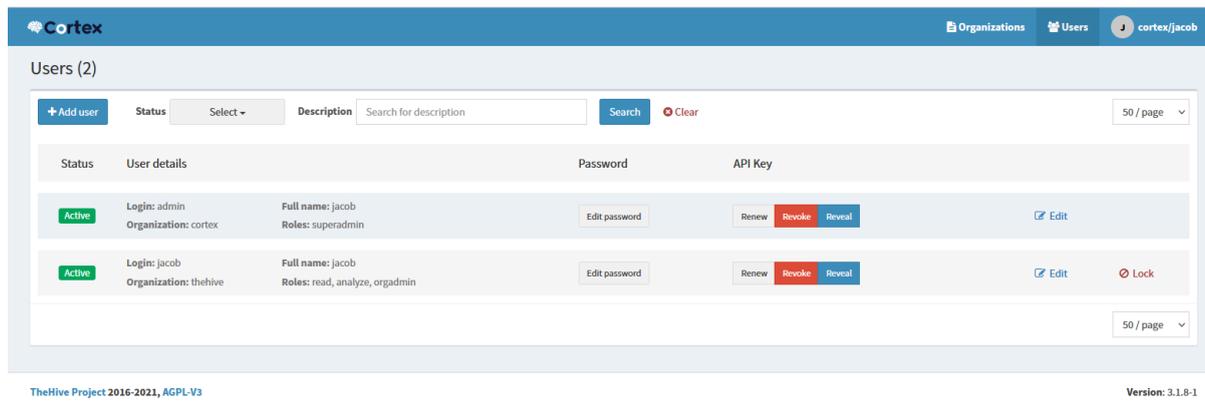


7.6.5 Interconnecter des analyseurs dans cortex

7.6.5.1 créer un nouveau compte sur cortex

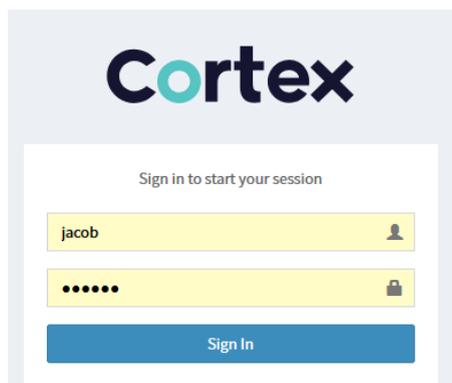
Vous devez créer un compte supplémentaire en plus de l'administrateur et avec des droits différents afin de débloquent cette fonctionnalité. Cliquez sur user en haut à droite de l'interface cortex, puis ajoutez un utilisateur avec les droits d'analyse, lecture et organisation.





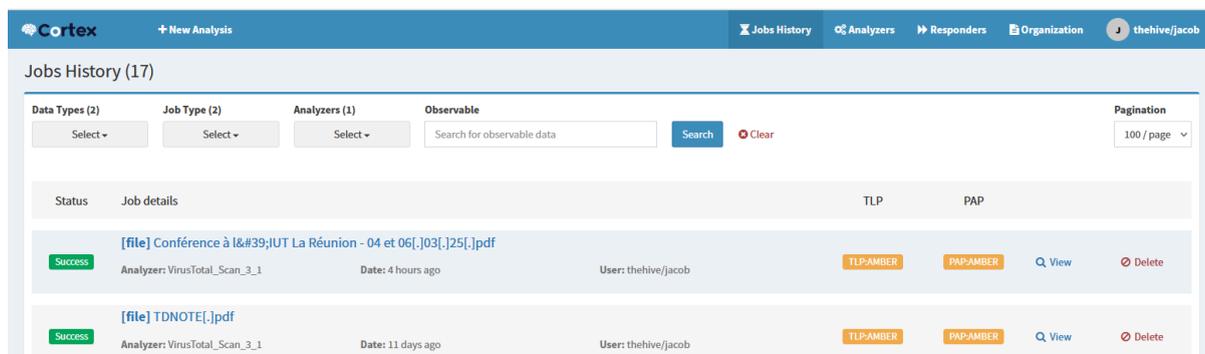
The screenshot shows the Cortex 'Users' management page. At the top, there are navigation tabs for 'Organizations' and 'Users', and a user profile for 'cortex/jacob'. Below the header, the page title is 'Users (2)'. There are filters for '+ Add user', 'Status', and 'Description'. A search bar is present with a 'Search' button and a 'Clear' button. The main content is a table with columns for 'Status', 'User details', 'Password', and 'API Key'. Two users are listed: 'admin' (roles: superadmin) and 'jacob' (roles: read, analyze, orgadmin). Each user row has buttons for 'Edit password', 'Renew', 'Revoke', 'Reveal', and 'Edit'. A 'Lock' button is also visible for the 'jacob' user. At the bottom, there is a footer with 'TheHive Project 2016-2021, AGPL-V3' and 'Version: 3.1.8-1'.

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



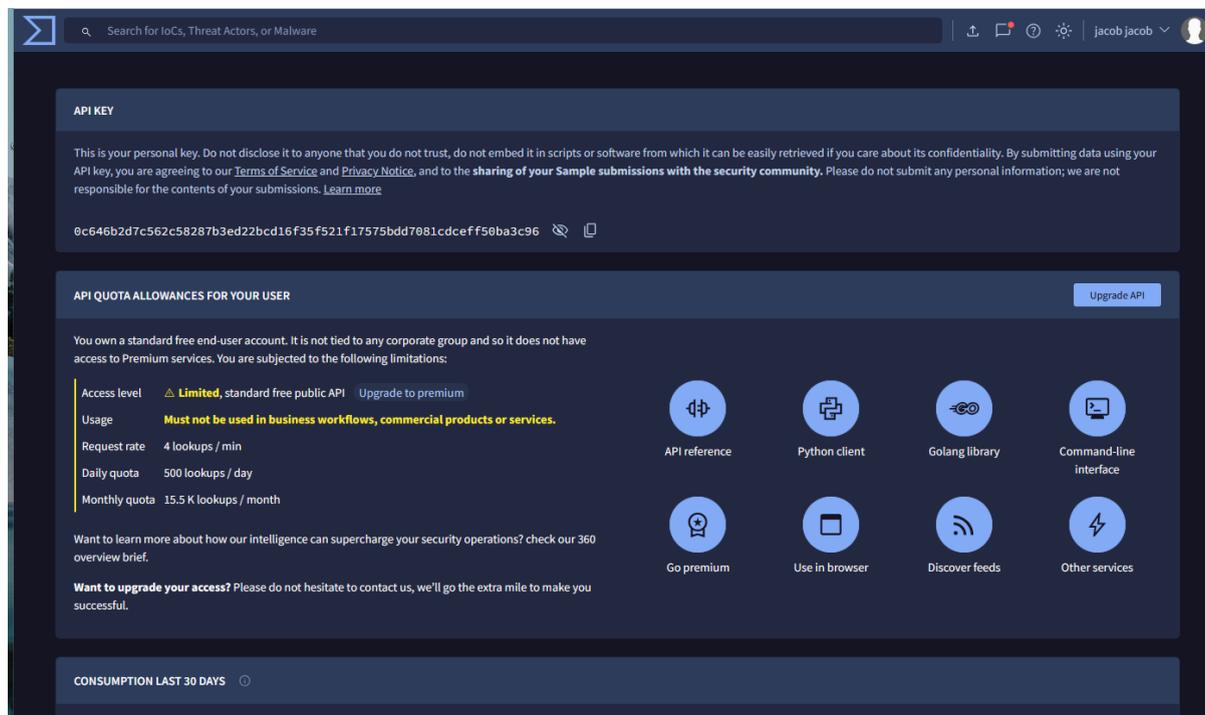
7.6.5.2 Ajouter des analyseurs: virus total

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



The screenshot shows the Cortex 'Jobs History' page. At the top, there are navigation tabs for '+ New Analysis', 'Jobs History', 'Analyzers', 'Responders', and 'Organization', and a user profile for 'thehive/jacob'. Below the header, the page title is 'Jobs History (17)'. There are filters for 'Data Types (2)', 'Job Type (2)', and 'Analyzers (1)'. A search bar is present with a 'Search' button and a 'Clear' button. The main content is a table with columns for 'Status', 'Job details', 'TLP', and 'PAP'. Two jobs are listed, both with a status of 'Success'. Each job entry includes the file name, analyzer used, date, user, and buttons for 'View' and 'Delete'. At the bottom, there is a footer with 'TheHive Project 2016-2021, AGPL-V3' and 'Version: 3.1.8-1'.

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



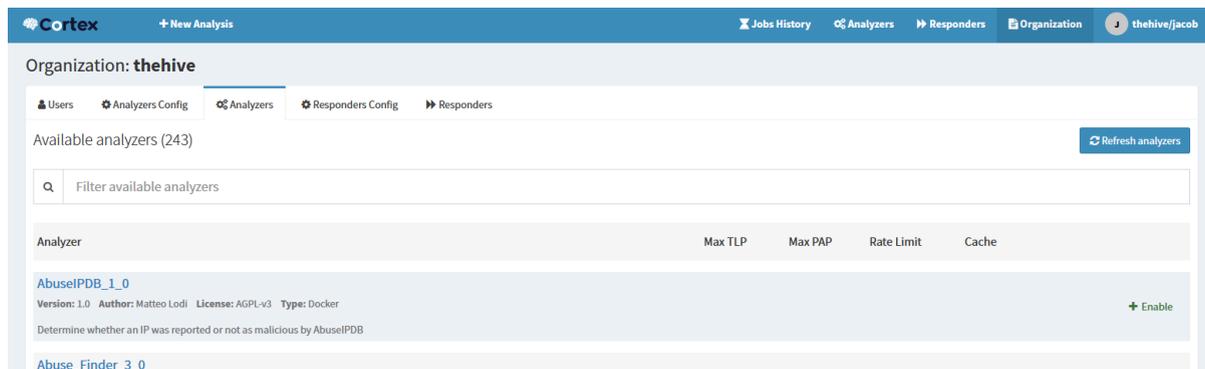
The screenshot shows the VirusTotal API Key management interface. At the top, there is a search bar for IoCs, Threat Actors, or Malware. Below it, the 'API KEY' section displays a personal key: `0c646b2d7c562c58287b3ed22bcd16f35f521f17575bdd7081cdceff50ba3c96`. A warning message states: "This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submissions with the security community. Please do not submit any personal information; we are not responsible for the contents of your submissions. Learn more".

