



République Tunisienne

Ministère de l'Enseignement Supérieur  
et de la Recherche Scientifique

École Supérieur Privée d'ingénierie et de technologie

TEK-UP



## RAPPORT DE PROJET DE FIN D'ÉTUDES

Présenté en vue de l'obtention du

Diplôme National d'Ingénieur en Sciences Appliquées et Technologiques

Spécialité : Sécurité des systèmes et réseaux informatiques

Réalisé par

**Amal DAAS**

---

## Mise en place d'un outil pour l'automatisation des tests de sécurité dans un SOC moderne

---

Encadrant professionnel : **Monsieur Ameur AMRI**

SOC Team Leader

Encadrant académique : **Monsieur Tarek HDIJI**

Expert Network

J'autorise l'étudiant à faire le dépôt de son rapport de stage en vue d'une soutenance.

Encadrant professionnel, **M. Ameur AMRI**

**Signature et cachet**

J'autorise l'étudiant à faire le dépôt de son rapport de stage en vue d'une soutenance.

Encadrant académique, **M. Tarek HDIJI**

**Signature**

# Dédicace

*À tous ceux qui, discrètement ou avec éclat, ont nourri en moi la force et la détermination d'aller jusqu'au bout.*

***À mes parents, Salwa et Hamadi,***

*Pour votre amour constant, votre confiance inébranlable et votre soutien sans faille. Vous êtes les piliers qui m'ont guidée, inspirée et encouragée chaque jour. Ce succès est le fruit de notre union et de votre présence indéfectible.*

***À ma famille,***

*À mon frère Amine, à mes belles-sœurs Imen, Asma, Samar et Sahar*

*Merci pour vos encouragements, votre tendresse et votre présence rassurante. Vous avez toujours été mon refuge, un lieu où je trouve force et réconfort. Merci d'être ma source d'équilibre.*

***À mon tendre soutien Chedly,***

*Pour ta présence constante, ton écoute attentive et ton soutien précieux tout au long de cette période. Tu as su m'apaiser dans les moments de doute, m'encourager dans les phases décisives et me rappeler, discrètement mais sûrement, que je pouvais y arriver. Merci pour ta bienveillance et ta force silencieuse.*

***À mes amies,***

*À Salsabil, Roua et Siwar*

*Merci pour vos sourires, votre complicité et les moments partagés, qu'ils soient pleins de joie ou de calme. Vous avez été ma lumière dans les jours sombres, ma source de bonheur et de motivation.*

*Merci d'avoir été là, tout simplement.*

# Remerciements

*Je désire exprimer mes remerciements les plus sincères à toutes les personnes ayant contribué à la bonne réalisation de mon projet.*

*Tout d'abord, je remercie très chaleureusement **M. Tarek HDIJI**, encadrant académique, pour son suivi efficace, sa disponibilité permanente et ses remarques toujours appréciées, qui ont contribué à la qualité et à l'avancée de ce travail.*

*Je remercie également **M. Ameur Amri**, encadrant professionnel pour ses précieux conseils et son écoute tout au long de cette expérience.*

*Je remercie également mes membres du jury, que je remercie sincèrement pour le temps consacré à l'évaluation de ce projet.*

*Merci.*

# Table des matières

<b>Introduction générale</b>	<b>1</b>
<b>1 Cadre général</b>	<b>2</b>
Introduction . . . . .	3
1.1 Présentation de l'entreprise . . . . .	3
1.1.1 Les engagements . . . . .	3
1.1.2 Keystone Labs . . . . .	3
1.1.3 Les services . . . . .	4
1.2 Présentation du projet . . . . .	5
1.2.1 Analyse de l'existant . . . . .	5
1.2.2 Solution proposée . . . . .	6
1.2.3 Objectif du projet . . . . .	6
1.2.4 Gestion de projet . . . . .	7
Conclusion . . . . .	9
<b>2 État de l'art</b>	<b>10</b>
Introduction . . . . .	11
2.1 Centre des opérations de sécurité (SOC) . . . . .	11
2.1.1 Définition du SOC . . . . .	11
2.1.2 L'importance du SOC . . . . .	12
2.1.3 Rôles et responsabilités de l'équipe SOC . . . . .	12
2.2 Système de gestion des informations et des événements de sécurité (SIEM) . . . . .	12
2.2.1 Définition . . . . .	12
2.2.2 Les avantages d'un SIEM . . . . .	13
2.3 Analyse comparative des solutions . . . . .	13
2.3.1 Solutions SIEM . . . . .	13
2.3.2 Solutions de détection d'intrusions . . . . .	18
2.4 Orchestration de la sécurité et d'automatisation de réponse (SOAR) . . . . .	22
2.4.1 Définition . . . . .	22
2.4.2 Le fonctionnement de SOAR . . . . .	22
2.4.3 Cas d'usage du SOAR . . . . .	24
2.4.4 Analyse comparative des outils SOAR . . . . .	24

---

2.5	Émulation d'adversaire (Adversary emulation) . . . . .	31
2.5.1	Renseignement sur les menaces . . . . .	31
2.5.2	Simulation des attaques . . . . .	33
2.5.3	Caldera . . . . .	34
2.6	Virtualisation . . . . .	36
2.6.1	Définition . . . . .	36
2.6.2	Machine virtuelle . . . . .	37
2.6.3	Hyperviseur . . . . .	37
2.6.4	Les différents types de virtualisation . . . . .	38
2.6.5	Les avantages de la virtualisation . . . . .	39
2.7	Conteneurisation . . . . .	39
2.7.1	Définition . . . . .	39
2.7.2	Les avantages de la conteneurisation . . . . .	39
2.7.3	Docker . . . . .	40
2.8	Cloud Computing . . . . .	40
2.8.1	Définition . . . . .	40
2.8.2	Les avantages de Cloud computing . . . . .	40
2.8.3	Google Cloud . . . . .	41
2.8.4	Oracle Cloud . . . . .	41
2.9	Intégration de l'intelligence artificielle (AI) . . . . .	41
2.9.1	L'intelligence artificielle (AI) . . . . .	41
2.9.2	Le grand modèle de langage (LLM) . . . . .	42
2.9.3	Les avantages d'intégrer un LLM dans un SOC . . . . .	43
2.10	Systèmes de notification et de messagerie . . . . .	43
2.10.1	Slack . . . . .	43
2.10.2	Zoho Mail . . . . .	44
2.11	Architecture envisagée . . . . .	44
	Conclusion . . . . .	44
<b>3</b>	<b>Mise en place de la solution SIEM</b> . . . . .	<b>45</b>
	Introduction . . . . .	46
3.1	Mise en place de Wazuh . . . . .	46
3.1.1	Déploiement de certificats . . . . .	46
3.1.2	Les agents wazuh . . . . .	47

---

---

3.1.3	Configuration de Sysmon . . . . .	48
3.1.4	Configuration des règles personnalisées . . . . .	49
3.1.5	Réponse active (Active Response) . . . . .	51
3.2	Installation et configuration d'un système de détection d'intrusion (IDS) . . . . .	52
3.2.1	Mise en place d'un système de détection d'intrusion réseau (NIDS) . . . . .	52
3.2.2	Mise en place d'un système de détection d'intrusion réseau (HIDS) . . . . .	54
	Conclusion . . . . .	55
<b>4</b>	<b>Mise en place de la solution SOAR</b>	<b>56</b>
	Introduction . . . . .	57
4.1	Les outils choisis SOAR . . . . .	57
4.2	Mise en place des outils . . . . .	57
4.2.1	Installation de Docker . . . . .	57
4.2.2	Mise en place de YETI . . . . .	58
4.2.3	Mise en place de Cortex . . . . .	60
4.2.4	Mise en place de TheHive . . . . .	62
4.2.5	Mise en place de Shuffle . . . . .	64
4.2.6	Scénario de test 1 : Attaque sur le réseau . . . . .	74
4.2.7	Scénario de test 2 : Attaque de Phishing . . . . .	78
	Conclusion . . . . .	81
<b>5</b>	<b>Mise en place d'une solution d'automatisation des tests de sécurité</b>	<b>82</b>
	Introduction . . . . .	83
5.1	Mise en place de Caldera . . . . .	83
5.1.1	Déploiement des agents . . . . .	85
5.1.2	Les capacités (Abilities) . . . . .	85
5.1.3	Le profil d'adversaire (Adversaries) . . . . .	86
5.1.4	Les opérations (operations) . . . . .	87
5.2	Simulations des scénarios de tests dans le SOC . . . . .	87
5.2.1	Tests des agents Windows . . . . .	87
5.2.2	Tests des agents Cloud . . . . .	91
5.3	Simulation de tests automatiques sur le workflow . . . . .	92
	Conclusion . . . . .	95

<b>Conclusion générale</b>	<b>96</b>
<b>Annexes</b>	<b>97</b>
Annexe A : Agent des agents Wazuh . . . . .	97
Annexe B : Configuration des décodeurs et des règles de détection . . . . .	98
Annexe B : Configuration des agents Caldera . . . . .	103
<b>Bibliographie</b>	<b>105</b>

# Table des figures

1.1	Logo de KEYSTONE . . . . .	3
1.2	Architecture existante . . . . .	5
1.3	Architecture proposée . . . . .	6
1.4	Processus de Kanban . . . . .	9
1.5	Diagramme de Gantt . . . . .	9
2.1	Les éléments constitutifs d'un SOC . . . . .	11
2.2	Processus opérationnel du SIEM . . . . .	13
2.3	Logo de Wazuh . . . . .	14
2.4	Fonctionnalités avancées de Wazuh . . . . .	16
2.5	Les composants de Wazuh . . . . .	17
2.6	Les agents Wazuh . . . . .	17
2.7	Architecture globale Wazuh . . . . .	18
2.8	Logo de Suricata . . . . .	22
2.9	Logo de Falco . . . . .	22
2.10	Fonctionnement de SOAR . . . . .	24
2.11	Logo de TheHive . . . . .	26
2.12	Logo de Cortex . . . . .	27
2.13	Logo de Yeti . . . . .	29
2.14	Logo de Shuffle . . . . .	31
2.15	Pyramid Of Pain . . . . .	32
2.16	Logo de Caldera . . . . .	34
2.17	L'infrastructure de Caldera . . . . .	36
2.18	Types d'hyperviseurs . . . . .	37
2.19	Logo de VMware Workstation . . . . .	38
2.20	Types de virtualisation . . . . .	39
2.21	Logo de Docker . . . . .	40
2.22	Logo de Google Cloud Platform . . . . .	41
2.23	Logo de Oracle Cloud . . . . .	41
2.24	Hiérarchie de l'AI . . . . .	42
2.25	Logo de LLM . . . . .	42

2.26 Logo de Slack . . . . .	43
2.27 Logo de Zoho Mail . . . . .	44
2.28 Architecture envisagée . . . . .	44
3.1 Cluster Wazuh . . . . .	46
3.2 Génération des certificats TLS . . . . .	47
3.3 Interface utilisateur de Wazuh . . . . .	47
3.4 Liste des agents . . . . .	48
3.5 Installation de Sysmon sur Windows10 . . . . .	48
3.6 Installation de Sysmon sur Ubuntu . . . . .	49
3.7 Collecte des logs Sysmon Windows . . . . .	49
3.8 Collecte des logs Sysmon Linux . . . . .	49
3.9 Règle Wazuh pour la protection SSH . . . . .	50
3.10 Test de la règle . . . . .	50
3.11 Validation de l'alerte dans les logs . . . . .	50
3.12 Description d'une alerte . . . . .	51
3.13 Configuration d'une réponse active dans Wazuh . . . . .	51
3.14 Vérification de la réponse active dans Wazuh . . . . .	52
3.15 Affichage des règles iptables sur l'agent . . . . .	52
3.16 Installation de Suricata . . . . .	52
3.17 Configuration de Suricata en tant que NIDS . . . . .	53
3.18 Configuration des règles . . . . .	53
3.19 Configuration des logs Suricata vers Wazuh . . . . .	53
3.20 Statut des agents du réseau local . . . . .	53
3.21 Configuration de Suricata en tant que HIDS . . . . .	54
3.22 Configuration des logs Falco vers Wazuh . . . . .	54
3.23 Alerta générée par Falco . . . . .	54
4.1 Installation de docker et docker compose . . . . .	58
4.2 Conteneurs de YETI . . . . .	58
4.3 Interface graphique de YETI . . . . .	59
4.4 Les flux de YETI . . . . .	59
4.5 Résultat de la recherche d'un observable dans Yeti . . . . .	60
4.6 Conteneurs de Cortex . . . . .	60
4.7 Interface graphique de Cortex . . . . .	61

4.8 Configuration d'une organisation dans Cortex . . . . .	61
4.9 Analyseurs de Cortex . . . . .	62
4.10 Conteneur de TheHive . . . . .	62
4.11 Interface de TheHive . . . . .	63
4.12 Création d'une organisation dans TheHive . . . . .	63
4.13 Création d'un utilisateur dans TheHive . . . . .	63
4.14 Conteneurs de Shuffle . . . . .	64
4.15 Association d'un nom de domaine . . . . .	64
4.16 Reverse proxy Nginx . . . . .	65
4.17 Interface de Shuffle . . . . .	66
4.18 Intégration de Wazuh avec Shuffle . . . . .	66
4.19 Intégration avec ZohoMail . . . . .	67
4.20 Intégration avec TheHive . . . . .	67
4.21 Intégration avec YETI . . . . .	68
4.22 Intégration avec LLM . . . . .	69
4.23 Prompt LLM – Attaque réseau . . . . .	70
4.24 Prompt LLM – Attaque Phishing . . . . .	71
4.25 Intégration avec Slack . . . . .	72
4.26 Contenu de la notification Slack - Attaque réseau . . . . .	72
4.27 Contenu de la notification Slack - Attaque de Phishing . . . . .	73
4.28 Réponse Active de Wazuh . . . . .	73
4.29 Workflow pour la détection des attaques dans le réseau . . . . .	74
4.30 Attaque par Brute Force . . . . .	75
4.31 Notification de Slack . . . . .	75
4.32 Résultat de YETI . . . . .	75
4.33 Rapport de YETI . . . . .	76
4.34 Description de l'alerte . . . . .	76
4.35 Observables de l'alerte d'une adresse légitime . . . . .	77
4.36 Observables de l'alerte d'une adresse malveillante . . . . .	77
4.37 Action de blocage d'une adresse IP malveillante . . . . .	77
4.38 Liste des règles iptables . . . . .	78
4.39 Workflow pour la détection des attaques de Phishing . . . . .	78
4.40 Envoi un nouveau mail . . . . .	79
4.41 Alerta de TheHive . . . . .	79

---

4.42	Création d'un cas dans TheHive . . . . .	80
4.43	Analyse des URLs par Cortex . . . . .	80
4.44	Notification de Slack . . . . .	80
5.1	Installation de Caldera . . . . .	83
5.2	Déploiement de Caldera . . . . .	83
5.3	Interface graphique de Caldera . . . . .	84
5.4	Le tableau de board de Caldera . . . . .	84
5.5	Les agents de Caldera . . . . .	85
5.6	Les capacités de Caldera . . . . .	86
5.7	Exemple de profil d'adversaire Caldera . . . . .	86
5.8	Opération simulée . . . . .	87
5.9	Création d'une capacité - Mimikatz . . . . .	88
5.10	Commandes utilisées - Mimikatz . . . . .	88
5.11	Création d'un adversaire - Mimikatz . . . . .	89
5.12	Création d'une opération . . . . .	90
5.13	Opération accomplie - Mimikatz . . . . .	90
5.14	Alerte de Wazuh - Mimikatz . . . . .	91
5.15	Création d'un adversaire - MySQL_Manipulation . . . . .	91
5.16	Opération accomplie - MySQL_Manipulation . . . . .	91
5.17	Alerte de wazuh - MySQL_Manipulation . . . . .	92
5.18	Création d'un adversaire - web-application-test . . . . .	92
5.19	Opération accomplie - web-application-test . . . . .	92
5.20	Alerte Slack . . . . .	93
5.21	Résultat de YETI . . . . .	93
5.22	Alerte TheHive - SQL Injection . . . . .	94
5.23	Rapport d'analyse de l'adresse IP . . . . .	94
6.1	Ajout d'un agent Ubuntu sur Wazuh . . . . .	97
6.2	Commandes d'installation de l'agent Wazuh . . . . .	98
6.3	Configuration des décodeurs Sysmon pour Wazuh . . . . .	99
6.4	La configuration de règles dédiées à Sysmon . . . . .	100
6.5	Fichier de configuration de Falco . . . . .	100
6.6	La configuration de règles dédiées à Falco . . . . .	101
6.7	Collecte des logs MySQL . . . . .	101

6.8 Configuration des décodeurs MYSQL . . . . .	102
6.9 Configuration des règles MYSQL . . . . .	103
6.10 Création de l'agent Sandcat . . . . .	104
6.11 Déploiement de l'agent Caldera sur Ubuntu . . . . .	104

# Liste des tableaux

1.1	Les méthodologies des projets . . . . .	8
2.1	Comparaison des SIEM . . . . .	14
2.2	Comparaison des outils HIDS . . . . .	19
2.3	Comparaison des NIDS . . . . .	21
2.4	Comparaison des outils de gestion des incidents . . . . .	25
2.5	Comparaison des outils d'analyseur . . . . .	27
2.6	Comparaison des CTI . . . . .	29
2.7	Comparaison des plateformes d'orchestration et d'automatisation . . . . .	30
2.8	Comparaison des outils d'émulation d'adversaire . . . . .	34

# Liste des abréviations

- **AI** = Intelligence Artificielle
- **API** = Application Programming Interface
- **ATT&Ck** = Adversarial Tactics, Techniques, & Common Knowledge
- **CTI** = Cyber Threat Intelligence
- **DL** = Deep Learning
- **HIDS** = Host Intrusion Detection Systems
- **HTTP** = Hypertext Transfer Protocol
- **IDS** = Intrusion Detection System
- **IoC** = Indicator of Compromise
- **LLM** = Large Language Model
- **MISP** = Malware Information Sharing Platform
- **ML** = Machine Learning
- **NIDS** = Network Intrusion Detection Systems
- **OSSEC** = Open Source Security Information and Event Management
- **SIEM** = Security Information and Event Management
- **SOAR** = Security Orchestration, Automation, and Response
- **SOC** = Security Operation Center
- **SSH** = Secure Shell
- **SSL** = Secure Sockets Layer
- **TTP** = Tactics, Techniques, and Procedure
- **URL** = Uniform Resource Locator
- **YETI** = Your Everyday Threat Intelligence

# Introduction générale

À l'ère du numérique, la cybersécurité est devenue un enjeu stratégique essentiel pour assurer la continuité des activités des entreprises. Face à des menaces toujours plus complexes et ciblées, les organisations doivent adopter des approches de défense intelligentes et adaptatives. Les centres opérationnels de sécurité (SOC) jouent un rôle clé en assurant la détection et la réponse aux incidents. Toutefois, pour rester performants, ces SOC doivent être régulièrement évalués. L'automatisation des tests de sécurité permet ainsi de simuler des attaques réalistes afin de mesurer leur efficacité et d'améliorer en continu leur posture défensive.

C'est dans ce contexte que s'inscrit le présent projet de fin d'études, réalisé au sein du SOC de KEYSTONE-Group. Il porte sur la mise en place et l'intégration d'un outil d'automatisation des tests de sécurité, en combinaison avec une solution d'orchestration et d'automatisation de la réponse (SOAR). L'objectif est de fournir une plateforme complète et intégrée, capable de simuler des attaques, de détecter les failles, d'analyser les résultats et d'optimiser la réponse aux incidents, tout en améliorant la posture globale de sécurité du SOC.

Le rapport débute par la présentation du cadre général du projet, avec une description de l'organisme d'accueil, une analyse de l'existant, les objectifs poursuivis ainsi que la méthodologie adoptée. Il se poursuit par un état de l'art, qui introduit les concepts fondamentaux de la cybersécurité opérationnelle, les technologies utilisées et les solutions comparées, avant de justifier les choix retenus et de décrire l'architecture globale déployée. Le troisième chapitre est consacré à la mise en place de la solution SIEM, en détaillant son déploiement, sa configuration ainsi que son rôle dans la collecte et la corrélation des événements de sécurité. Le quatrième chapitre traite de l'intégration de la solution SOAR, en présentant les outils choisis, les workflows développés, ainsi que les mécanismes d'orchestration et d'automatisation des réponses aux incidents. Enfin, le cinquième chapitre porte sur la mise en œuvre de l'outil d'automatisation des tests de sécurité, en décrivant les scénarios d'attaques simulées, les résultats obtenus et leur impact sur l'évaluation continue de la posture de sécurité du SOC.

Cette approche intégrée vise à garantir une évaluation continue et proactive de la sécurité du SOC, en tirant parti de l'intelligence artificielle, de l'automatisation et de l'orchestration pour faire face aux défis croissants du paysage cyber actuel.

# CADRE GÉNÉRAL

---

## Plan

Introduction . . . . .	3
1    Présentation de l'entreprise . . . . .	3
2    Présentation du projet . . . . .	5
Conclusion . . . . .	9

## Introduction

Dans ce chapitre, nous poserons le cadre général de notre projet. Nous commencerons par une présentation de l'entreprise d'accueil afin de mieux situer le contexte dans lequel il s'inscrit. Ensuite, nous donnerons un aperçu du projet en mettant en avant les défis à relever ainsi que les solutions existantes. Enfin, nous détaillerons notre approche en proposant une solution adaptée, tout en expliquant la méthodologie de gestion de projet mise en place pour assurer une planification rigoureuse et une réalisation efficace des objectifs fixés.

### 1.1 Présentation de l'entreprise

[1] KEYSTONE-Group est un bureau de Consulting en cybersécurité et en cyberdéfense basé à Tunis et Alger, disposant d'une équipe d'experts dans différentes disciplines de sécurité, allant du conseil à l'Ethical Hacking à l'R&D. Keystone travaille sur la région d'Afrique pour accompagner les gouvernements dans la mise en place de leurs programmes de cybersécurité et dans la mise en place de structure dédiée. Et fournit aussi des services pour les grandes entreprises pour développer leurs stratégies de sécurité et aussi pour mesurer le niveau de sécurité de leurs infrastructures technique et intervient aussi pour investiguer en cas d'attaque. Pour les PME, Keystone offre des packages de services pour gérer toute leur sécurité.



FIGURE 1.1 : Logo de KEYSTONE

#### 1.1.1 Les engagements

- Développement de politiques de sécurité flexibles et abordables.
- Mise en place de programmes de gestion des risques pour entreprises de toutes tailles.
- Formation pour experts en cybersécurité et sensibilisation des employés.

#### 1.1.2 Keystone Labs

[1] Keystone dispose d'un laboratoire de R&D axé sur l'analyse des menaces, la cybersécurité des IoT, et l'intelligence artificielle pour la détection des cyberattaques. Elle travaille aussi en partenariat avec l'Agence Tunisienne d'Internet pour analyser les menaces en temps réel

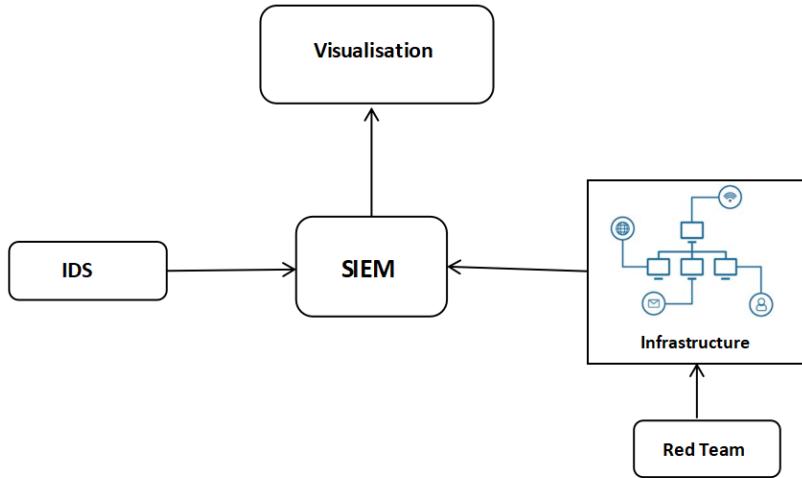
### 1.1.3 Les services

[1] Keystone Group propose des services avancés pour protéger les infrastructures informatiques des organisations. Grâce à une expertise approfondie, elle accompagne ses clients dans la gestion des risques, la conformité et la sécurisation des systèmes d'information.

- **Virtual CISO** : Un expert en sécurité externalisé qui aide à définir et gérer la stratégie de cybersécurité d'une entreprise.
- **Penetration Testing** : Simulations d'attaques pour identifier et corriger les vulnérabilités des systèmes.
- **Incident Response** : Intervention rapide en cas d'attaque pour limiter les dégâts et restaurer la sécurité.
- **Controls and Compliance** : Assistance pour respecter les réglementations et normes en cybersécurité.
- **Security Consulting** : Conseil en cybersécurité pour améliorer la résilience des entreprises face aux cybermenaces.
- **Capacity Building** : Formations et sensibilisation à la cybersécurité pour renforcer les compétences internes.
- **Security Audit** : Évaluation détaillée des systèmes pour détecter les faiblesses et proposer des améliorations.
- **Managed Security Services** : Supervision et gestion continue de la sécurité des systèmes d'information.

## 1.2 Présentation du projet

### 1.2.1 Analyse de l'existant



**FIGURE 1.2 : Architecture existante**

Cette architecture repose principalement sur des règles statiques et une intervention humaine pour détecter et gérer les incidents, ce qui entraîne plusieurs limitations. D'une part, la dépendance aux règles statiques empêche la détection efficace des menaces inconnues, car ces règles sont préétablies et ne peuvent s'adapter aux attaques émergentes ou sophistiquées. D'autre part, le manque d'automatisation ralentit considérablement la réponse aux incidents, car une intervention manuelle est souvent nécessaire, allongeant ainsi les délais de traitement et compromettant la réactivité du SOC.

De plus, l'absence de tests continus complique l'évaluation permanente de l'efficacité du SOC, rendant difficile l'identification des failles et l'optimisation des capacités de détection. Enfin, la surcharge des analystes, due au volume important de faux positifs générés par les règles statiques, réduit leur efficacité et augmente le temps de réponse face aux menaces réelles.

Cette architecture limite :

- **Dépendance aux règles statiques** : inefficaces face aux menaces inconnues et évolutives.
- **Manque d'automatisation** : ralenti la détection et la réponse aux incidents en raison d'une forte intervention manuelle.
- **Absence de tests continus** : empêche l'évaluation régulière des performances du SOC et l'identification des failles.
- **Surcharge des analystes** : augmentation des faux positifs, entraînant une perte de temps et une baisse de réactivité.

### 1.2.2 Solution proposée

Nous adoptons une approche avancée intégrant de nouvelles technologies pour améliorer la détection, l'analyse et la réponse aux menaces. Cette évolution renforce les capacités du SOC grâce à la Threat Intelligence, qui collecte et analyse les menaces en temps réel afin d'anticiper les attaques avant qu'elles ne surviennent.

Par ailleurs, la mise en place de simulations d'attaques automatiques permet d'évaluer en continu la posture de sécurité du système. L'intégration d'une solution SOAR (Security Orchestration, Automation & Response) améliore la gestion des incidents en orchestrant les outils du SOC, en automatisant les tâches de réponse et en réduisant considérablement le temps de réaction face aux menaces.

L'optimisation du traitement et de l'analyse des données permet une meilleure corrélation des événements de sécurité, l'automatisation des procédures via des playbooks et une gestion plus efficace des alertes. Enfin, une interface de visualisation avancée offre une représentation claire des indicateurs de sécurité à travers des tableaux de bord dynamiques, facilitant ainsi la prise de décision.

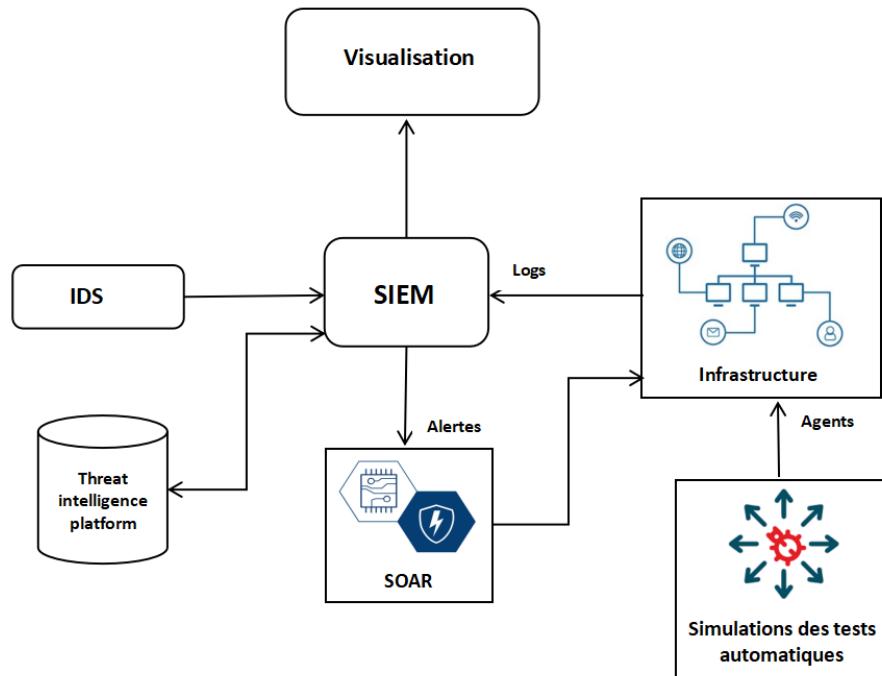


FIGURE 1.3 : Architecture proposée

### 1.2.3 Objectif du projet

L'objectif est de concevoir un SOC moderne en intégrant le SOAR et des simulations des tests d'intrusion automatiques afin d'automatiser la gestion des incidents, réduisant ainsi le temps de réaction et limitant les impacts des attaques. De plus, l'intégration de tests d'intrusion automatisés assurera

une évaluation continue des performances du SOC, garantissant ainsi une adaptation proactive face aux nouvelles menaces.