The 'API QUOTA ALLOWANCES FOR YOUR USER' section indicates a standard free end-user account with the following limitations:

- Access level: **Limited**, standard free public API. Upgrade to premium.
- Usage: **Must not be used in business workflows, commercial products or services.**
- Request rate: 4 lookups / min
- Daily quota: 500 lookups / day
- Monthly quota: 15.5 K lookups / month

Below the quotas, there are icons for various integration methods: API reference, Python client, Golang library, Command-line interface, Go premium, Use in browser, Discover feeds, and Other services. A 'Go premium' button is also visible. At the bottom, there is a 'CONSUMPTION LAST 30 DAYS' section.

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.



The screenshot shows the Cortex web interface for the 'thehive' organization. The top navigation bar includes '+ New Analysis', 'Jobs History', 'Analyzers', 'Responders', 'Organization', and a user profile 'thehive/jacob'. The main content area is titled 'Organization: thehive' and contains a breadcrumb trail: 'Users > Analyzers Config > Analyzers > Responders Config > Responders'. Below this, there is a section for 'Available analyzers (243)' with a search filter and a 'Refresh analyzers' button.

Analyzer	Max TLP	Max PAP	Rate Limit	Cache
AbuseIPDB_1_0				
Version: 1.0 Author: Matteo Lodi License: AGPL-v3 Type: Docker + Enable				
Determine whether an IP was reported or not as malicious by AbuseIPDB				
Abuse_Finder_3_0				

Analyzer	Max TLP	Max PAP	Rate Limit	Cache
AbuseIPDB_1_0 Version: 1.0 Author: Matteo Lodi License: AGPL-V3 Type: Docker + Enable Determine whether an IP was reported or not as malicious by AbuseIPDB				
Abuse_Finder_3_0 Version: 3.0 Author: CERT-BDF License: AGPL-V3 Type: Docker + Enable Find abuse contacts associated with domain names, URLs, IPs and email addresses.				
AnyRun_Sandbox_Analysis_1_1 Version: 1.1 Author: Andrea Garavaglia, Davide Arcuri, LDO-CERT; Nate Olsen, WSECU License: AGPL-V3 Type: Docker + Enable Any.Run Sandbox file analysis				
Autofocus_GetSampleAnalysis_1_0 Version: 1.0 Author: ANSSI License: AGPL-V3 Type: Docker + Enable Get full analysis from a sample based on its hash				
Autofocus_SearchIOC_1_0 Version: 1.0 Author: ANSSI License: AGPL-V3 Type: Docker + Enable Search samples in Autofocus based on a single IOC				
Autofocus_SearchJSON_1_0 Version: 1.0 Author: ANSSI License: AGPL-V3 Type: Docker + Enable Search samples in Autofocus with a full search query in JSON				

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

Edit configuration: VirusTotal

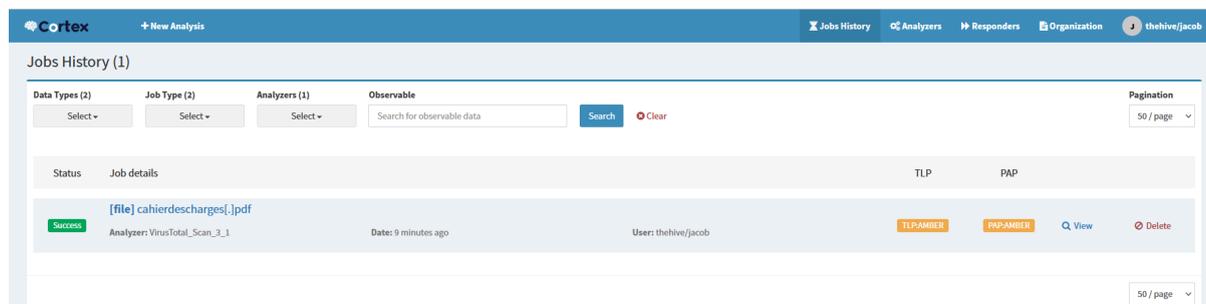
key	<input type="text" value="0c646b2d7c562c58287b3ed22bcd16f35f521f17575bdd7081cdceff50ba3c96"/>
	API key for Virustotal
polling_interval	<input type="text" value="60"/> ⌵
	Define time interval between two requests attempts for the report
highlighted_antivirus	<input type="text" value="1."/> Add option ✕
	Add taxonomy if selected AV don't recognize observable
rescan_hash_older_than_days	<input type="text" value="30"/> ⌵
	Rescan hash observable if report is older than selected days
download_sample	<input type="checkbox"/> True <input checked="" type="checkbox"/> False
	Download automatically sample as observable when looking for hash
download_sample_if_highlighted	<input type="checkbox"/> True <input checked="" type="checkbox"/> False
	Download automatically sample as observable if highlighted antivirus didn't recognize

Cancel
Save

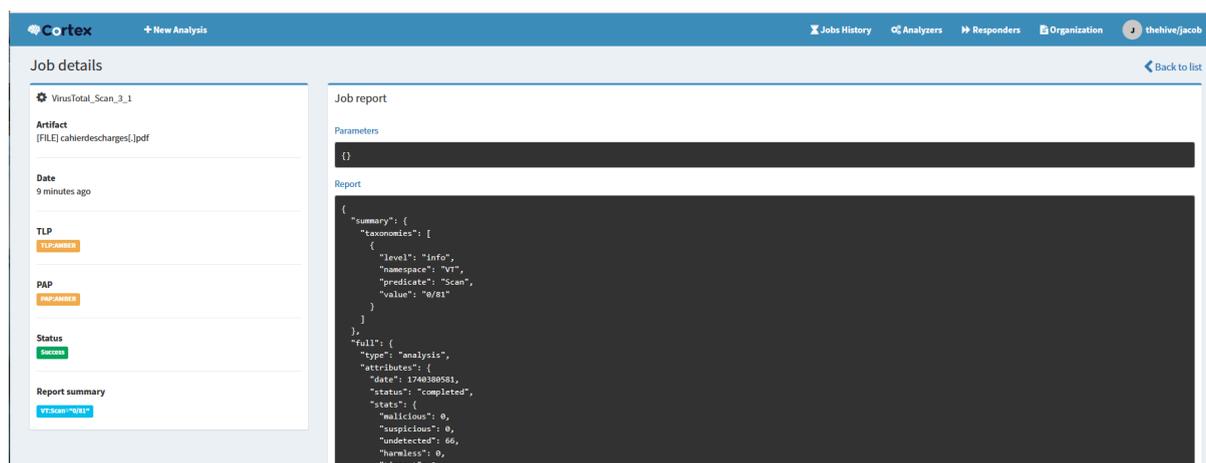
7.6.5.3 Vérifiez l'intégration de virustotal sur cortex:

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
```

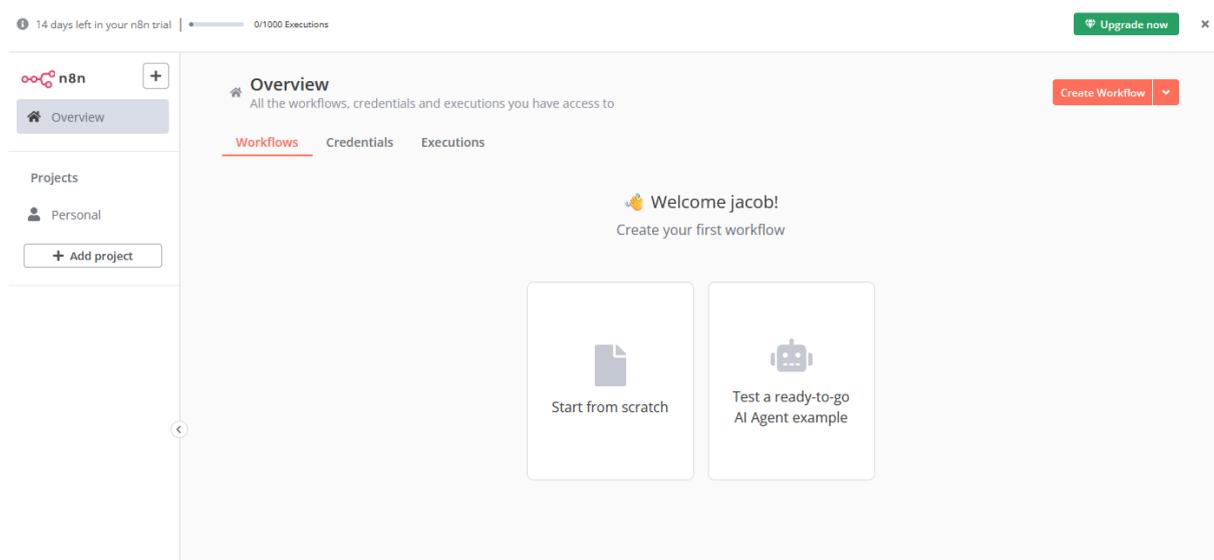
```
n8n_data:/home/node/.n8n docker.n8n.io/n8nio/n8n
```

```
Received 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
Permissions 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.
Server settings loaded from: /home/node/.n8n/config
Initializing n8n process
n8n ready on 0.0.0.0, port 5678
Version: 1.79.3