### 1.2.4 Gestion de projet

#### 1.2.4.1 Méthodologie de travail

[2] Dans cette partie du rapport, nous présenterons la méthodologie adoptée, en mettant en avant les raisons qui ont guidé notre choix de cadre de travail. Par la suite, nous détaillerons le plan de mise en œuvre, en précisant l'organisation des différentes étapes, la répartition des tâches et l'élaboration d'un calendrier adapté pour garantir une progression efficace et maîtrisée.

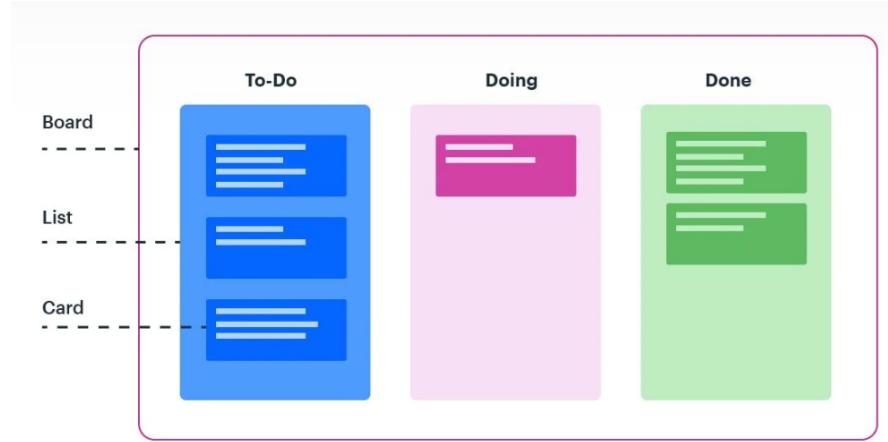
Méthodologie	Description	Avantages	Inconvénients
Cascade	Approche linéaire et séquentielle où chaque phase (conception, développement, test, déploiement) doit être terminée avant de passer à la suivante.	<ul style="list-style-type: none"> <li>- Structure claire et bien définie.</li> <li>- Facilité de gestion et de suivi.</li> <li>- Documentation détaillée.</li> </ul>	<ul style="list-style-type: none"> <li>- Manque de flexibilité en cas de changements.</li> <li>- Risque élevé de non-conformité aux besoins réels si mal définis au départ.</li> <li>- Adaptation difficile aux projets évolutifs.</li> </ul>
Cycle en V	Variante du modèle en cascade où les phases de validation et de vérification sont bien définies et liées à chaque étape du développement.	<ul style="list-style-type: none"> <li>- Meilleure gestion des tests et de la validation.</li> <li>- Approche rigoureuse et bien structurée.</li> <li>- Documentation complète.</li> </ul>	<ul style="list-style-type: none"> <li>- Peu flexible face aux évolutions des besoins.</li> <li>- Détection tardive des erreurs, car les tests interviennent après le développement.</li> </ul>

<b>Circulaire</b>	Approche itérative qui combine les éléments du modèle en cascade et du prototypage, en intégrant une évaluation des risques à chaque cycle.	- Prise en compte des risques dès le début du projet. - Grande flexibilité et adaptation aux besoins évolutifs. - Approche progressive avec tests à chaque itération.	- Coût élevé dû aux nombreuses itérations. - Processus complexe à gérer. - Non adapté aux petits projets à faible budget.
<b>Agile</b>	Approche itérative et incrémentale, favorisant l'adaptation aux changements et l'implication des parties prenantes.	- Grande flexibilité et réactivité. - Amélioration continue grâce aux retours fréquents. - Meilleure collaboration avec les parties prenantes.	- Difficulté à gérer sur des projets avec des exigences strictes. - Moins adapté aux projets nécessitant une documentation exhaustive.

**TABLEAU 1.1 : Les méthodologies des projets**

#### 1.2.4.2 Méthode choisie

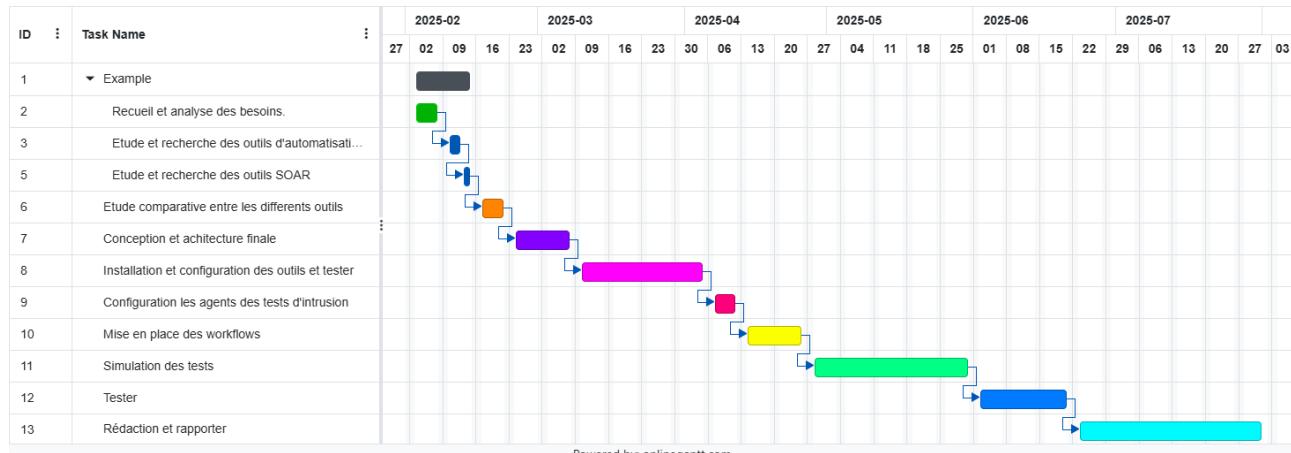
Nous avons choisi la méthode Agile Kanban pour ce projet car elle offre une grande flexibilité, une gestion visuelle efficace et une adaptation continue aux besoins évolutifs. Contrairement aux méthodes classiques comme le Cycle en V ou Scrum, Kanban ne repose pas sur des sprints fixes ni des étapes rigides. Avec Kanban, nous pouvons prioriser les tâches en temps réel, éviter la surcharge de travail et optimiser le flux d'exécution. Grâce à son tableau visuel, il devient plus facile de suivre l'avancement des tâches et d'identifier rapidement les blocages. De plus, il favorise une amélioration continue, permettant d'ajuster les actions au fur et à mesure, ce qui est essentiel dans un projet où les exigences et les défis peuvent évoluer. Voici un tableau Kanban divisé en colonnes qui représentent les différentes étapes du processus, par exemple : "À faire", "En cours" et "Terminé". Chaque tâche est matérialisée par une carte, qui est déplacée à travers ces colonnes au fur et à mesure de son avancement. Cette visualisation permet de suivre l'état des tâches en temps réel et de mieux comprendre le flux de travail.



**FIGURE 1.4** : Processus de Kanban

#### 1.2.4.3 Planning du projet

[3] La planification d'un projet est essentielle pour définir clairement les objectifs et structurer les tâches. Elle permet d'optimiser les ressources, d'éviter les imprévus et d'assurer une meilleure gestion du temps. Sans une bonne planification, le projet risque de rencontrer des retards et un manque de coordination. Une planification efficace garantit ainsi une exécution fluide et un aboutissement réussi du projet. Voici notre planification du projet ci-dessous :



**FIGURE 1.5** : Diagramme de Gantt

## Conclusion

Dans ce chapitre, nous avons défini le cadre général du projet. Tout d'abord, nous avons présenté l'entreprise d'accueil afin de situer le contexte. Ensuite, nous avons analysé l'architecture existante en mettant en évidence ses limites, ce qui nous a conduit à proposer une solution plus adaptée. Enfin, nous avons exposé l'approche méthodologique choisie pour la gestion du projet, en justifiant l'adoption de la méthode Agile Kanban pour assurer une planification efficace et une exécution optimisée des tâches.

# ÉTAT DE L'ART

---

## Plan

<b>Introduction . . . . .</b>	<b>11</b>
<b>1    Centre des opérations de sécurité (SOC) . . . . .</b>	<b>11</b>
<b>2    Système de gestion des informations et des événements de sécurité (SIEM) . . . . .</b>	<b>12</b>
<b>3    Analyse comparative des solutions . . . . .</b>	<b>13</b>
<b>4    Orchestration de la sécurité et d'automatisation de réponse (SOAR) . . . . .</b>	<b>22</b>
<b>5    Émulation d'adversaire (Adversary emulation) . . . . .</b>	<b>31</b>
<b>6    Virtualisation . . . . .</b>	<b>36</b>
<b>7    Conteneurisation . . . . .</b>	<b>39</b>
<b>8    Cloud Computing . . . . .</b>	<b>40</b>
<b>9    Intégration de l'intelligence artificielle (AI) . . . . .</b>	<b>41</b>
<b>10   Systèmes de notification et de messagerie . . . . .</b>	<b>43</b>
<b>11   Architecture envisagée . . . . .</b>	<b>44</b>
<b>Conclusion . . . . .</b>	<b>44</b>

## Introduction

Dans ce chapitre, nous présenterons les éléments clés de notre projet. Nous débuterons par une introduction à la sécurité informatique et au rôle fondamental d'un SOC. Nous aborderons ensuite les concepts de SIEM, de SOAR, ainsi que l'émulation d'adversaire, en détaillant les outils utilisés dans notre solution. Enfin, nous décrirons l'architecture finale de notre solution ainsi que l'environnement de travail dans lequel elle est déployée. Centre des opérations de sécurité.

### 2.1 Centre des opérations de sécurité (SOC)

#### 2.1.1 Définition du SOC

[4] Un SOC (Centre des opérations de sécurité) est une entité dédiée à la cybersécurité, chargée de la surveillance, de la détection, de l'analyse et de la réponse aux menaces en temps réel. Cela regroupe des experts, des processus et des technologies pour assurer la protection des systèmes informatiques d'une organisation. Le SOC réalise une surveillance permanente des réseaux, serveurs, ordinateurs de bureau, bases de données et autres dispositifs afin d'identifier les activités suspectes et de prévenir les cyberattaques. Il fonctionne généralement en continu et peut être soit intégré à l'entreprise, soit externalisé.



**FIGURE 2.1 :** Les éléments constitutifs d'un SOC

### 2.1.2 L'importance du SOC

- **Contrôle continu** : Un SOC assure une surveillance 24h/24 et 7j/7 pour contrer les attaques souvent lancées en dehors des heures de bureau.
- **Visibilité centralisée** : Un SOC fournit une visibilité complète sur une infrastructure réseau complexe et distribuée.
- **Réduction des coûts de cybersécurité** : Un SOC centralisé permet de mutualiser les ressources, d'éviter les redondances et de réduire les coûts liés aux incidents.
- **Une meilleure collaboration** : Le SOC favorise la coordination des équipes de sécurité pour une détection et une réponse rapide aux menaces.

### 2.1.3 Rôles et responsabilités de l'équipe SOC

[4] Généralement, une équipe SOC est constituée d'analystes de différents niveaux et de leurs responsables attitrés :

- **Analyste SOC Niveau 1 – Spécialiste du tri** : Il surveille les alertes, trie les faux positifs, enrichit les données et escalade les incidents qu'il ne peut pas résoudre.
- **Analyste SOC Niveau 2 – Expert en réponse à incident** : Il analyse les incidents complexes, évalue les dégâts, propose des solutions, et coordonne les actions de réponse.
- **Analyste SOC Niveau 3 – Threat Hunter** : Il traque les menaces avancées, identifie les failles inconnues et améliore la détection et la sécurité globale
- **Responsable SOC** : Il gère l'équipe, définit les processus, supervise les incidents, organise la formation, et rend compte à la direction.

## 2.2 Système de gestion des informations et des événements de sécurité (SIEM)

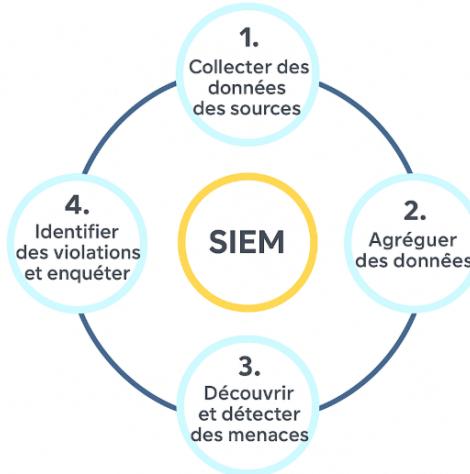
### 2.2.1 Définition

[5] Un élément essentiel d'une cybersécurité efficace est une solution de gestion des informations et des événements de sécurité (SIEM). Ces types de solutions collectent, agrègent et analysent de grands volumes de données provenant d'applications, de dispositifs, de serveurs et d'utilisateurs à l'échelle de l'organisation en temps réel.

### 2.2.2 Les avantages d'un SIEM

[5] Les solutions de gestion des informations et des événements de sécurité offrent des capacités clés de détection des menaces, un reporting en temps réel, des outils de conformité et une analyse des journaux à long terme. Les principaux avantages sont les suivants :

- Efficacité accrue de la sécurité et réponse plus rapide aux menaces.
- Démonstration efficace de la conformité.
- Réduction significative de la complexité.