Editor is now accessible via:
http://localhost:5678/

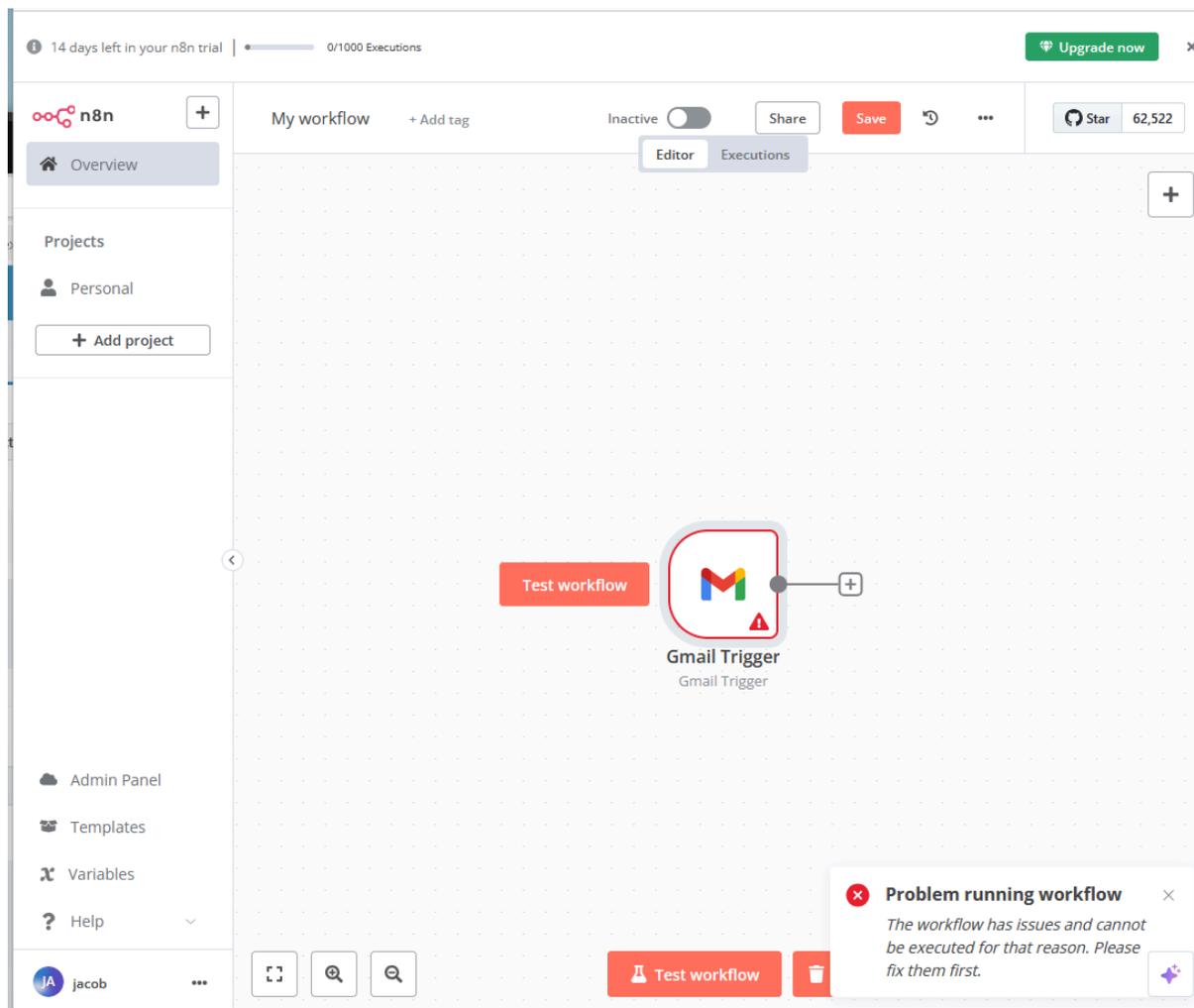
Press "o" to open in Browser.
Banner was set up successfully
Server survey updated successfully
```

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

What happens next?

- Advanced AI**
Build autonomous agents, summarize or search documents, etc. →
- Action in an app**
Do something in an app or service like Google Sheets, Telegram or Notion →
- Data transformation**
Manipulate, filter or convert data →
- Flow**
Branch, merge or loop the flow, etc. →
- Core**
Run code, make HTTP requests, set webhooks, etc. →
- Human in the loop**
Wait for approval or human input before continuing →

- Add another trigger**
Triggers start your workflow. Workflows can have multiple triggers. →

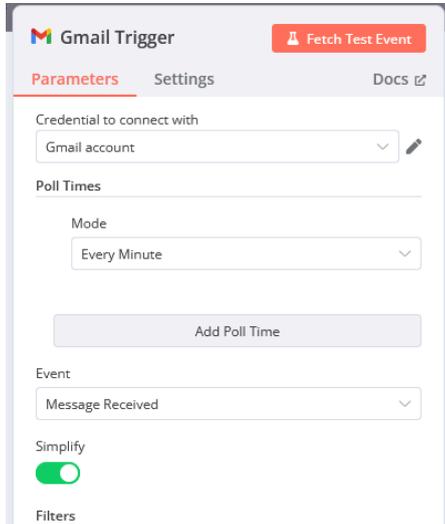
Vous pouvez ajouter votre recherche

← What triggers this workflow?

A trigger is a step that starts your workflow

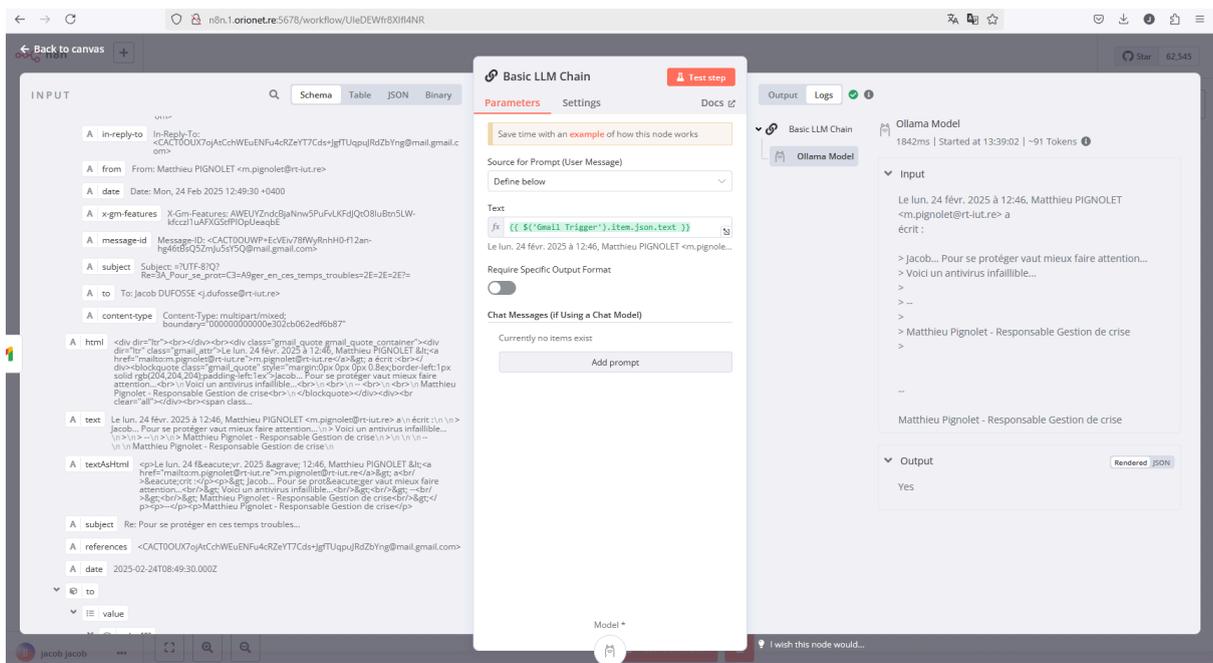
- Gmail** →
- Figma (Beta)** →
- Gumroad Trigger** ⚡
- Google Cloud Realtime Database** →
- Email Trigger (IMAP)** ⚡
Triggers the workflow when a new email is received

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

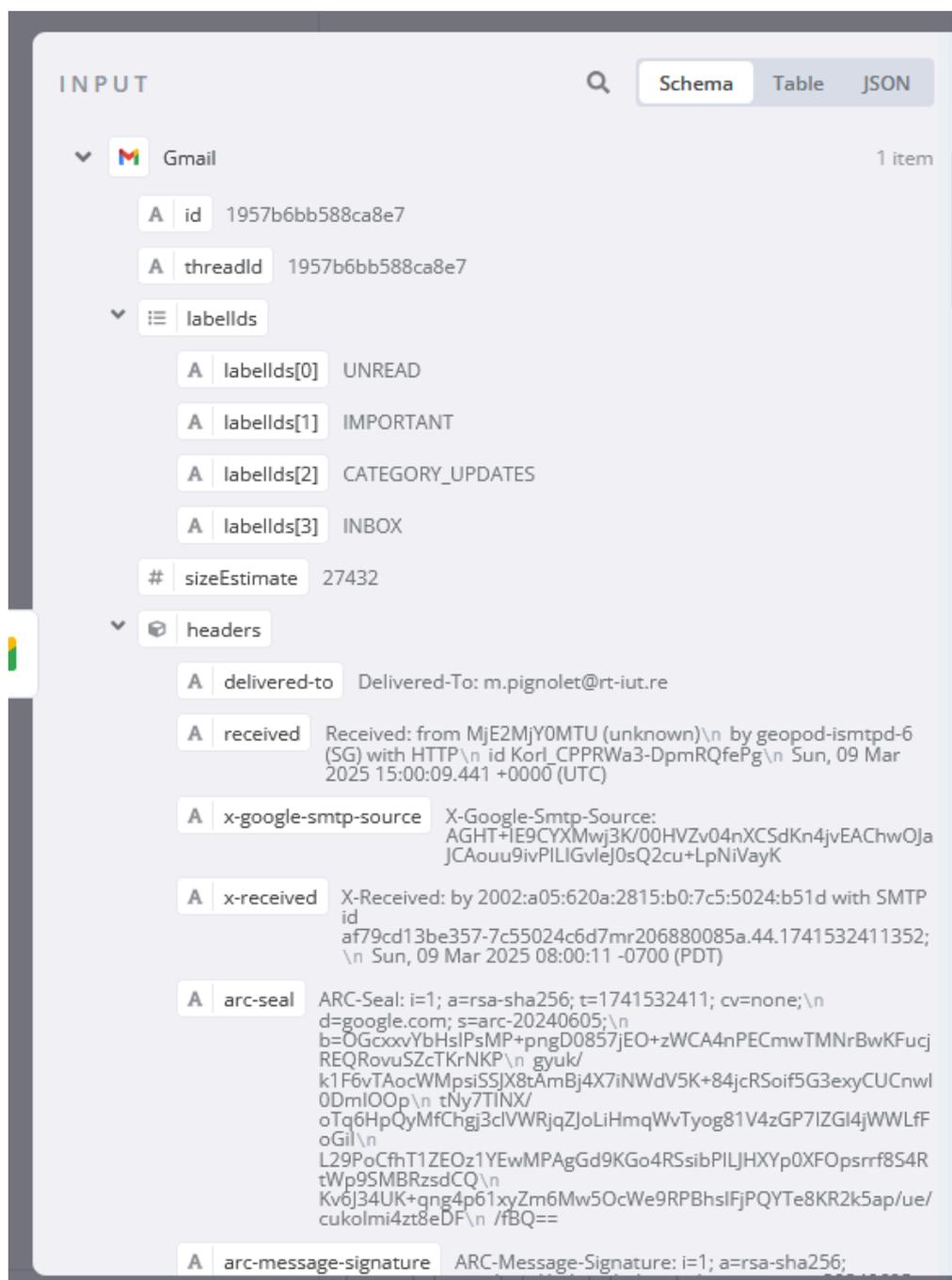


L'intérêt principal réside dans l'utilisation rapide et facile des données provenant des précédents modules. Par exemple, à la suite de la réception d'un courriel, nous pouvons immédiatement ajouter les différents éléments directement dans les champs d'un module suivant.

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



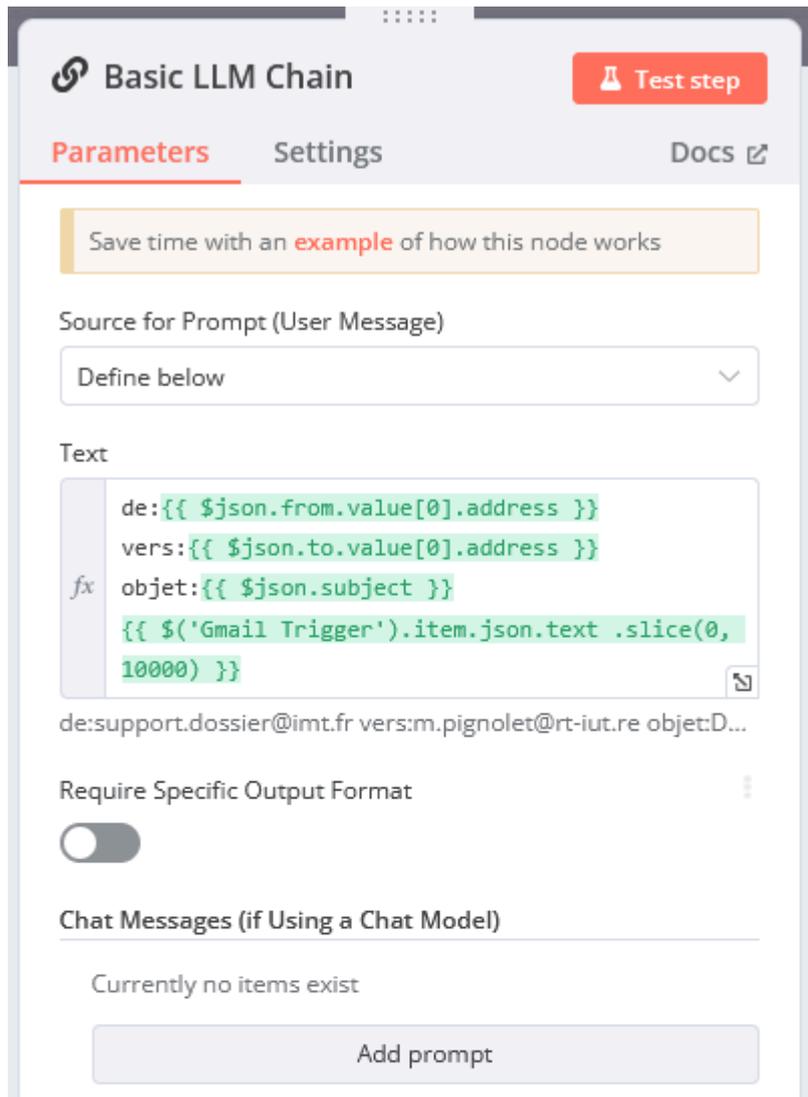
Dans la partie de gauche nous avons à disposition tous les éléments en provenance du courriel que nous pouvons glisser dans la fenêtre de configuration de notre module LLM AI. Les données sont disponibles en table, schéma et JSON format.



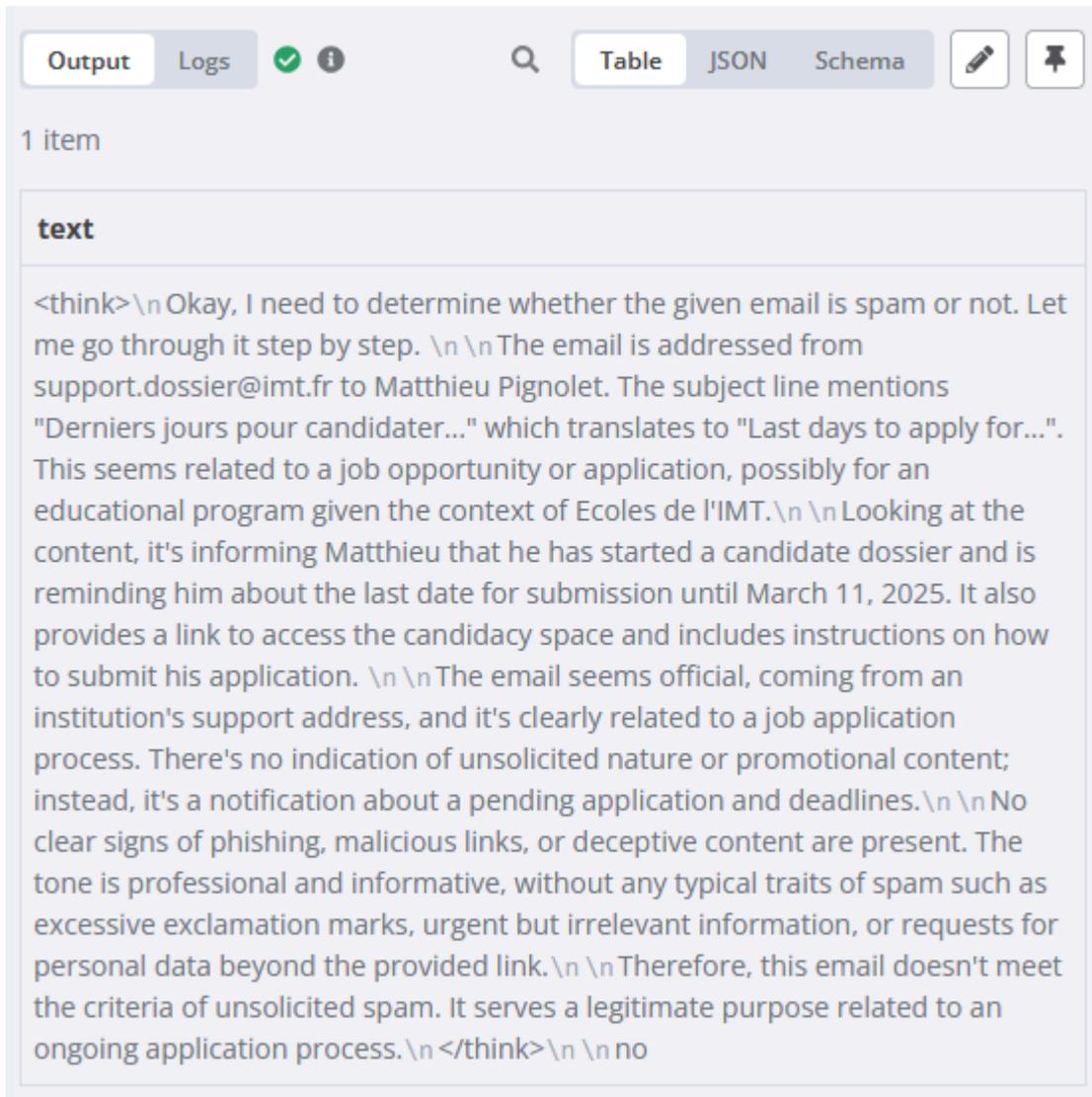
The screenshot shows an 'INPUT' section with tabs for 'Schema', 'Table', and 'JSON'. It displays a single email item from Gmail with the following fields:

- id**: 1957b6bb588ca8e7
- threadId**: 1957b6bb588ca8e7
- labelIds**:
 - labelIds[0]: UNREAD
 - labelIds[1]: IMPORTANT
 - labelIds[2]: CATEGORY_UPDATES
 - labelIds[3]: INBOX
- sizeEstimate**: 27432
- headers**:
 - delivered-to**: Delivered-To: m.pignolet@rt-iut.re
 - received**: Received: from MjE2MjY0MTU (unknown)\n by geopod-ismtpd-6 (SG) with HTTP\n id Korl_CPPRWa3-DpmRQfePg\n Sun, 09 Mar 2025 15:00:09.441 +0000 (UTC)
 - x-google-smtp-source**: X-Google-Smtp-Source: AGHT+IE9CYXMwj3K/00HVZv04nXCSdKn4jvEACHwOJa JCAouu9ivPILIGvleJ0sQ2cu+LpNiVayK
 - x-received**: X-Received: by 2002:a05:620a:2815:b0:7c5:5024:b51d with SMTP id af79cd13be357-7c55024c6d7mr206880085a.44.1741532411352;\n Sun, 09 Mar 2025 08:00:11 -0700 (PDT)