**FIGURE 2.2 : Processus opérationnel du SIEM**

## 2.3 Analyse comparative des solutions

### 2.3.1 Solutions SIEM

SIEM	Définition	Avantages	Inconvénients
<b>Wazuh</b>	SIEM open source basé sur OSSEC, intégrant la détection d'intrusion, la conformité et l'analyse de logs.	<ul style="list-style-type: none"> <li>- Gratuit et open source.</li> <li>- Intégration native avec ELK stack.</li> <li>- Détection d'intrusion (HIDS) intégrée.</li> <li>- Conformité (PCI-DSS, GDPR...).</li> <li>- Grande communauté et documentation riche.</li> </ul>	<ul style="list-style-type: none"> <li>- Interface plus complexe à prendre en main.</li> <li>- Moins de support commercial officiel.</li> <li>- Moins intuitif que les solutions payantes.</li> </ul>

<b>Splunk</b>	SIEM commercial puissant centré sur l'analyse des données machine et la recherche rapide.	<ul style="list-style-type: none"> <li>- Interface intuitive et visuelle.</li> <li>- Moteur de recherche puissant.</li> <li>- Forte évolutivité.</li> <li>- Nombreux add-ons et intégrations.</li> </ul>	<ul style="list-style-type: none"> <li>- Coût élevé.</li> <li>- Complexité de licence.</li> <li>- Ressources matérielles importantes.</li> </ul>
<b>QRadar</b>	SIEM développé par IBM, centré sur la corrélation des logs, des flux et la Threat Intelligence.	<ul style="list-style-type: none"> <li>- Intégration Threat Intelligence.</li> <li>- Analyse comportementale intégrée.</li> <li>- Corrélation d'événements efficace.</li> </ul>	<ul style="list-style-type: none"> <li>- Complexité de déploiement.</li> <li>- Coût élevé.</li> <li>- Interface un peu datée.</li> </ul>
<b>ArcSight</b>	SIEM proposé par Micro Focus, spécialisé dans les environnements complexes.	<ul style="list-style-type: none"> <li>- Capacité de traitement massive.</li> <li>- Très bon moteur de corrélation logique.</li> <li>- Haut niveau de sécurité.</li> </ul>	<ul style="list-style-type: none"> <li>- Interface complexe à maîtriser.</li> <li>- Déploiement et maintenance lourds.</li> <li>- Moins adapté aux petites structures.</li> </ul>

**TABLEAU 2.1 :** Comparaison des SIEM

[6] Puisque l'entreprise utilise à la fois Wazuh et Splunk comme solutions SIEM, j'ai choisi de travailler sur Wazuh en raison de son caractère open source, mais aussi pour ses capacités de visualisation via son tableau de bord intégré. Selon le tableau 2.1, cette solution répond parfaitement à nos besoins. Wazuh se distingue par sa richesse fonctionnelle, son support communautaire actif et sa facilité de déploiement. Son logo est présenté dans la figure suivante :

**FIGURE 2.3 :** Logo de Wazuh

### 2.3.1.1 Wazuh

- **Fonctionnalité de Wazuh :**

Wazuh est une plateforme de sécurité SI tout-en-un, open source et puissante, conçue pour protéger les organisations contre les menaces cybernétiques. Elle se distingue par plusieurs fonctionnalités essentielles :

- **Détection d'Intrusions (IDS/IPS)** : Wazuh surveille en temps réel les activités du système et les journaux de sécurité, repérant les comportements suspects qui pourraient indiquer une intrusion.
- **Corrélation des Événements** : La plateforme analyse et connecte les informations provenant de diverses sources pour identifier les attaques complexes, permettant une réponse plus efficace.
- **Analyse des Logs** : Wazuh excelle dans l'analyse approfondie des journaux, aidant les utilisateurs à comprendre les activités du système et à réagir rapidement en cas d'incident.
- **Gestion de Vulnérabilités** : En identifiant et évaluant les faiblesses potentielles du système, Wazuh aide à renforcer la sécurité en anticipant les vulnérabilités.
- **Conformité et Rapports** : La plateforme génère des rapports détaillés pour aider les organisations à respecter les normes de sécurité, facilitant ainsi la démonstration de la conformité.
- **Extensibilité et Intégrations** : Wazuh peut être facilement étendu grâce à des modules complémentaires et s'intègre avec d'autres outils de sécurité, offrant une flexibilité d'utilisation.
- **Architecture Évolutive** : Que ce soit dans des environnements de petite ou grande envergure, sur site ou dans le cloud, Wazuh propose une architecture évolutive pour répondre aux besoins variés.
- **Corrélation et Threat Intelligence** : La plateforme utilise des mécanismes avancés de corrélation et s'appuie sur des informations sur les menaces pour améliorer la précision de la détection.

**FIGURE 2.4 :** Fonctionnalités avancées de Wazuh

- **Les composants de Wazuh :**

[7] La plateforme dispose de trois composants principaux :

- **L'indexeur de Wazuh :** L'indexeur de Wazuh est un composant central de Wazuh, il indexe et stocke les alertes générées par le serveur Wazuh, offrant des capacités de recherche et d'analyse de données quasi temps réel, permettant une recherche rapide et efficace des données tout en facilitant l'analyse des alertes générées par le serveur Wazuh.
- **Le serveur Wazuh :** Le serveur Wazuh exerce une analyse approfondie des données émanant des agents (composants qui récoltent les logs depuis les endpoints), traitant ces informations à l'aide de renseignements sur les menaces.  
De plus, il joue un rôle crucial dans la gestion des agents, en permettant des configurations à distance, une fonctionnalité essentielle pour garantir une sécurité proactive et optimale.
- **Le tableau de bord (Wazuh Dashboard) :** Le tableau de bord [7] Wazuh constitue l'interface utilisateur web dédiée à la visualisation, à l'analyse et à la gestion des données. Il offre des tableaux de bord spécifiques pour la conformité réglementaire, les vulnérabilités, l'intégrité des fichiers, l'évaluation de la configuration, ainsi que pour les événements de l'infrastructure cloud, entre autres fonctionnalités.

**W. indexer**

L'indexeur Wazuh est un moteur de recherche et d'analyse en texte intégral hautement évolutif. Ce composant central indexe et stocke les alertes générées par le serveur Wazuh.

**W. server**

Le serveur Wazuh analyse les données reçues des agents et les traite à l'aide de renseignements sur les menaces. Un seul serveur peut analyser les données de milliers d'agents et évoluer lorsqu'il est configuré en cluster. Il est également utilisé pour gérer les agents, en les configurant à distance si nécessaire.

**W. dashboard**

Le tableau de bord Wazuh est l'interface utilisateur Web pour la visualisation, l'analyse et la gestion des données. Il comprend des tableaux de bord pour la conformité réglementaire, les vulnérabilités, l'intégrité des fichiers, l'évaluation de la configuration, les événements de

**FIGURE 2.5 :** Les composants de Wazuh

- **Les agents Wazuh (Wazuh agents) :**

[7] Les agents Wazuh sont des composants stratégiques déployés sur les endpoints d'un réseau informatique. Leur rôle central consiste à collecter et à surveiller de manière proactive les données, notamment les journaux, sur les systèmes où ils sont installés. En analysant ces données au niveau central via le serveur Wazuh, les agents assurent une corrélation avancée, une détection d'anomalies et la génération d'alertes en cas d'activités suspectes.

**W.agent**

Les agents Wazuh sont installés sur des points de terminaison tels que des ordinateurs portables, des ordinateurs de bureau, des serveurs, des instances cloud ou des machines virtuelles. Ils offrent des capacités de prévention, de détection et de réponse aux menaces.



**FIGURE 2.6 :** Les agents Wazuh

- **Architecture Wazuh :**

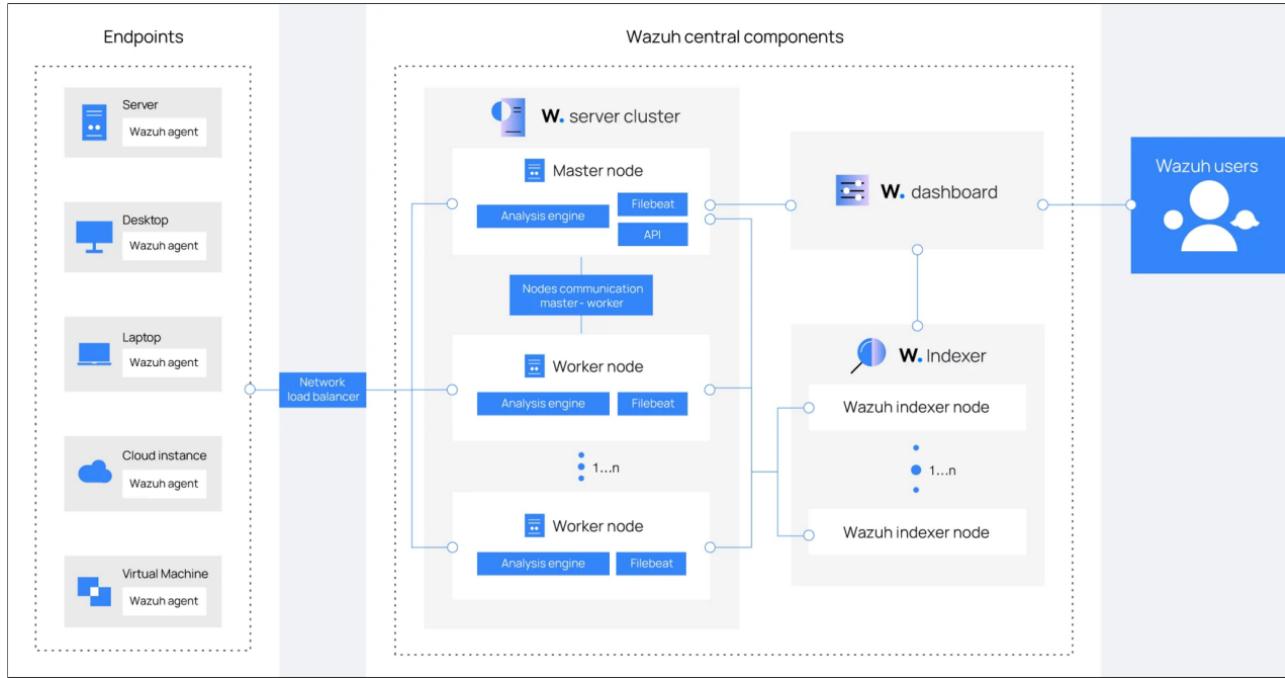


FIGURE 2.7 : Architecture globale Wazuh

### 2.3.2 Solutions de détection d'intrusions

#### 2.3.2.1 Solutions HIDS

[8] Le système de détection d'intrusion basé sur l'hôte (HIDS) est un logiciel de sécurité conçu pour surveiller et analyser les activités d'un hôte individuel ou d'un point d'extrémité afin de détecter et de répondre à des violations potentielles de la sécurité. Il examine les journaux système, l'intégrité des fichiers, les activités des utilisateurs et les connexions réseau, afin d'identifier les comportements suspects ou les signes d'un accès non autorisé ou d'une altération.

Outil	Définition	Avantages	Inconvénients
<b>Wazuh agent</b>	Plateforme open source HIDS basée sur OSSEC, fournissant la surveillance des fichiers, la détection d'anomalies et la conformité.	<ul style="list-style-type: none"> <li>- Surveillance complète des fichiers, logs et intégrité système.</li> <li>- Intégration native avec ELK / OpenSearch.</li> <li>- Capacités avancées de détection et alerting.</li> <li>- Grande communauté et support actif.</li> </ul>	<ul style="list-style-type: none"> <li>- Installation et configuration complexes pour débutants.</li> <li>- Consommation de ressources selon la taille du parc.</li> </ul>

<b>OSSEC</b>	Système HIDS open source pour la surveillance de l'intégrité des fichiers, analyse des logs, et détection d'intrusions côté hôte.	<ul style="list-style-type: none"> <li>- Léger et facile à déployer.</li> <li>- Intégration avec Wazuh possible.</li> <li>- Mature et éprouvé.</li> </ul>	<ul style="list-style-type: none"> <li>- Interface utilisateur basique.</li> <li>- Moins axé sur la détection comportementale avancée.</li> </ul>
<b>Suricata</b>	Principalement un IDS réseau (NIDS), mais aussi utilisé en contexte HIDS via la journalisation locale et intégration avec Wazuh pour une analyse approfondie côté hôte.	<ul style="list-style-type: none"> <li>- Analyse multi-thread du trafic et journalisation locale.</li> <li>- Sortie JSON facilitant l'intégration avec Wazuh/OpenSearch.</li> <li>- Supporte protocoles récents et détection fine.</li> </ul>	<ul style="list-style-type: none"> <li>- Pas un HIDS natif, nécessite une architecture complémentaire.</li> <li>- Configuration plus complexe que solutions purement HIDS.</li> </ul>
<b>AIDE</b>	Outil HIDS open source axé sur la vérification de l'intégrité des fichiers par comparaison avec une base de données initiale.	<ul style="list-style-type: none"> <li>- Simple et efficace pour la surveillance d'intégrité.</li> <li>- Léger, adapté aux systèmes embarqués.</li> </ul>	<ul style="list-style-type: none"> <li>- Pas de détection en temps réel, analyses manuelles.</li> <li>- Moins complet que Wazuh ou OSSEC.</li> </ul>
<b>Falco</b>	Système HIDS open source orienté détection en temps réel des comportements suspects au niveau noyau Linux, utilisé en cloud natif et conteneurs.	<ul style="list-style-type: none"> <li>- Très efficace pour la surveillance runtime.</li> <li>- Intégration facile avec Kubernetes et Docker.</li> <li>- Détection basée sur règles flexibles.</li> <li>- Idéal pour environnements cloud natifs.</li> </ul>	<ul style="list-style-type: none"> <li>- Limité aux systèmes Linux.</li> <li>- Courbe d'apprentissage pour règles personnalisées.</li> </ul>

**TABLEAU 2.2 :** Comparaison des outils HIDS

### 2.3.2.2 Solutions NIDS

[9] Un système de détection d'intrusion basé sur le réseau (NIDS) est une solution de sécurité conçue pour surveiller et analyser le trafic réseau afin de détecter d'éventuelles failles de sécurité ou activités malveillantes. Il fonctionne comme un système de surveillance passif, observant en temps réel les paquets de données qui passent par le réseau. Le NIDS permet d'identifier et de répondre à diverses cybermenaces, telles que les logiciels malveillants, les tentatives d'accès non autorisé et les schémas suspects, afin d'améliorer la sécurité globale du réseau.

Outil	Définition	Avantages	Inconvénients
Suricata	NIDS open source performant capable d'analyser le trafic réseau en temps réel, détectant les intrusions, exploits et malwares.	<ul style="list-style-type: none"> <li>- Multi-threading natif pour une haute performance.</li> <li>- Supporte l'analyse de protocoles modernes (HTTP/2, TLS 1.3, etc.).</li> <li>- Génère des logs en JSON facilitant l'intégration avec SIEMs comme Wazuh et OpenSearch.</li> <li>- Détection précise grâce à des règles Snort compatibles et des signatures spécifiques.</li> <li>- Peut faire de la détection basée sur le comportement.</li> </ul>	<ul style="list-style-type: none"> <li>- Configuration complexe pour les débutants.</li> <li>- Besoin de ressources importantes selon le volume de trafic.</li> </ul>

<b>Snort</b>	NIDS open source historique, largement utilisé pour la détection d'intrusions réseau via des signatures.	<ul style="list-style-type: none"> <li>- Large base de règles et communauté active.</li> <li>- Documentation abondante.</li> <li>- Relativement simple à déployer.</li> </ul>	<ul style="list-style-type: none"> <li>- Monothread, donc moins performant sur gros trafic.</li> <li>- Moins adapté aux protocoles récents.</li> </ul>
<b>Zeek</b>	NIDS orienté analyse comportementale et protocolaire, centré sur la compréhension des flux réseau.	<ul style="list-style-type: none"> <li>- Excellente visibilité sur le trafic réseau.</li> <li>- Puissante capacité d'analyse comportementale et scripting.</li> <li>- Utile pour la détection d'attaques avancées.</li> </ul>	<ul style="list-style-type: none"> <li>- Courbe d'apprentissage élevée.</li> <li>- Moins orienté signature traditionnelle.</li> </ul>
<b>Security Onion</b>	Distribution Linux intégrée combinant plusieurs outils NIDS comme Suricata, Zeek et Wazuh pour une solution complète.	<ul style="list-style-type: none"> <li>- Solution clé en main avec intégration de multiples outils.</li> <li>- Interface unifiée pour la gestion et l'analyse.</li> <li>- Bon support communautaire.</li> </ul>	<ul style="list-style-type: none"> <li>- Poids lourd, nécessite des ressources matérielles conséquentes.</li> <li>- Complexité d'administration plus élevée.</li> </ul>

**TABLEAU 2.3 :** Comparaison des NIDS

[10] Puisque l'entreprise utilise Suricata comme NIDS, et suite à une analyse comparative des outils HIDS et NIDS, l'agent Wazuh a été déployé en tant que HIDS sur les endpoints, garantissant une surveillance fine et en temps réel des événements système. Cette solution est renforcée par l'intégration des logs générés par Suricata, offrant ainsi une double capacité de détection, à la fois réseau (NIDS) et hôte (HIDS), pour une couverture de sécurité complète et cohérente, Son logo est illustré par la figure suivante :



**FIGURE 2.8 : Logo de Suricata**

[11] Enfin, Falco est intégré pour assurer la détection des comportements suspects dans les environnements cloud natifs et conteneurisés, notamment Kubernetes, renforçant ainsi la protection dans les infrastructures modernes et dynamiques. La figure 2.9 représente le logo de Falco.