 - arc-seal**: ARC-Seal: i=1; a=rsa-sha256; t=1741532411; cv=none;\n d=google.com; s=arc-20240605;\n b=OGcxxvYbHsIPsMP+pngD0857jEO+zWCA4nPECmwTMNrBwKFucj REQROvuSZcTKrNKP\n gyuk/ k1F6vTAocWMpsiSSjX8tAmBj4X7iNWdV5K+84jcRSoif5G3exyCUCnwl 0DmIOOp\n tNy7TINX/ oTq6HpQyMfChgj3clVWRjqZJoLiHmqWvTyog81V4zGP7IZGI4jWWLF oGil\n L29PoCfhT1ZEOz1YEwMPAgGd9KGo4RSsibPILJHXYp0XFOpsrrf8S4R tWp95MBRzsdCQ\n Kv6j34UK+qng4p61xyZm6Mw5OcWe9RPBhsIFjPQYTe8KR2k5ap/ue/ cukolmi4zt8eDF\n /fBQ==
 - arc-message-signature**: ARC-Message-Signature: i=1; a=rsa-sha256;

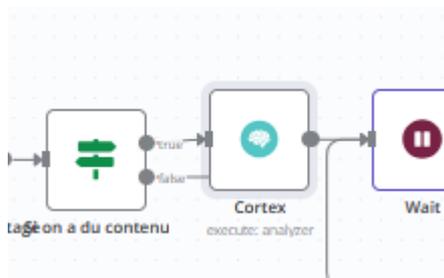
Dans la partie centrale, nous pouvons simplement les glisser dans la fenêtre et constituer par exemple l'entrant principal à analyser par notre LLM. Ici **de: , vers:....., objet:... et contenu...** Ce contenu est désormais dynamiquement rempli et à chaque nouvel email, les informations seront remplacées.



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.

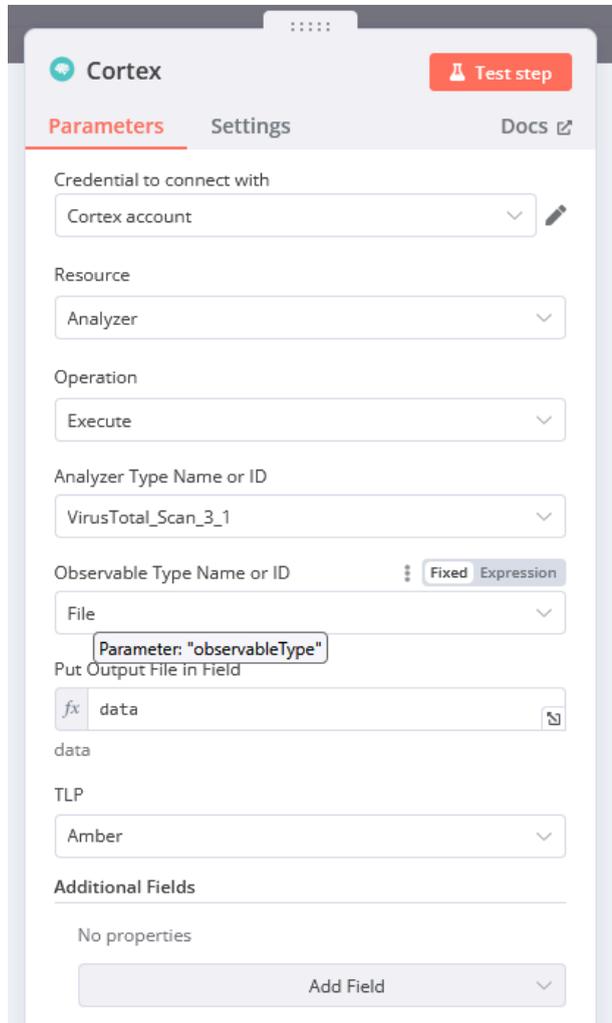


Un dernier exemple de module facile à implémenter c'est la connexion avec cortex

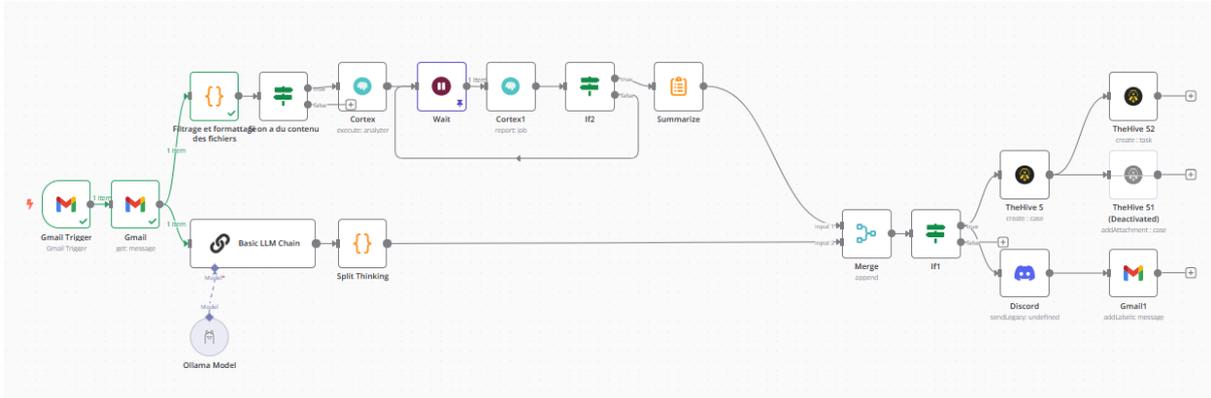


En connectant le compte cortex (cliquez sur le stylo et rentrez API et adresse URL du serveur), vous obtiendrez immédiatement des informations comme les analyseurs à

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

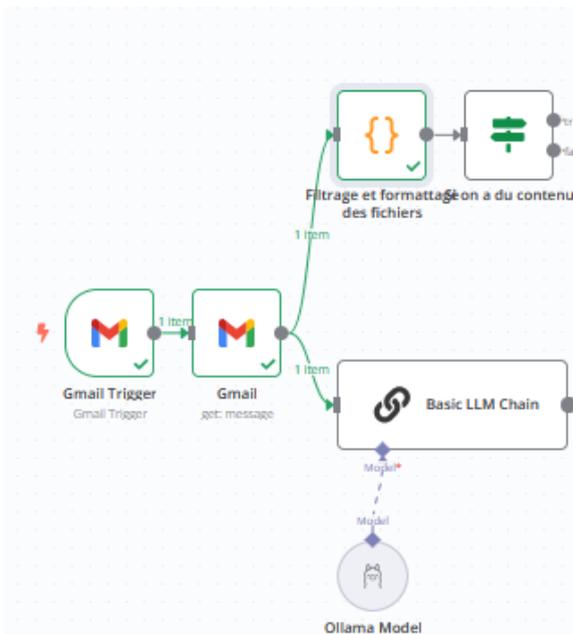


7.7 Orchestration complète



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).

{} Filtrage et formattage des fichiers
Test step

Parameters
Settings
Docs [↗](#)

Mode

Run Once for All Items
▼

Language

JavaScript
▼

JavaScript

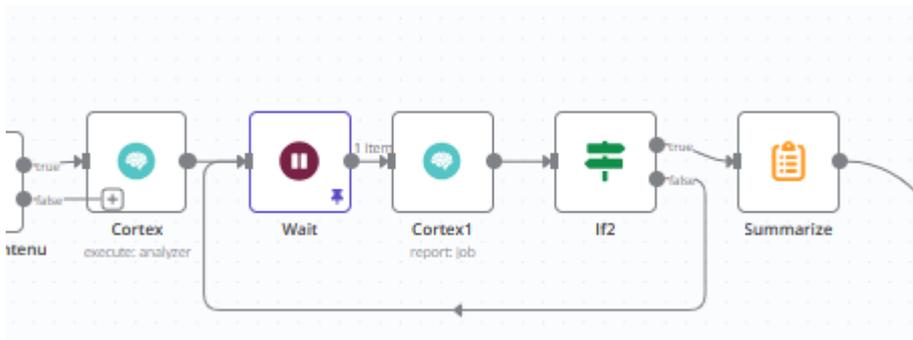
```

1  let results = [];
2
3  let extensions = [
4    "eml",
5    "",
6    null,
7    undefined,
8  ];
9
10 for (item of items) {
11   for (key of Object.keys(item.binary || [])) {
12    if (!extensions.includes(item.binary[key].fileExtension)) {
13     results.push({
14       json: {},
15       binary: {
16         data: item.binary[key],
17       },
18     });
19   }
20 }

```

Type \$ for a list of [special vars/methods](#). Debug by using `console.log()` statements and viewing their output in the browser console.

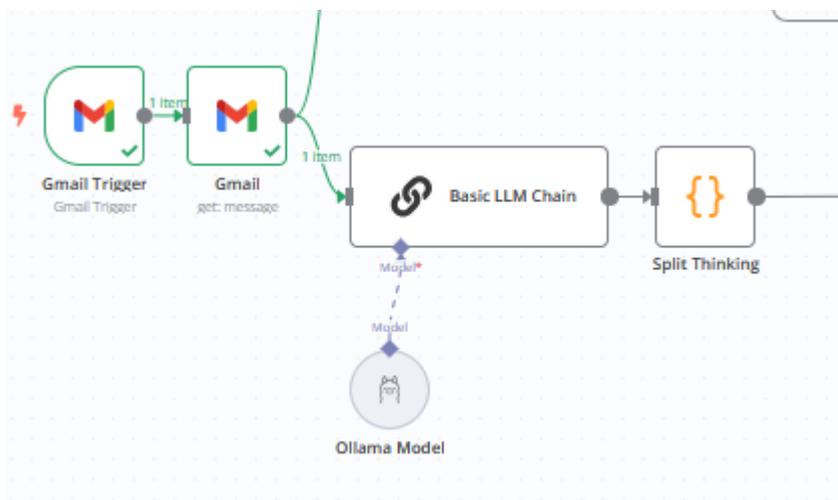
7.7.2 Bloc de traitement cortex : analyse de chaque pièce jointe via cortex (et virus total)



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).

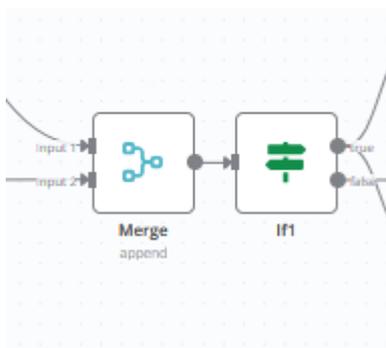
7.7.3 Bloc de traitement LLM IA : la branche qui analyse du contenu textuel pour verdict, phishing ou non.

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

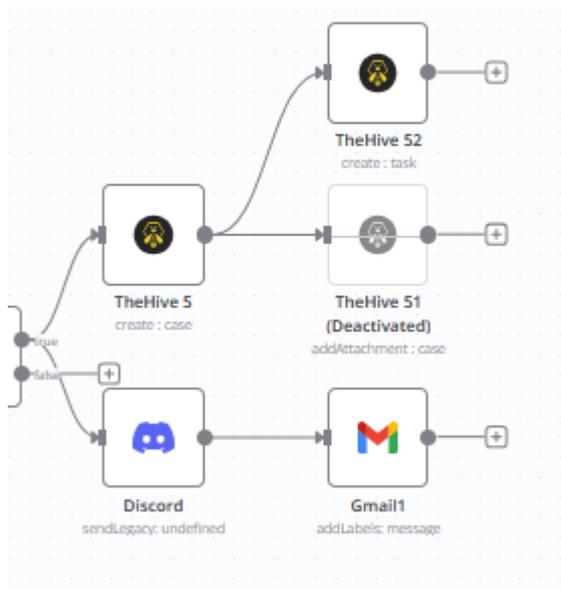


7.7.4 Bloc de regroupement des informations décisionnelles :

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



7.7.5 Bloc d'actions:



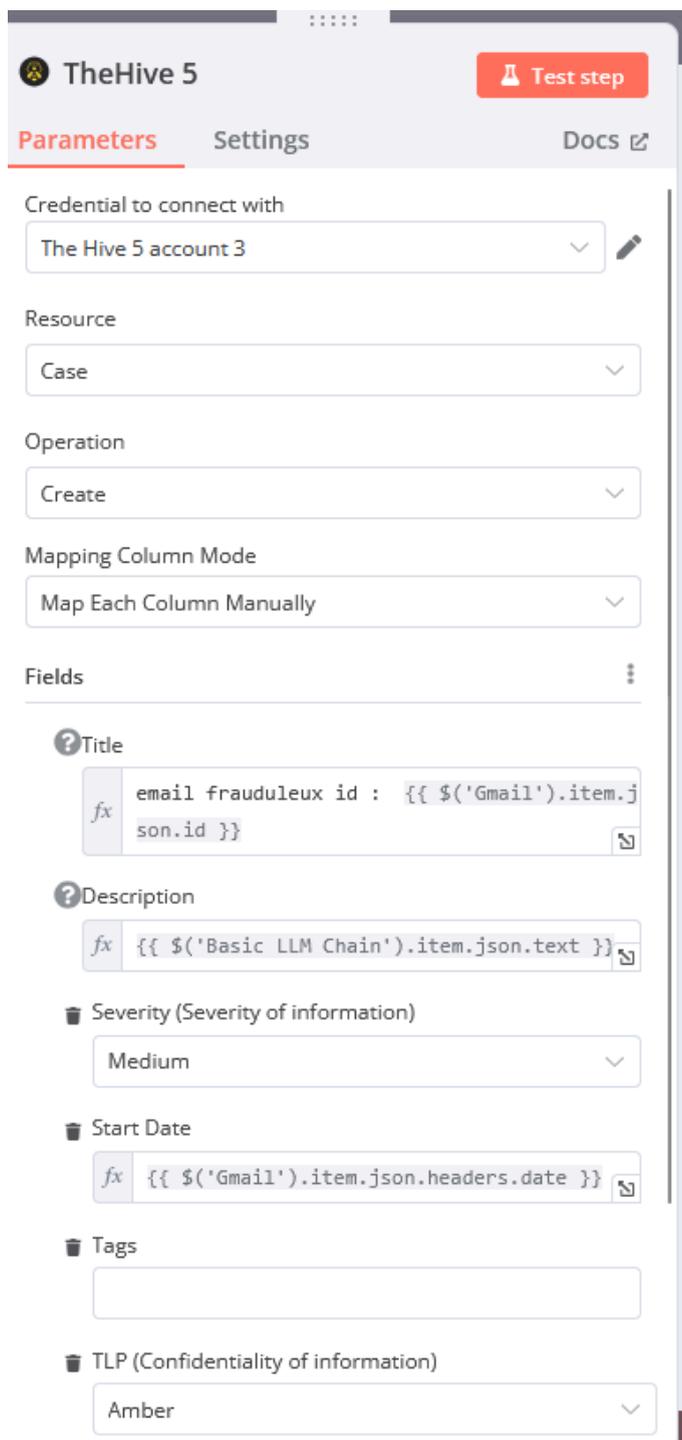
Exemple du module thehive, nous choisissons créer un case et nous pouvons pré remplir dynamiquement les informations qui vont peupler le case dans l'interface thehive.

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

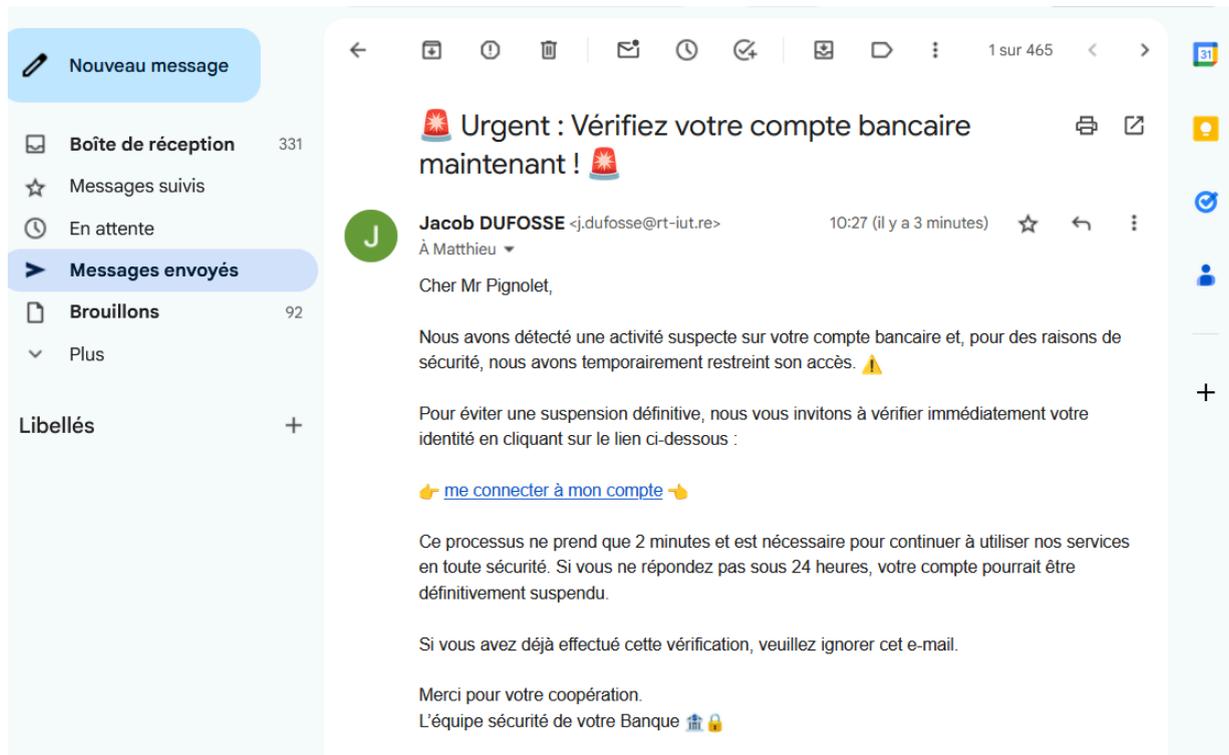
Sur la page suivante vous pouvez voir la configuration dynamique du module.



The screenshot shows the configuration page for a TheHive 5 module. The interface includes a header with the module name 'TheHive 5', a 'Test step' button, and tabs for 'Parameters', 'Settings', and 'Docs'. The configuration is organized into several sections:

- Credential to connect with:** A dropdown menu set to 'The Hive 5 account 3'.
- Resource:** A dropdown menu set to 'Case'.
- Operation:** A dropdown menu set to 'Create'.
- Mapping Column Mode:** A dropdown menu set to 'Map Each Column Manually'.
- Fields:** A list of fields with their corresponding values:
 - Title:** A text field containing the expression `email frauduleux id : {{ $('Gmail').item.json.id }}`.
 - Description:** A text field containing the expression `{{ $('Basic LLM Chain').item.json.text }}`.
 - Severity (Severity of information):** A dropdown menu set to 'Medium'.
 - Start Date:** A text field containing the expression `{{ $('Gmail').item.json.headers.date }}`.
 - Tags:** An empty text input field.
 - TLP (Confidentiality of information):** A dropdown menu set to 'Amber'.

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

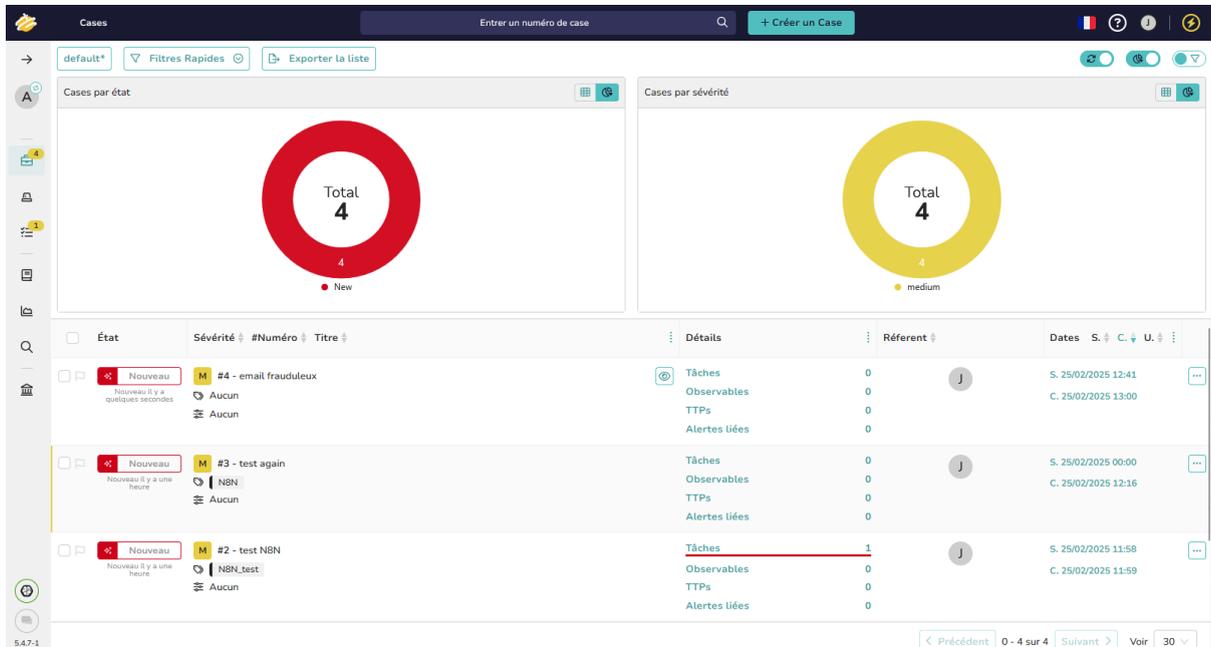


La détection est effective, le LLM juge que c'est un courriel de phishing. Le cas est automatiquement créé dans la plateforme thehive comme on peut le voir sur la page suivante, sous le titre de cas email frauduleux. Les informations sont bien collectées comme souhaité (description et date).