**FIGURE 2.9 : Logo de Falco**

## 2.4 Orchestration de la sécurité et d'automatisation de réponse (SOAR)

### 2.4.1 Définition

[12] Le SOAR est un type de solution logicielle qui permet aux équipes de sécurité d'intégrer et de coordonner des outils de sécurité distincts, d'automatiser les tâches répétitives et de rationaliser les workflows de réponse aux incidents et aux menaces.

### 2.4.2 Le fonctionnement de SOAR

#### 2.4.2.1 Orchestration de la sécurité

[12] L'orchestration de la sécurité coordonne de façon automatique une série d'actions de sécurité interdépendantes, dont l'investigation, la réponse et la résolution, sur une infrastructure complexe et unique. Cette fonctionnalité met au diapason l'ensemble des outils (de sécurité ou autres), que ce soit en automatisant les tâches de différents produits et workflows ou en notifiant manuellement les agents des incidents qui nécessitent leur attention.

L'orchestration de la sécurité offre de nombreux avantages :

- **Contextualisation des incidents de sécurité :** Un outil d'orchestration de la sécurité agrège les données provenant de plusieurs sources pour offrir des analyses plus poussées. Vos équipes obtiennent ainsi une visibilité complète sur l'ensemble de l'environnement.
- **Investigations approfondies :** Les analystes de sécurité peuvent s'affranchir de la gestion des alertes pour se concentrer sur l'investigation des causes racines. Les outils d'orchestration proposent aussi des visuels (graphiques, chronologies, tableaux de bord...) hautement interactifs et intuitifs, qui peuvent s'avérer très utiles au cours de l'investigation.
- **Amélioration de la collaboration :** Analystes, managers, CTO, dirigeants, équipe juridique, ressources humaines... d'autres collaborateurs doivent parfois intervenir dans les processus de réponse à incident. L'orchestration de la sécurité met à la disposition de tous les acteurs concernés l'ensemble des données nécessaires afin de faciliter la collaboration, le dépannage et la résolution des problèmes.

#### 2.4.2.2 Automatisation de la sécurité

[12] L'automatisation de la sécurité désigne l'exécution automatique d'actions de sécurité visant à détecter, investiguer et neutraliser les cybermenaces sans intervention humaine. Cette fonctionnalité fait gagner un temps précieux au SOC, qui n'a plus besoin de trier et de traiter manuellement chaque alerte. L'automatisation de la sécurité peut :

- Déetecter les menaces au sein de votre environnement.
- Trier les menaces.
- Déterminer si une intervention est nécessaire.
- Endiguer et résoudre le problème.

Ces tâches sont exécutées en quelques secondes, sans aucune intervention humaine. Les analystes de sécurité ne sont plus soumis à des workflows chronophages (multiples étapes et instructions, suivi du processus décisionnel) pour investiguer l'événement et déterminer s'il s'agit d'un incident réel. Libérés des tâches répétitives, ils peuvent se concentrer sur les activités stratégiques.

#### 2.4.2.3 Réponse aux incidents

[12] L'orchestration et l'automatisation constituent la base de la fonction de réponse d'un système SOAR. Avec SOAR, une organisation peut gérer, planifier et coordonner la façon dont elle réagit à une menace de sécurité. La fonction d'automatisation de SOAR élimine le risque d'erreur humaine. Cela rend les réponses plus précises et réduit le temps nécessaire pour résoudre les problèmes de sécurité.

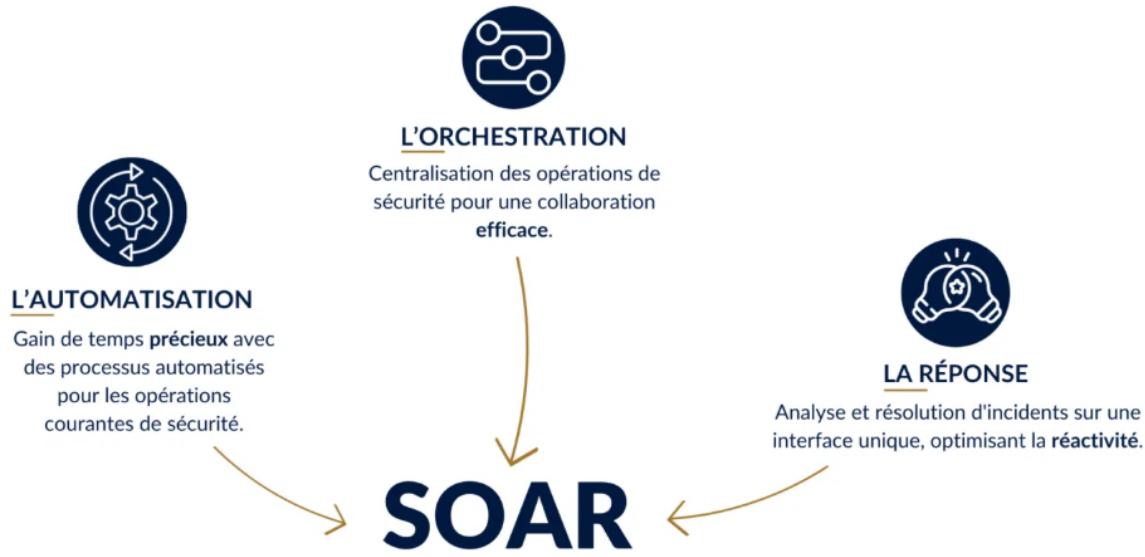


FIGURE 2.10 : Fonctionnement de SOAR

### 2.4.3 Cas d'usage du SOAR

- **Réponse aux incidents** : Si un incident de sécurité s'est produit, une réponse coordonnée est nécessaire pour atténuer l'impact de la violation.
- **Gestion des cas** : Lorsqu'une menace a été identifiée, elle déclenche un cas. Le nombre de cas peut rapidement s'accumuler, et une solution SOAR performante aidera les équipes à établir des priorités et à réagir de manière efficace.
- **Gestion de la vulnérabilité** : Il est essentiel de comprendre où se situe une organisation en ce qui concerne la vulnérabilité globale de la sécurité. Les solutions SOAR peuvent aider à fournir une perspective plus objective sur l'évaluation des risques - ce dont tout RSSI (responsable de la sécurité de l'information) a besoin pour faire son travail.
- **Chasse aux menaces** : La recherche proactive des menaces au sein de l'environnement informatique d'une entreprise. Une pratique mature de chasse aux menaces nécessite un moteur rapide pour interroger de vastes quantités de données.

### 2.4.4 Analyse comparative des outils SOAR

#### 2.4.4.1 Outils de gestion des incidents de sécurité

[13] Les outils de gestion des incidents ont pour objectif de centraliser et automatiser la collecte et l'analyse des alertes, d'orchestrer les actions de réponse à travers différents systèmes de sécurité, et d'améliorer la coordination entre les équipes. Ils permettent ainsi de réduire le temps de détection et de réaction, tout en assurant une traçabilité complète et une gestion efficace des incidents.

Outil	Définition	Avantages	Inconvénients
<b>TheHive</b>	Plateforme open source de gestion collaborative des incidents, conçue pour une réponse rapide et efficace.	<ul style="list-style-type: none"> <li>- Interface intuitive et collaborative.</li> <li>- Forte intégration avec Cortex pour l'analyse automatisée.</li> <li>- Open source et hautement personnalisable.</li> <li>- Bonne gestion des cas et workflows.</li> </ul>	<ul style="list-style-type: none"> <li>- Nécessite une configuration initiale.</li> <li>- Courbe d'apprentissage pour les débutants.</li> </ul>
<b>Splunk SOAR</b>	Solution commerciale de SOAR pour automatiser la réponse aux incidents et orchestrer les outils de sécurité.	<ul style="list-style-type: none"> <li>- Très puissante et riche en fonctionnalités.</li> <li>- Support commercial solide.</li> <li>- Large intégration d'outils et sources de données.</li> </ul>	<ul style="list-style-type: none"> <li>- Coût élevé.</li> <li>- Complexité de déploiement et gestion.</li> </ul>
<b>IBM Resilient</b>	Plateforme commerciale de gestion des incidents et orchestration SOAR, adaptée aux grandes entreprises.	<ul style="list-style-type: none"> <li>- Robuste et fiable.</li> <li>- Nombreux playbooks prédéfinis.</li> <li>- Support et formations disponibles.</li> </ul>	<ul style="list-style-type: none"> <li>- Prix élevé.</li> <li>- Moins flexible pour les petites structures.</li> </ul>
<b>DFIR-IRIS</b>	Outil open source focalisé sur la gestion et l'analyse des incidents de sécurité.	<ul style="list-style-type: none"> <li>- Gratuit et open source.</li> <li>- Focus sur l'analyse forensique.</li> <li>- Personnalisable.</li> </ul>	<ul style="list-style-type: none"> <li>- Interface moins intuitive.</li> <li>- Moins d'automatisation intégrée que TheHive.</li> </ul>

**TABLEAU 2.4 :** Comparaison des outils de gestion des incidents

[14] Suite à une évaluation comparative détaillée, il apparaît clairement que TheHive est la solution la mieux adaptée à nos exigences. Sa grande flexibilité et son interface conviviale simplifient la gestion des incidents tout en s'intégrant harmonieusement à notre infrastructure actuelle. Cette

plateforme offre ainsi une réponse solide et performante. Le logo de TheHive est présenté à la figure ci-dessous :



**FIGURE 2.11 : Logo de TheHive**

#### 2.4.4.2 Analyseurs d'observables

Un analyseur est un outil utilisé pour examiner des indicateurs de compromission (IoCs) tels que les adresses IP, fichiers, URLs ou hachages. Il permet d'identifier des comportements malveillants ou des menaces potentielles à partir de ces données.

Outil	Définition	Avantages	Inconvénients
<b>Cortex</b>	Plateforme open source permettant l'automatisation de l'analyse d'indicateurs de compromission (IoCs) via des analyseurs et des observables.	<ul style="list-style-type: none"> <li>- Intégration native avec TheHive.</li> <li>- Plus de 100 analyseurs (VirusTotal, MalwareBazaar, Shodan, etc.).</li> <li>- API RESTful facile à intégrer.</li> <li>- Traitement automatisé des IoCs.</li> <li>- Open source, flexible et personnalisable.</li> </ul>	<ul style="list-style-type: none"> <li>- Requiert une configuration initiale des analyseurs.</li> <li>- Peut dépendre de services tiers pour certaines analyses.</li> </ul>
<b>VirusTotal</b>	Service en ligne qui analyse les fichiers et URL suspectes via plusieurs antivirus et moteurs de détection.	<ul style="list-style-type: none"> <li>- Multi-moteur de détection.</li> <li>- Facile à utiliser.</li> <li>- Accès API pour automatisation.</li> </ul>	<ul style="list-style-type: none"> <li>- Limité dans sa version gratuite.</li> <li>- Ne fournit pas de corrélation ni enrichissement avancé.</li> </ul>

<b>Hybrid Analysis</b>	Plateforme d'analyse dynamique de malwares proposée par CrowdStrike.	- Analyse dynamique détaillée. - Visualisation du comportement malveillant.	- Nécessite l'envoi de fichiers. - Pas d'automatisation complète sans abonnement.
<b>Joe Sandbox</b>	Solution avancée d'analyse de malwares avec sandbox pour l'analyse comportementale.	- Analyse statique et dynamique poussée. - Interface graphique complète. - Supporte de nombreux OS (Windows, Android, etc.).	- Licence payante coûteuse. - Usage limité dans la version gratuite.

**TABLEAU 2.5 :** Comparaison des outils d'analyseur

[14] Le choix de Cortex s'impose naturellement grâce à son intégration native avec TheHive, ce qui facilite l'automatisation de l'enrichissement des incidents. Il dispose également d'un large catalogue d'analyseurs permettant d'examiner efficacement divers types d'observables. Cette combinaison renforce la rapidité et la précision dans le traitement des alertes. La figure suivante présente le logo de Cortex :

**FIGURE 2.12 :** Logo de Cortex

#### 2.4.4.3 Plateformes de Cyber Threat Intelligence (CTI)

[15] Les plateformes de CTI permettent de centraliser et d'exploiter des données sur les menaces afin d'identifier, comprendre et prévenir les attaques informatiques. Elles analysent des sources variées pour fournir des renseignements exploitables. Ces outils renforcent la détection, la réponse et la stratégie de cybersécurité.

Outil	Définition	Avantages	Inconvénients
MISP	Plateforme open source dédiée au partage d'informations sur les menaces entre organisations.	<ul style="list-style-type: none"> <li>- Favorise le partage communautaire.</li> <li>- Grande communauté active.</li> <li>- Supporte les formats standards (STIX, TAXII...).</li> </ul>	<ul style="list-style-type: none"> <li>- Interface parfois complexe.</li> <li>- Consommation élevée de mémoire et de ressources.</li> <li>- Nécessite une configuration poussée pour un usage optimal.</li> </ul>
OpenCTI	Plateforme open source de CTI centrée sur la modélisation des connaissances sur les menaces en s'appuyant sur le standard STIX.	<ul style="list-style-type: none"> <li>- Très bonne intégration avec MISP et TheHive.</li> <li>- Visualisation graphique des relations entre entités.</li> <li>- API GraphQL performante.</li> </ul>	<ul style="list-style-type: none"> <li>- Déploiement initial complexe.</li> <li>- Utilisation intensive de ressources</li> </ul>
Yeti	Plateforme open source de gestion de renseignements sur les menaces, permettant de collecter, stocker et analyser les artefacts malveillants.	<ul style="list-style-type: none"> <li>- Léger en ressources, adapté aux environnements limités.</li> <li>- Interface simple et intuitive.</li> <li>- API RESTful pour intégration facile (TheHive, Cortex...).</li> <li>- Bonne organisation des entités CTI (TTPs, observables, groupes APT...).</li> <li>- Open source sans licence commerciale.</li> </ul>	<ul style="list-style-type: none"> <li>- Moins de fonctionnalités avancées que OpenCTI.</li> <li>- Moins actif en termes de mises à jour.</li> <li>- Interface moins moderne.</li> </ul>

<b>ThreatQ</b>	Solution commerciale de CTI permettant d'automatiser, d'analyser et de visualiser les renseignements de menaces.	- Intégration avancée avec SOAR/SIEM. - Visualisation enrichie et workflows automatisés.	- Coût élevé. - Solution propriétaire.
----------------	--	---	---

**TABLEAU 2.6** : Comparaison des CTI

[16] Le choix de YETI (Your Everyday Threat Intelligence) comme plateforme CTI repose sur sa légèreté, sa simplicité de déploiement et sa faible consommation de ressources. Il permet une gestion efficace des informations sur les menaces avec une interface intuitive et une API performante. Cette solution est idéale pour les environnements nécessitant rapidité et optimisation des ressources. La figure ci-dessous illustre le logo de Yeti :

**FIGURE 2.13** : Logo de Yeti

#### 2.4.4.4 Solutions d'orchestration et d'automatisation des workflows

Les plateformes d'orchestration et d'automatisation sont des solutions logicielles qui permettent de coordonner, automatiser et optimiser les processus de gestion des incidents de sécurité. Elles facilitent l'intégration de multiples outils, l'exécution automatique de tâches répétitives, et accélèrent la réponse aux menaces en centralisant les workflows.

Outil	Définition	Avantages	Inconvénients
<b>Shuffle</b>	Plateforme open source d'orchestration et d'automatisation dédiée à la gestion des incidents de sécurité.	<ul style="list-style-type: none"> <li>- Interface intuitive et facile à prendre en main.</li> <li>- Large bibliothèque d'intégrations (plugins).</li> <li>- Forte communauté open source.</li> <li>- Fonctionnalités avancées pour la création de playbooks.</li> </ul>	<ul style="list-style-type: none"> <li>- Moins mature que certaines solutions commerciales.</li> <li>- Documentation parfois incomplète.</li> </ul>
<b>Tines</b>	Plateforme no-code/low-code d'automatisation de la sécurité, adaptée aux équipes SOC pour créer des workflows sans coder.	<ul style="list-style-type: none"> <li>- Interface utilisateur simple et visuelle.</li> <li>- Fort accent sur la sécurité et la confidentialité.</li> <li>- Intégration facile avec des outils du SOC.</li> </ul>	<ul style="list-style-type: none"> <li>- Fonctionnalités avancées réservées aux offres payantes.</li> <li>- Moins personnalisable que les solutions open source.</li> </ul>
<b>Swimlane</b>	Plateforme commerciale d'orchestration SOAR pour la gestion automatisée des réponses aux incidents.	<ul style="list-style-type: none"> <li>- Solution robuste et complète.</li> <li>- Fonctionnalités avancées de reporting et de gestion des cas.</li> <li>- Support et maintenance professionnels.</li> </ul>	<ul style="list-style-type: none"> <li>- Coût élevé.</li> <li>- Complexité à déployer et administrer.</li> </ul>

**TABLEAU 2.7 :** Comparaison des plateformes d'orchestration et d'automatisation

[17] Parmi les différentes plateformes d'orchestration, Shuffle se distingue par sa légèreté, sa simplicité de déploiement et son orientation open source. Il offre une interface intuitive pour concevoir des workflows automatisés, tout en assurant une intégration fluide avec divers outils de cybersécurité. Ces avantages en font une solution idéale et efficace pour automatiser les réponses aux incidents dans notre environnement. La figure 2.14 représente son logo.



FIGURE 2.14 : Logo de Shuffle

- **Mode de fonctionnement de Shuffle :**

- **Connecteurs (Apps)** : Shuffle intègre différents outils à l'aide de connecteurs (appelés apps). Ces connecteurs interagissent avec les APIs des outils.
- **Workflows visuels** : L'utilisateur crée des workflows graphiques en glissant-déposant des blocs (actions) pour définir des scénarios de réponse ou d'automatisation.
- **Webhooks et Triggers** : Shuffle peut être déclenché automatiquement par un webhook.
- **Exécution automatisée** : Lorsqu'un événement se produit, Shuffle exécute le workflow correspondant en appelant les APIs des outils définis dans le flux.

## 2.5 Émulation d'adversaire (Adversary emulation)

[18] L'émulation des adversaires est une méthode d'évaluation de la cybersécurité qui vise à tester les contrôles de sécurité d'une organisation par rapport aux tactiques, techniques et procédures (TTP) utilisées par les acteurs de la menace qui représentent le plus grand risque pour son secteur d'activité. Cette stratégie consiste à comprendre les derniers logiciels malveillants et les campagnes d'attaque des adversaires, puis à les simuler dans un environnement contrôlé afin d'évaluer la posture de sécurité de l'organisation.

### 2.5.1 Renseignement sur les menaces

[18] Le renseignement sur les menaces est la pratique qui consiste à collecter, analyser et appliquer les connaissances sur les menaces et les adversaires afin d'améliorer les défenses de cybersécurité d'une organisation. Il fournit des informations exploitables sur les tactiques, techniques et procédures (TTP) utilisées par les acteurs malveillants, ce qui permet de prendre des mesures proactives contre les attaques potentielles. Les tactiques, techniques et procédures (TTP) constituent la base de la compréhension du comportement des adversaires sur le site.

- **Les tactiques** : font référence aux buts ou objectifs généraux d'un attaquant à un stade spécifique d'une opération, comme l'obtention d'un accès ou l'exfiltration de données.

- **Les techniques** : décrivent les méthodes utilisées pour atteindre ces objectifs, comme le spearphishing pour l'accès initial ou le credential dumping pour l'escalade des priviléges.
- **Les procédures** : représentent les mises en œuvre spécifiques de ces techniques, adaptées aux outils et aux environnements d'un adversaire particulier.

[18] En analysant les TTP, les organisations peuvent anticiper le comportement des attaquants, identifier les vulnérabilités et mettre en œuvre des contre-mesures efficaces. Ces informations sont souvent documentées dans des cadres tels que MITRE ATT&CK, qui cataloguent systématiquement les comportements des adversaires afin d'aider les organisations à cartographier les schémas d'attaque et à améliorer les défenses.

Un autre concept clé du renseignement sur les menaces est celui des indicateurs de compromission (IOC), qui sont des artefacts observables suggérant qu'un système a pu être violé. Parmi les exemples d'IOC figurent les hachages de fichiers, les adresses IP, les noms de domaine, les URL, les modifications du registre et les noms de processus inhabituels. Si les IOC sont utiles pour identifier les menaces actives, ils sont souvent éphémères, car les attaquants peuvent facilement les modifier pour échapper à la détection. Pour remédier à ce problème, la pyramide de la douleur (Pyramid Of Pain) de la figure 1.16 classe les IOC en fonction du niveau de difficulté qu'ils posent aux attaquants pour les modifier. À la base de la pyramide se trouvent des artefacts simples comme les hachages de fichiers, qui sont faciles à modifier, tandis que les TTP se trouvent au sommet, car ils sont beaucoup plus difficiles à modifier. En se concentrant sur les TTP, les défenseurs peuvent perturber les stratégies des adversaires, les obligeant à consacrer beaucoup de temps et de ressources pour s'adapter.

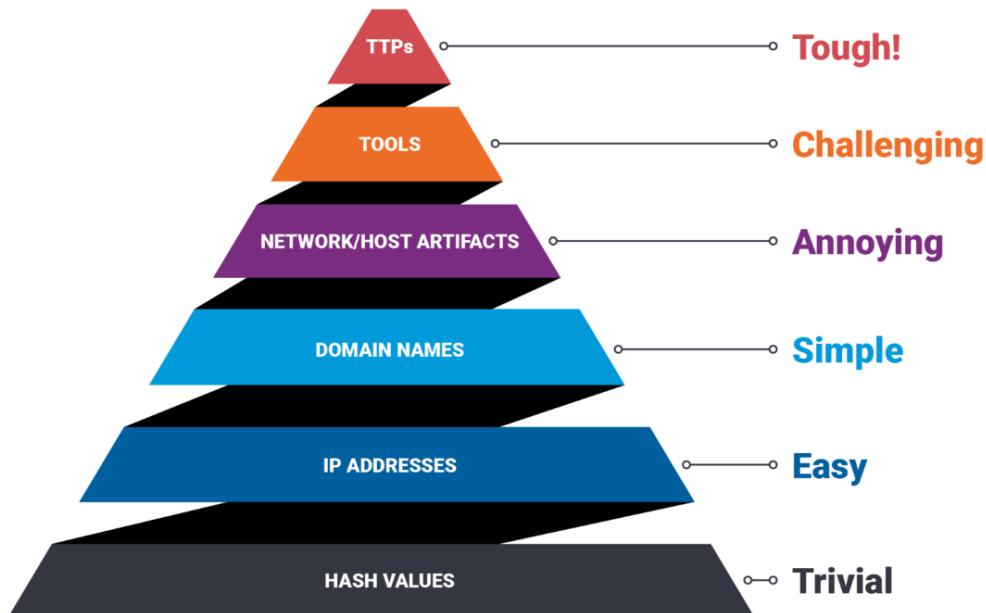


FIGURE 2.15 : Pyramid Of Pain

Les renseignements sur les menaces, lorsqu'ils sont associés à une compréhension des IOC et des

TPP, fournissent une vue d'ensemble du paysage des menaces, permettant aux organisations de contrer les adversaires de manière proactive et de mettre en place des systèmes de sécurité plus résistants.

### 2.5.2 Simulation des attaques

#### 2.5.2.1 Analyse comparative des outils d'émulation d'adversaire

Outil	Définition	Avantages	Inconvénients
CALDERA	Plateforme d'émulation d'adversaire open source développée par le MITRE, utilisant le framework MITRE ATT&CK.	<ul style="list-style-type: none"> <li>- Automatisation complète des campagnes d'attaque.</li> <li>- Interface web intuitive.</li> <li>- Agents multiplateformes (Sandcat).</li> <li>- Intégration facile de plugins personnalisés.</li> </ul>	<ul style="list-style-type: none"> <li>- Configuration initiale technique.</li> <li>- Moins adaptée aux tests 100% manuels.</li> </ul>
Atomic Red Team	Framework open source fournissant des scripts pour tester des techniques MITRE ATT&CK sur différents environnements.	<ul style="list-style-type: none"> <li>- Facile à utiliser et à déployer.</li> <li>- Large base de tests disponibles.</li> <li>- Compatible avec plusieurs OS.</li> </ul>	<ul style="list-style-type: none"> <li>- Pas d'interface graphique.</li> <li>- Pas d'agent, pas d'automatisation native.</li> </ul>
Red Team Toolkit	Ensemble d'outils manuels utilisés pour simuler des attaques réelles lors d'exercices Red Team.	<ul style="list-style-type: none"> <li>- Grande flexibilité.</li> <li>- Contrôle total sur les actions.</li> </ul>	<ul style="list-style-type: none"> <li>- Fortement dépendant de l'expertise humaine.</li> <li>- Pas d'automatisation, pas de normalisation.</li> </ul>

<b>Infection Monkey</b>	Outil open source de simulation d'attaque axé sur la propagation et la détection des failles réseau.	- Facile à déployer. - Visualisation graphique des mouvements latéraux. - Bon pour tester la segmentation réseau.	- Moins axé ATT&CK. - Moins flexible pour scénarios avancés.
-------------------------	--	---	---

**TABLEAU 2.8 :** Comparaison des outils d'émulation d'adversaire

[19] Parmi les outils d'émulation d'adversaire présentés, CALDERA se distingue comme le choix le plus pertinent pour une utilisation complète et automatisée développé par le MITRE, conçu pour automatiser la simulation d'attaques en s'appuyant sur le framework MITRE ATT&CK. Il permet de reproduire de manière réaliste les tactiques et techniques utilisées par les cybercriminels, facilitant ainsi l'évaluation de la posture de sécurité des organisations. Grâce à son interface web intuitive et à ses agents multiplateformes, elle offre une solution flexible et puissante pour tester et renforcer les défenses sans nécessiter une expertise manuelle approfondie. La figure suivante présente son logo :

**FIGURE 2.16 :** Logo de Caldera

### 2.5.3 Caldera

#### 2.5.3.1 Définition

[19] Caldera est une plateforme open-source développée par MITRE qui permet de simuler des attaques informatiques automatisées. Elle utilise des agents déployés sur les machines cibles pour exécuter des techniques basées sur le framework MITRE ATT&CK. Son objectif est de tester et renforcer la sécurité des systèmes informatiques.

#### 2.5.3.2 Mode de fonctionnement de Caldera

[19] Caldera fonctionne comme une plateforme de simulation d'attaques automatisées. Elle permet aux équipes de sécurité de tester la défense d'un système en simulant le comportement de véritables attaquants, selon le modèle **Red Team vs Blue Team**.

- **Red Team – Simuler l'attaquant** L'équipe rouge utilise Caldera pour lancer des attaques simulées dans le but d'évaluer la robustesse de la défense. Elle se concentre sur la compromission des systèmes cibles via des campagnes d'attaque automatisées.

- **Déploiement des agents** : Les agents sont des programmes installés sur des machines cibles. Ils se connectent régulièrement au serveur Caldera pour recevoir des instructions. Chaque agent possède une "empreinte" unique (appelée *paw*), qui permet de l'identifier. Il existe plusieurs types d'agents, chacun avec ses propres méthodes de communication et de compatibilité, par exemple :

- \* **Sandcat (en Go)** : communique via HTTP, GitHub GIST, DNS, etc.
- \* **Manx** : fonctionne en ligne de commande via TCP (reverse shell).
- \* **Ragdoll** : agent Python qui utilise une interface HTML.

- **Les capacités (Abilities)** : Les abilities sont des actions ou techniques spécifiques (basées sur le framework ATT&CK de MITRE) que Caldera peut exécuter sur un agent. Une ability contient :

- \* Les commandes à exécuter.
- \* La plateforme cible (Windows, Linux, etc.).
- \* Le type d'exécution (ex. PowerShell, Bash).
- \* Des fichiers ou charges utiles nécessaires.
- \* Un parser pour analyser les résultats et en extraire des informations utiles (facts).

- **Profils d'adversaire** : Un *adversary profile* est un ensemble structuré d'abilities organisées selon les tactiques et techniques utilisées par des attaquants réels. Ces profils permettent de simuler des comportements complexes d'APT ou de groupes malveillants.

- **Opérations** : Une opération est une campagne de simulation dans laquelle Caldera exécute automatiquement les abilities définies dans un profil d'adversaire sur un ou plusieurs agents cibles.

#### • **Blue Team – Défendre et détecter**

L'équipe bleue est chargée de la surveillance, de la détection et de la réponse aux attaques simulées. Elle utilise les outils de sécurité pour identifier les actions malveillantes effectuées par les agents Caldera.