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.

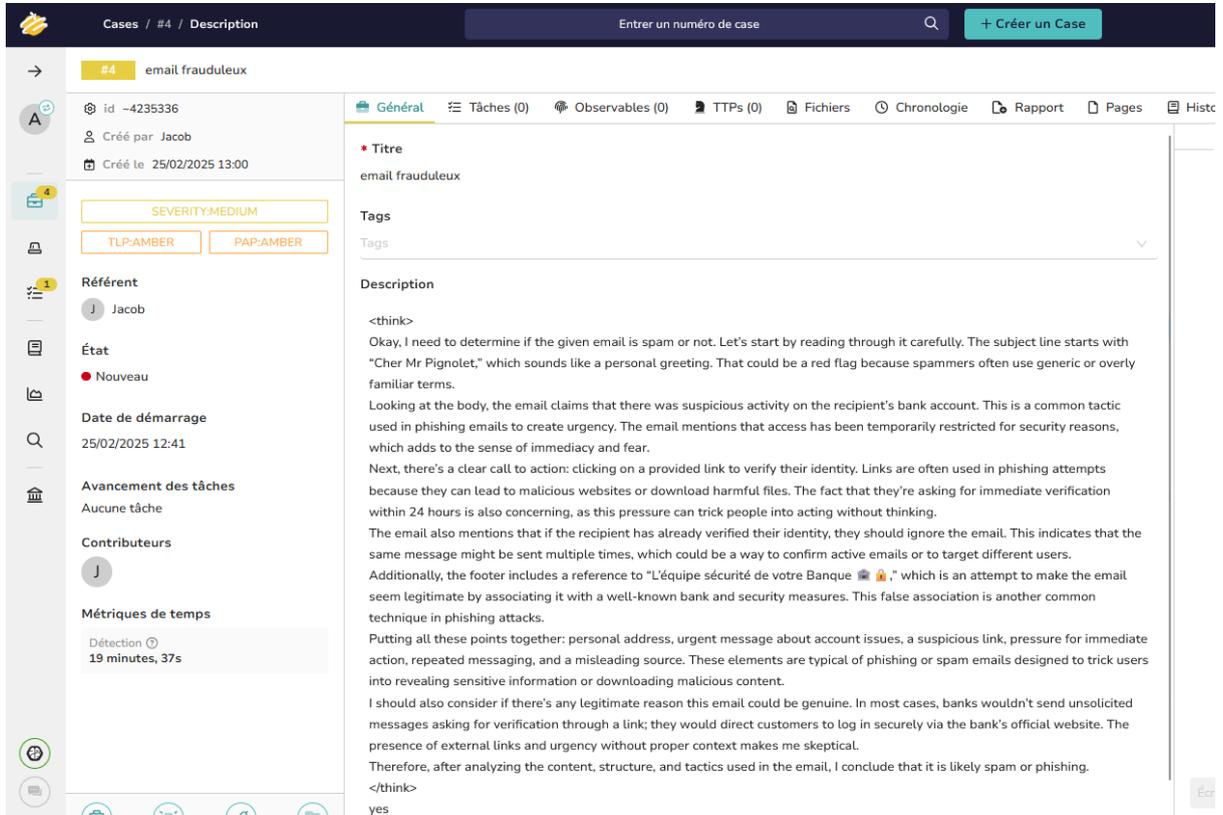


The screenshot shows the TheHive interface with two summary charts at the top: 'Cases par état' (Total 4, New) and 'Cases par sévérité' (Total 4, medium). Below these is a table of cases:

État	Sévérité	#Numéro	Titre	Détails	Référent	Dates
Nouveau	M	#4	#4 - email frauduleux	Tâches: 0, Observables: 0, TTPs: 0, Alertes liées: 0	J	S. 25/02/2025 12:41, C. 25/02/2025 13:00
Nouveau	M	#3	#3 - test again	Tâches: 0, Observables: 0, TTPs: 0, Alertes liées: 0	J	S. 25/02/2025 00:00, C. 25/02/2025 12:16
Nouveau	M	#2	#2 - test NBN	Tâches: 1, Observables: 0, TTPs: 0, Alertes liées: 0	J	S. 25/02/2025 11:58, C. 25/02/2025 11:59

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.



#4 email frauduleux

id -4235336
Créé par Jacob
Créé le 25/02/2025 13:00

SEVERITY:MEDIUM
TLP:AMBER PAP:AMBER

Référent
Jacob

État
Nouveau

Date de démarrage
25/02/2025 12:41

Avancement des tâches
Aucune tâche

Contributeurs
Jacob

Métriques de temps
Détection 19 minutes, 37s

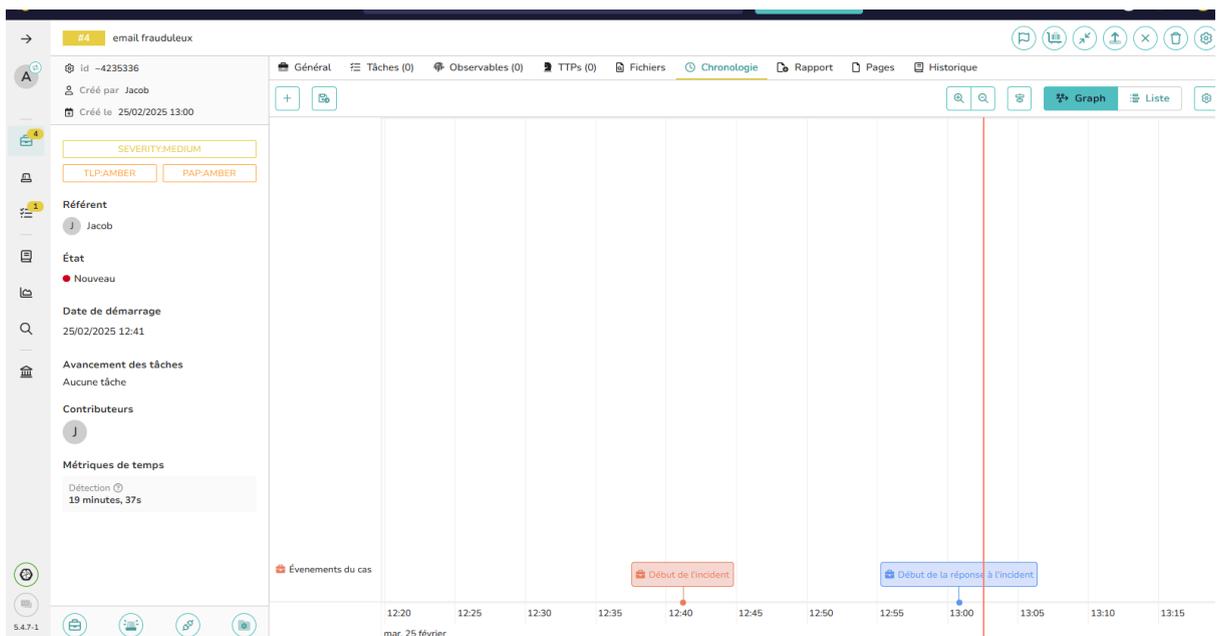
Titre
email frauduleux

Tags
Tags

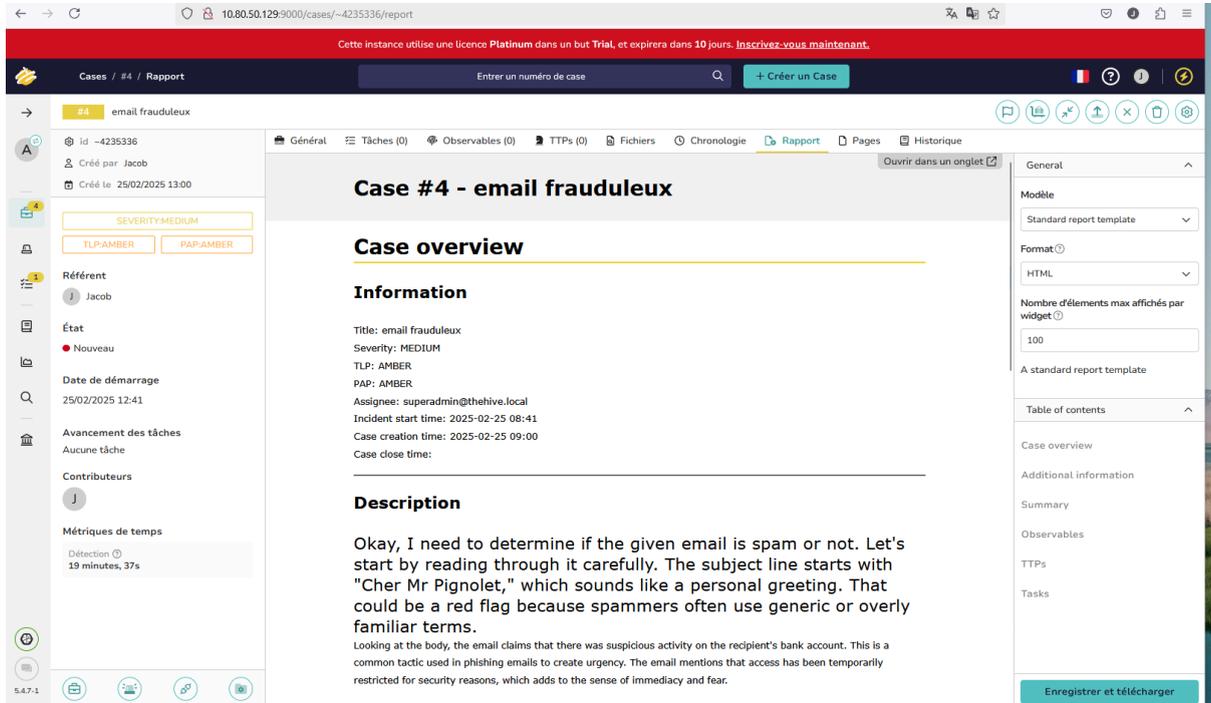
Description

<think>
Okay, I need to determine if the given email is spam or not. Let's start by reading through it carefully. The subject line starts with "Cher Mr Pignolet," which sounds like a personal greeting. That could be a red flag because spammers often use generic or overly familiar terms.
Looking at the body, the email claims that there was suspicious activity on the recipient's bank account. This is a common tactic used in phishing emails to create urgency. The email mentions that access has been temporarily restricted for security reasons, which adds to the sense of immediacy and fear.
Next, there's a clear call to action: clicking on a provided link to verify their identity. Links are often used in phishing attempts because they can lead to malicious websites or download harmful files. The fact that they're asking for immediate verification within 24 hours is also concerning, as this pressure can trick people into acting without thinking.
The email also mentions that if the recipient has already verified their identity, they should ignore the email. This indicates that the same message might be sent multiple times, which could be a way to confirm active emails or to target different users.
Additionally, the footer includes a reference to "L'équipe sécurité de votre Banque" which is an attempt to make the email seem legitimate by associating it with a well-known bank and security measures. This false association is another common technique in phishing attacks.
Putting all these points together: personal address, urgent message about account issues, a suspicious link, pressure for immediate action, repeated messaging, and a misleading source. These elements are typical of phishing or spam emails designed to trick users into revealing sensitive information or downloading malicious content.
I should also consider if there's any legitimate reason this email could be genuine. In most cases, banks wouldn't send unsolicited messages asking for verification through a link; they would direct customers to log in securely via the bank's official website. The presence of external links and urgency without proper context makes me skeptical.
Therefore, after analyzing the content, structure, and tactics used in the email, I conclude that it is likely spam or phishing.
</think>
yes

La timeline du cas :



Le résumé du cas en question:



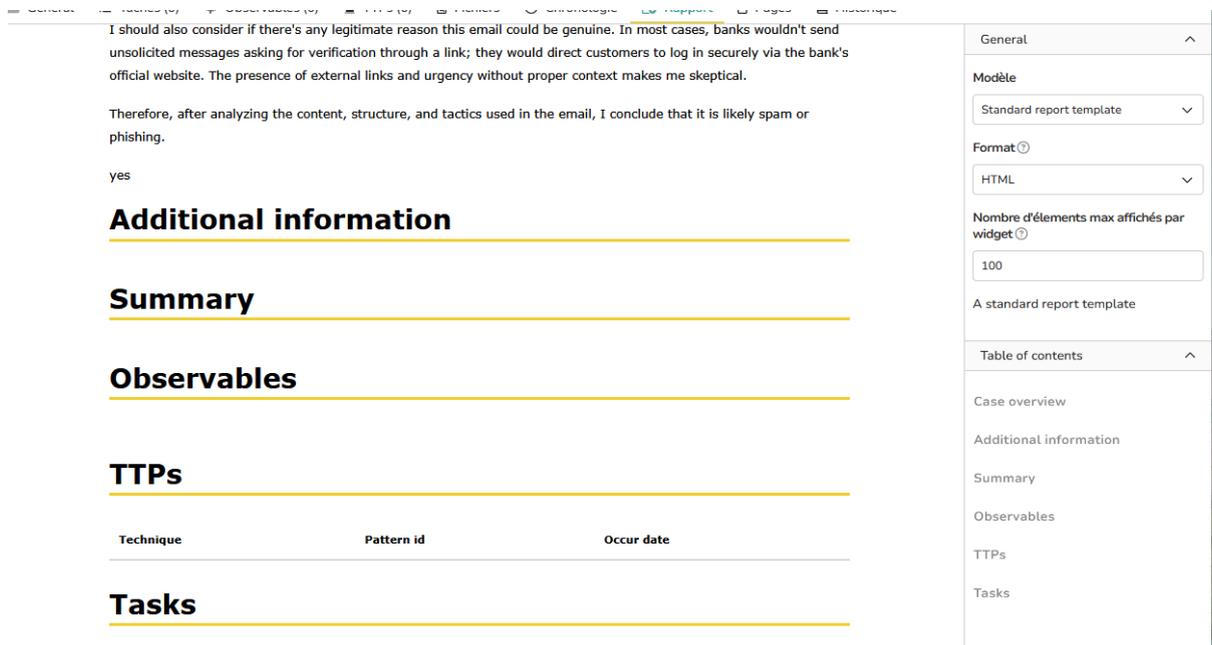
The screenshot shows a web application interface for a case report. The main content area is titled "Case #4 - email frauduleux" and includes a "Case overview" section with the following information:

- Information:**
 - Title: email frauduleux
 - Severity: MEDIUM
 - TLP: AMBER
 - PAP: AMBER
 - Assignee: superadmin@thehive.local
 - Incident start time: 2025-02-25 08:41
 - Case creation time: 2025-02-25 09:00
 - Case close time:
- Description:**

Okay, I need to determine if the given email is spam or not. Let's start by reading through it carefully. The subject line starts with "Cher Mr Pignolet," which sounds like a personal greeting. That could be a red flag because spammers often use generic or overly familiar terms.

Looking at the body, the email claims that there was suspicious activity on the recipient's bank account. This is a common tactic used in phishing emails to create urgency. The email mentions that access has been temporarily restricted for security reasons, which adds to the sense of immediacy and fear.

The interface also shows a sidebar with case details, a top navigation bar, and a right-hand panel with report settings.



The detailed view of the case report content includes the following sections:

- Additional information:**

I should also consider if there's any legitimate reason this email could be genuine. In most cases, banks wouldn't send unsolicited messages asking for verification through a link; they would direct customers to log in securely via the bank's official website. The presence of external links and urgency without proper context makes me skeptical.

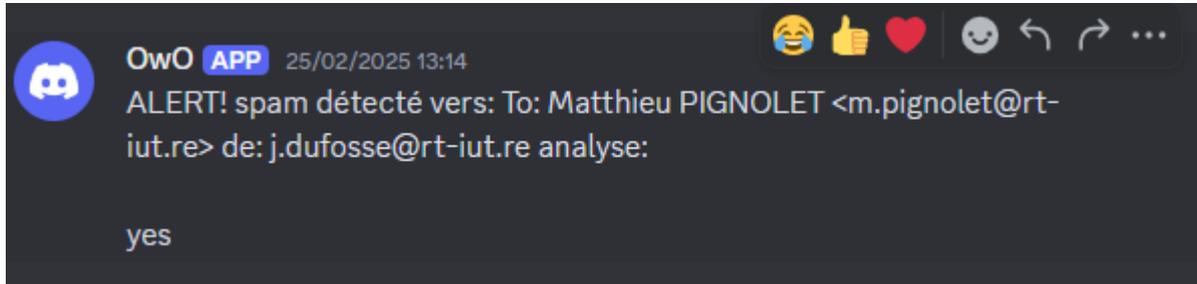
Therefore, after analyzing the content, structure, and tactics used in the email, I conclude that it is likely spam or phishing.

yes
- Summary:**
- Observables:**
- TTPs:**

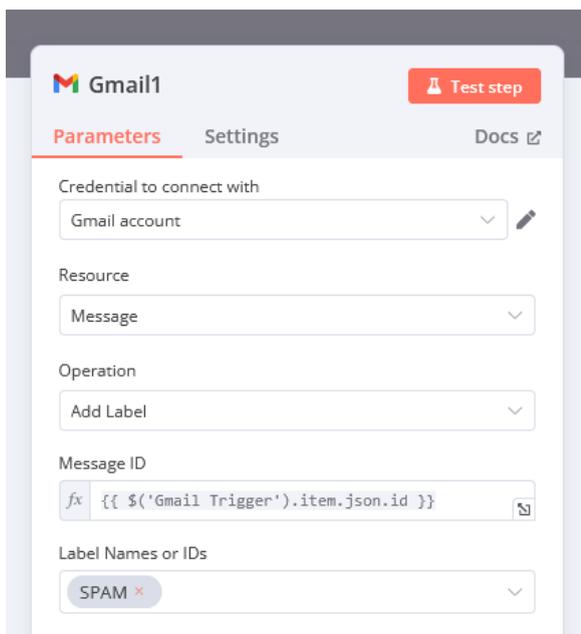
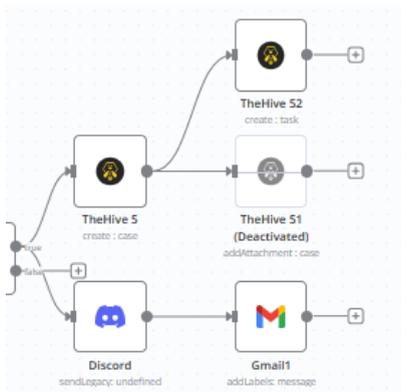
Technique	Pattern id	Occur date
- Tasks:**

The right-hand panel shows report settings such as "Modèle" (Standard report template), "Format" (HTML), and "Nombre d'éléments max affichés par widget" (100).

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.