- Surveiller les comportements suspects générés par les agents.
- Corréler les événements dans les journaux systèmes et les alertes avec les techniques MITRE ATT&CK.

- Évaluer les capacités de détection, le temps de réponse, et l'efficacité des solutions de sécurité (SIEM, EDR, HIDS, etc.).
- Améliorer les règles de détection et renforcer les politiques de sécurité en réponse aux tests réalisés.

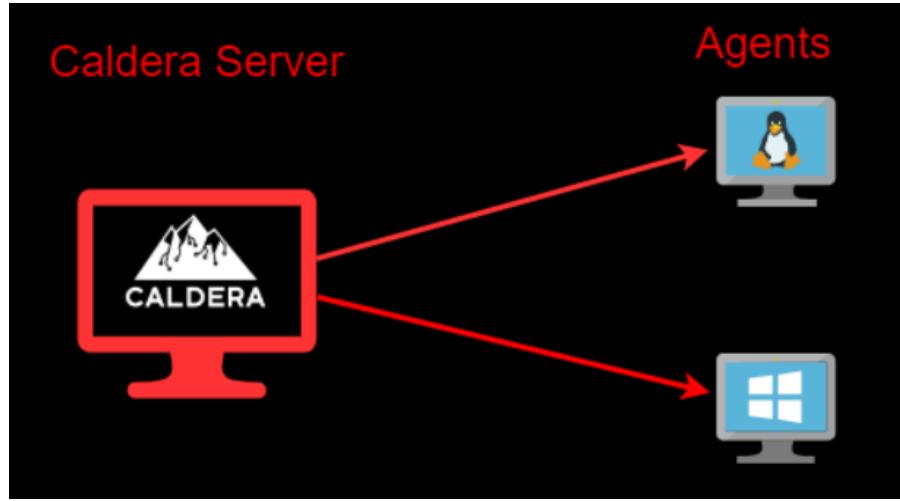


FIGURE 2.17 : L'infrastructure de Caldera

## 2.6 Virtualisation

[20] La virtualisation est une technologie que vous pouvez utiliser pour créer des représentations virtuelles de serveurs, de stockage, de réseaux et d'autres machines physiques. Le logiciel virtuel imite les fonctions du matériel physique pour exécuter plusieurs machines virtuelles sur une seule machine physique. Les entreprises ont recours à la virtualisation pour utiliser efficacement leurs ressources matérielles et obtenir un meilleur rendement de leurs investissements. Elle alimente également les services de cloud computing qui aident les organisations à gérer leur infrastructure plus efficacement.

### 2.6.1 Définition

[20] La virtualisation est une technologie que vous pouvez utiliser pour créer des représentations virtuelles de serveurs, de stockage, de réseaux et d'autres machines physiques. Le logiciel virtuel imite les fonctions du matériel physique pour exécuter plusieurs machines virtuelles sur une seule machine physique. Les entreprises ont recours à la virtualisation pour utiliser efficacement leurs ressources matérielles et obtenir un meilleur rendement de leurs investissements. Elle alimente également les services de cloud computing qui aident les organisations à gérer leur infrastructure plus efficacement.

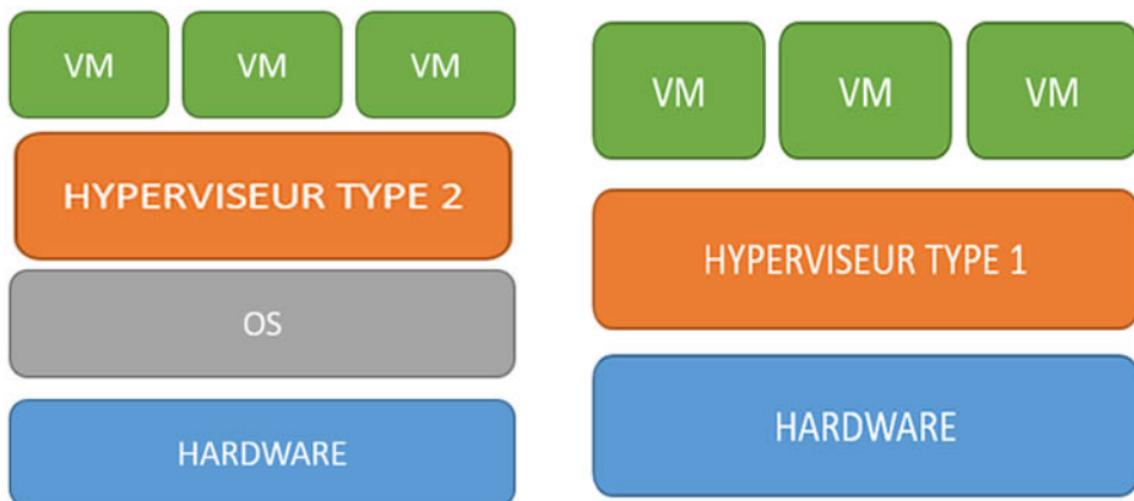
### 2.6.2 Machine virtuelle

[20] Une machine virtuelle est un ordinateur défini par logiciel qui s'exécute sur un ordinateur physique doté d'un système d'exploitation et de ressources informatiques distincts. L'ordinateur physique est appelé machine hôte et les machines virtuelles sont des machines invitées. Plusieurs machines virtuelles peuvent être exécutées sur une seule machine physique. Les machines virtuelles sont extraites du matériel informatique par un hyperviseur.

### 2.6.3 Hyperviseur

[20] L'hyperviseur est un composant logiciel qui gère plusieurs machines virtuelles sur un ordinateur. Il garantit que chaque machine virtuelle reçoit les ressources allouées et n'interfère pas avec le fonctionnement des autres machines virtuelles. Il existe deux types d'hyperviseurs.

- **Hyperviseurs de type 1** : Un hyperviseur de type 1, ou hyperviseur de matériel nu, est un programme d'hyperviseur installé directement sur le matériel de l'ordinateur plutôt que sur le système d'exploitation. Par conséquent, les hyperviseurs de type 1 offrent de meilleures performances et sont couramment utilisés par les applications d'entreprise. KVM utilise l'hyperviseur de type 1 pour héberger plusieurs machines virtuelles sur le système d'exploitation Linux.
  - **Hyperviseurs de type 2** : Un hyperviseur de type 2 s'exécute comme une application sur un matériel informatique doté d'un système d'exploitation existant. Utiliser ce type d'hyperviseur lorsque vous exécutez plusieurs systèmes d'exploitation sur une seule machine. Exemple : Oracle VM VirtualBox, VMware Workstation.



**FIGURE 2.18 :** Types d'hyperviseurs

### 2.6.3.1 VMware Workstation

[20] VMware Workstation est un hyperviseur de type 2 développé par VMware, qui permet d'exécuter plusieurs machines virtuelles sur un même ordinateur physique. Il s'installe sur un système d'exploitation (comme Windows ou Linux) et permet de tester, développer ou exécuter différents systèmes d'exploitation (Windows, Linux, etc.) dans des environnements isolés, sans modifier le système principal. La figure suivante présente son logo :

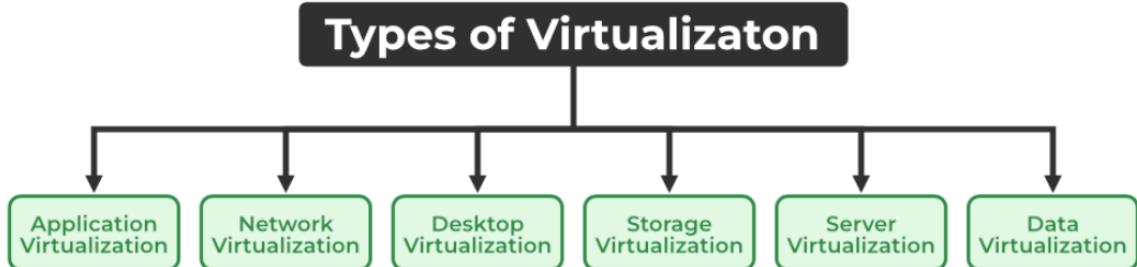


FIGURE 2.19 : Logo de VMware Workstation

### 2.6.4 Les différents types de virtualisation

- **Virtualisation des serveurs** : C'est le fait de diviser un serveur physique en plusieurs serveurs virtuels. Cela permet d'utiliser toute la puissance de la machine et d'éviter qu'elle reste partiellement inutilisée.
- **Virtualisation du stockage** : Elle regroupe plusieurs équipements de stockage (même s'ils sont différents) pour en faire un seul espace de stockage virtuel, plus facile à gérer, sauvegarder et utiliser.
- **Virtualisation des réseaux** : Elle permet de contrôler les composants réseau (commutateurs, routeurs, pare-feux) à distance via un logiciel, sans manipuler le matériel, ce qui simplifie la gestion du réseau.
- **Virtualisation des données** : Elle crée une couche logicielle qui permet d'accéder à des données stockées à différents endroits (cloud, serveurs locaux) comme si elles étaient toutes au même endroit.
- **Virtualisation des données** : Elle permet de faire fonctionner une application sur un système différent de celui pour lequel elle a été conçue, sans l'installer localement. Exemple : lancer une application Windows sur Linux.
  - **Streaming d'application** : Les utilisateurs diffusent l'application à partir d'un serveur distant, de sorte qu'elle ne s'exécute que sur l'appareil de l'utilisateur final lorsque cela est nécessaire.

- **Virtualisation des applications sur serveur** : Les utilisateurs peuvent accéder à l'application distante à partir de leur navigateur ou de l'interface client sans l'installer.
- **Virtualisation locale de l'application** : Le code de l'application est livré avec son propre environnement pour fonctionner sur tous les systèmes d'exploitation sans modification.



**FIGURE 2.20 :** Types de virtualisation

### 2.6.5 Les avantages de la virtualisation

- Utilisation efficace des ressources.
- Gestion informatique automatisée.
- Reprise plus rapide après sinistre.

## 2.7 Conteneurisation

### 2.7.1 Définition

[20] La conteneurisation est une méthode qui permet de regrouper une application avec tout ce dont elle a besoin (fichiers, bibliothèques, etc.) pour fonctionner, peu importe l'ordinateur ou le système utilisé. Contrairement à avant, où il fallait une version spécifique pour chaque système (comme Windows), un conteneur peut tourner partout, sans modification.

### 2.7.2 Les avantages de la conteneurisation

- **Portabilité** : La conteneurisation permet d'utiliser une même application sur différents systèmes (Linux, Windows...) sans changer son code. Les développeurs créent l'application une seule fois et peuvent la déployer partout, même pour mettre à jour d'anciens programmes.
- **Capacité de mise à l'échelle** : Les conteneurs sont légers et rapides à lancer. On peut facilement en faire tourner plusieurs sur une même machine, car ils partagent les ressources sans se gêner entre eux.
- **Tolérance aux pannes** : Si un conteneur tombe en panne, les autres continuent de fonctionner normalement. Cela rend l'application plus stable et disponible, même en cas de problème.

- **Agilité** : Les développeurs peuvent corriger ou mettre à jour une application conteneurisée sans toucher au reste du système. Cela permet de travailler plus vite et de publier les nouveautés rapidement.

### 2.7.3 Docker

#### 2.7.3.1 Définition

[21] Docker est une plateforme qui permet de créer, tester et lancer des applications facilement. Elle regroupe tout ce qu'il faut pour faire fonctionner une application (code, outils, bibliothèques...) dans des conteneurs. Grâce à Docker, on peut déployer une application sur n'importe quel environnement, en étant sûr qu'elle fonctionnera correctement. La figure suivante montre le logo de Docker :



**FIGURE 2.21** : Logo de Docker

## 2.8 Cloud Computing

### 2.8.1 Définition

[22] Le cloud computing est la disponibilité à la demande de ressources informatiques (telles que le stockage et l'infrastructure) en tant que services sur Internet. Ainsi, les particuliers et les entreprises n'ont plus besoin de gérer eux-mêmes leurs ressources physiques, et de ne payer que ce qu'ils utilisent.

### 2.8.2 Les avantages de Cloud computing

- **Flexibilité** : Le cloud permet d'accéder aux services à distance, depuis n'importe quel endroit avec Internet. Il est aussi facile d'augmenter ou de réduire les ressources selon les besoins.
- **Efficacité** : Les entreprises peuvent créer et lancer des applications rapidement, sans devoir gérer les serveurs ou l'infrastructure technique.
- **Valeur stratégique** : Grâce au cloud, les entreprises profitent rapidement des dernières technologies sans devoir investir lourdement. Cela leur donne un avantage concurrentiel.
- **Sécurité** : Le cloud est généralement très sécurisé. Les fournisseurs mettent en place des protections avancées, souvent meilleures que celles des entreprises elles-mêmes.

### 2.8.3 Google Cloud

[22] Google Cloud Platform (GCP) est une plateforme de services cloud développée par Google, qui fournit une infrastructure informatique à la demande, évolutive et sécurisée, hébergée dans les centres de données de Google à travers le monde. Son logo présente dans la figure suivante :



**FIGURE 2.22 :** Logo de Google Cloud Platform

### 2.8.4 Oracle Cloud

[23] Oracle Cloud est une plateforme de services cloud proposée par Oracle Corporation. Elle fournit une gamme complète de services permettant aux entreprises de développer, déployer, intégrer, sécuriser et gérer des applications et des bases de données dans le cloud. La figure 2.23 présente son logo.



**FIGURE 2.23 :** Logo de Oracle Cloud

## 2.9 Intégration de l'intelligence artificielle (AI)

### 2.9.1 L'intelligence artificielle (AI)

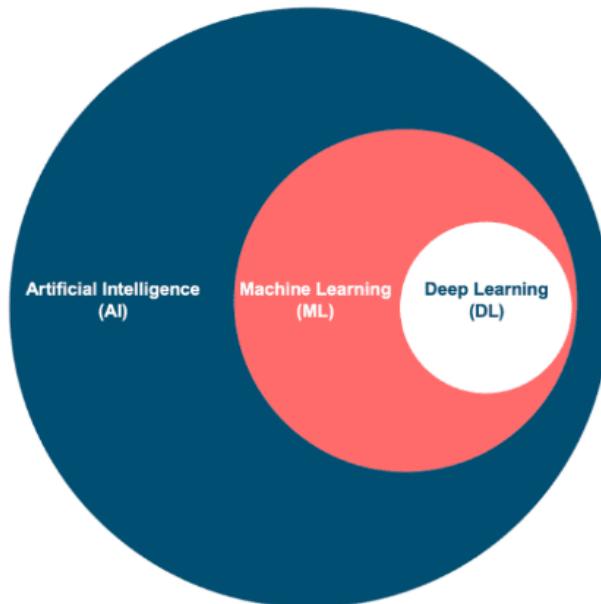
[24] L'AI est un domaine de l'informatique qui vise à créer des systèmes capables de simuler l'intelligence humaine, notamment dans l'analyse de données, la prise de décision ou la compréhension du langage naturel.

#### 2.9.1.1 La machine Learning (ML)

[24] Le ML est une branche de l'intelligence artificielle qui permet aux machines d'apprendre à partir de données sans être explicitement programmées. Il consiste à entraîner des modèles à reconnaître des motifs et à faire des prédictions ou des décisions automatisées. Ce processus repose sur des algorithmes capables d'améliorer leur performance au fil du temps grâce à l'expérience.

### 2.9.1.2 Le Deep Learning (DL)

[24] Le DL est un sous-domaine du machine learning basé sur des réseaux de neurones artificiels à plusieurs couches. Il permet aux machines de traiter des données complexes comme des images, du texte ou du son avec un haut niveau d'abstraction. Grâce à ses architectures profondes, il atteint des performances élevées dans des tâches comme la reconnaissance vocale ou la vision par ordinateur.



**FIGURE 2.24 :** Hiérarchie de l'AI

### 2.9.2 Le grand modèle de langage (LLM)

[25] Un grand modèle linguistique (LLM) est un programme d'intelligence artificielle capable de reconnaître, comprendre et générer du texte. Il est entraîné sur de vastes ensembles de données en utilisant des techniques de Machine Learning (ML), et plus précisément de Deep Learning (DL), via des modèles transformateurs. Grâce à cet apprentissage en profondeur, le LLM analyse de manière probabiliste les relations entre les caractères, les mots et les phrases, ce qui lui permet d'interpréter le langage humain de façon autonome sans intervention humaine directe.



**FIGURE 2.25 :** Logo de LLM

### 2.9.3 Les avantages d'intégrer un LLM dans un SOC

- **Automatisation et gain de temps :** Le LLM peut automatiquement analyser un grand volume d'alertes en un temps réduit, ce qui permet aux analystes de se concentrer sur les incidents les plus critiques.
- **Amélioration de la précision des analyses :** Grâce à sa compréhension fine du langage naturel et des contextes, le LLM peut mieux interpréter les descriptions d'alertes, réduire les faux positifs et aider à prioriser les menaces.
- **Enrichissement des alertes :** Le LLM peut contextualiser les alertes en ajoutant des informations complémentaires issues de bases de connaissances, rapports de menaces ou données historiques, facilitant ainsi la prise de décision.
- **Support à l'investigation et au triage :** En analysant les logs et les métadonnées associées, le LLM peut proposer des hypothèses sur la nature des attaques, suggérer des pistes d'investigation et recommander des actions de mitigation.
- **Capacité d'apprentissage continu :** Le LLM peut être mis à jour régulièrement avec de nouvelles données de menace, ce qui améliore continuellement sa capacité à détecter et analyser des attaques émergentes.
- **Réduction de la charge cognitive :** En synthétisant et reformulant des alertes complexes en langage compréhensible, le LLM facilite la compréhension et accélère la réaction des équipes de sécurité.

## 2.10 Systèmes de notification et de messagerie

### 2.10.1 Slack

Slack est une plateforme de messagerie collaborative conçue pour faciliter la communication au sein des équipes, notamment dans les environnements professionnels et projets IT comme les SOC.



FIGURE 2.26 : Logo de Slack

### 2.10.2 Zoho Mail

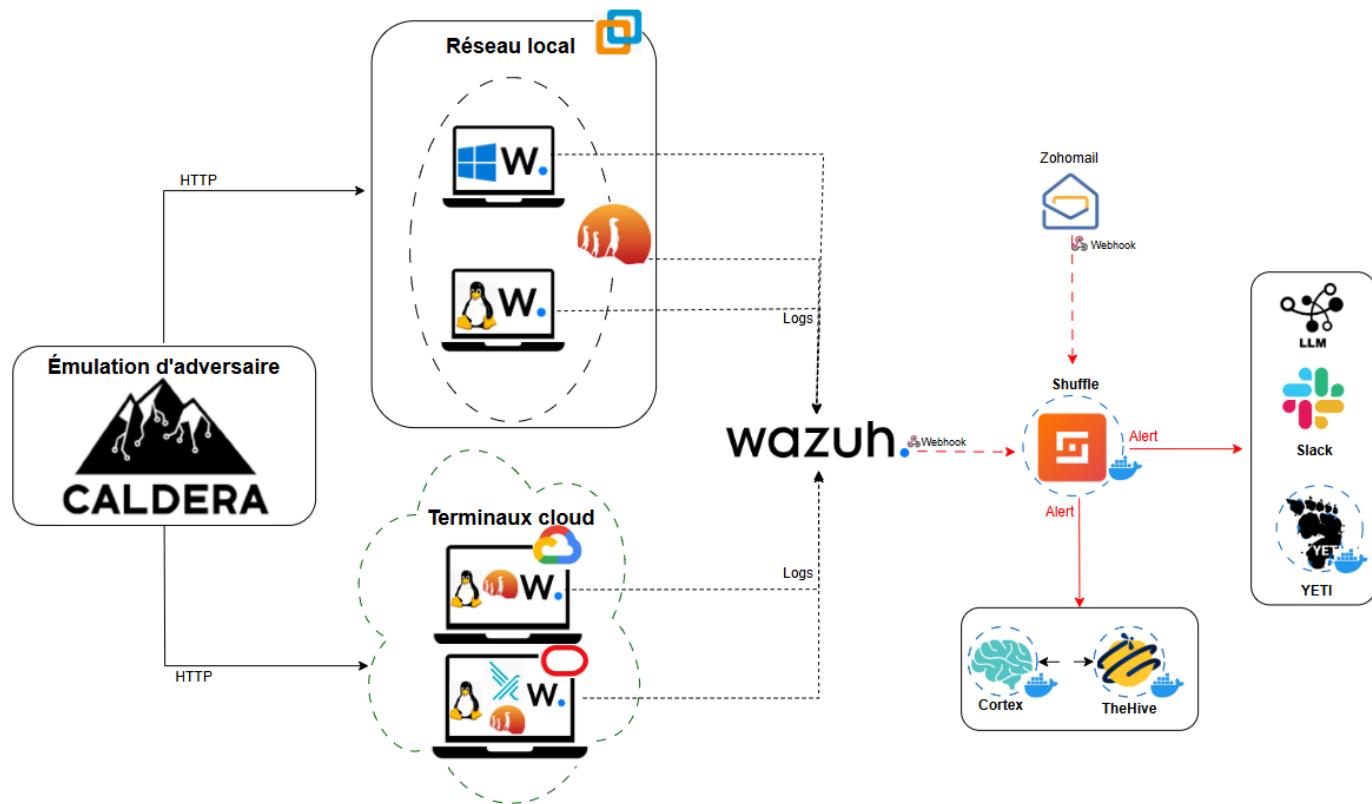
Zoho Mail est un service de messagerie électronique sécurisé et professionnel proposé par la suite Zoho. Il permet d'envoyer, recevoir et gérer des e-mails au sein d'une organisation.



**FIGURE 2.27 :** Logo de Zoho Mail

## 2.11 Architecture envisagée

Cette architecture a été choisie pour notre projet à l'issue d'une comparaison entre plusieurs outils.



**FIGURE 2.28 :** Architecture envisagée

## Conclusion

Ce chapitre établit le cadre théorique en présentant les éléments essentiels de notre projet et en évaluant les différentes technologies, le chapitre suivant abordera l'implémentation pratique.

# MISE EN PLACE DE LA SOLUTION SIEM

---

## Plan

<b>Introduction</b> . . . . .	<b>46</b>
<b>1 Mise en place de Wazuh</b> . . . . .	<b>46</b>
<b>2 Installation et configuration d'un système de détection d'intrusion (IDS)</b> . . . . .	<b>52</b>
<b>Conclusion</b> . . . . .	<b>55</b>

## Introduction

Dans ce chapitre, nous aborderons la phase initiale de notre projet en déployant Wazuh en tant que solution SIEM. Cette implémentation permettra d'effectuer la collecte des logs, leur corrélation basée sur des règles configurées, et le déclenchement d'alertes en cas de détection d'événements suspects.

### 3.1 Mise en place de Wazuh

Nous avons déployé Wazuh sur une instance Ubuntu hébergée dans le cloud, dans la figure suivante montre la réussite d'installation du cluster Wazuh : l'indexeur wazuh, le serveur Wazuh et le tableau de bord, tous sont le même serveur d'adresse IP publique :"35.204.57.76"

```
daas_amall@manager-vm:~$ sudo cat /root/config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "35.204.57.76"
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "35.204.57.76"
    #- node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "35.204.57.76"
```

FIGURE 3.1 : Cluster Wazuh

#### 3.1.1 Déploiement de certificats

L'utilisation des certificats TLS a été retenue pour sécuriser la connexion. La figure suivante illustre la configuration des certificats TLS :

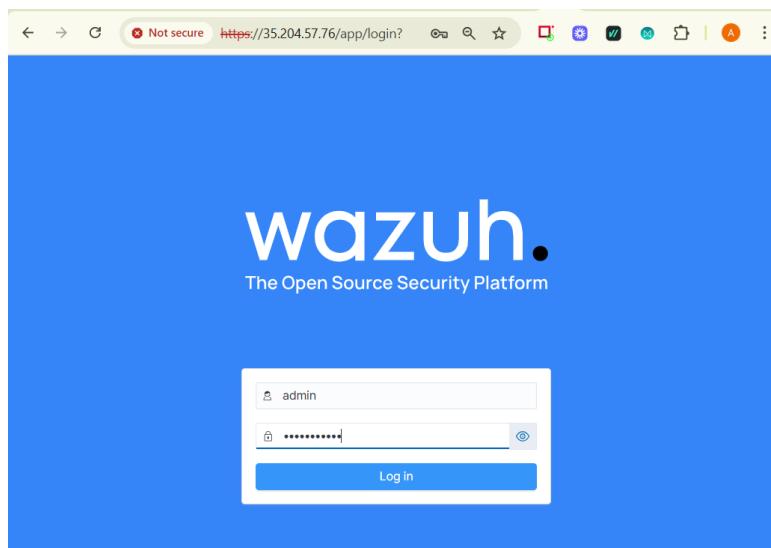
```

server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://10.164.0.4:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant", "Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wz-home

```

**FIGURE 3.2 :** Génération des certificats TLS

Maintenant, nous pouvons accéder à l'interface utilisateur via l'URL `https://35.204.57.76`.

**FIGURE 3.3 :** Interface utilisateur de Wazuh

### 3.1.2 Les agents wazuh

Nous avons actuellement déployé quatre agents répartis entre le réseau local et le cloud. Le réseau local d'adresse réseau 192.168.219.0/24 héberge deux systèmes : l'agent Ubuntu "Agent-ubuntu01" (192.168.219.138) et une machine Windows 10 (192.168.219.132). Les terminaux cloud incluent deux instances Ubuntu "web-cloud" (10.164.0.5) et "ubn-cloud" (10.0.0.118), tous deux configurés dans le groupe "cloud-endpoints". L'ensemble de ces agents maintiennent une connectivité active avec le cluster Wazuh node01, assurant une surveillance de sécurité complète tant pour l'infrastructure locale que pour les ressources cloud (Pour plus de détails sur la création d'un agent, se référer à l'annexe A).

Comme illustre la figure suivante :

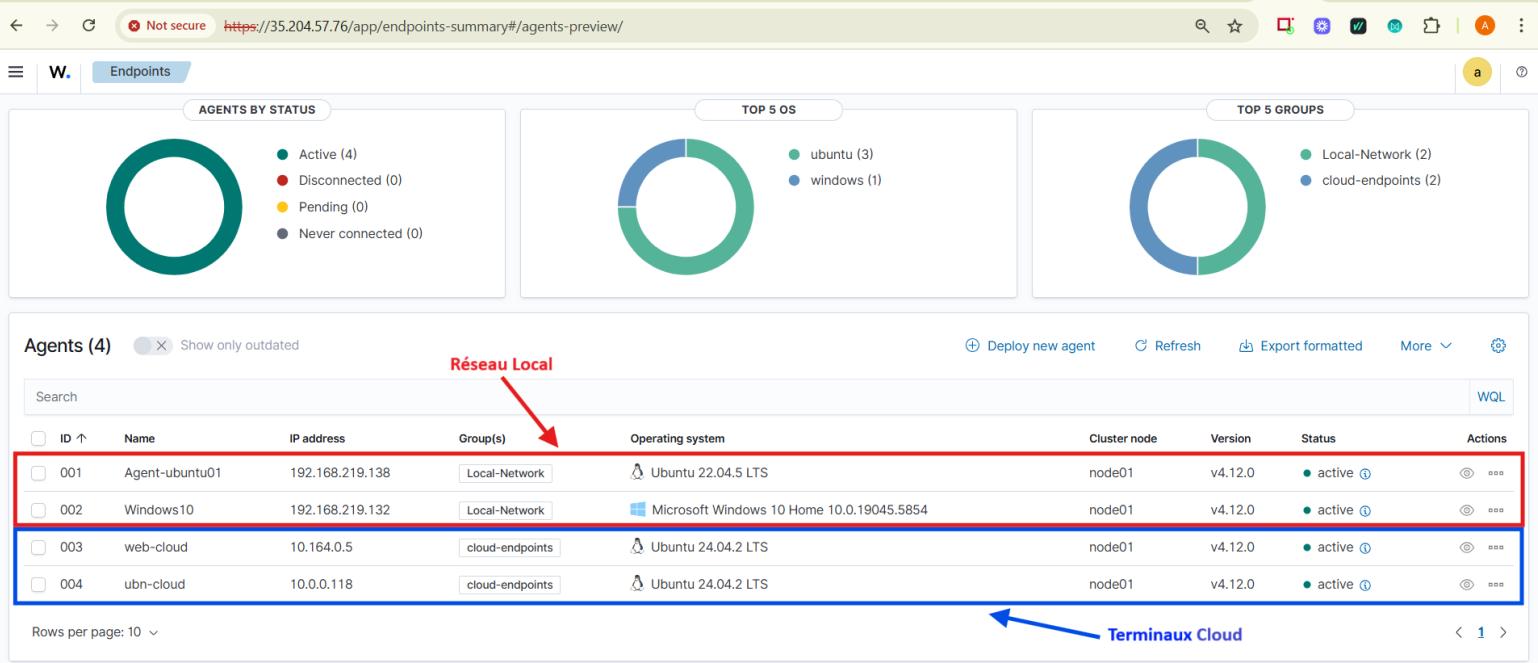


FIGURE 3.4 : Liste des agents

### 3.1.3 Configuration de Sysmon

#### 3.1.3.1 Définition

Sysmon (System Monitor) est un outil de Microsoft qui surveille et journalise les activités système critiques comme la création de processus, les connexions réseau et l'accès aux fichiers. Il enregistre ces événements dans le journal Windows pour l'analyse de sécurité et la détection des menaces. Une version expérimentale existe aussi pour Linux, basée sur eBPF. Nous avons configuré Sysmon sur la machine Windows ainsi que sur la machine Ubuntu du réseau local.

#### 3.1.3.2 Installation de Sysmon

La figure ci-dessous illustre l'installation de Sysmon sur la machine Windows.

```
PS C:\Users\lama\Downloads\Sysmon> .\Sysmon64.exe -accepteula -i sysmonconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
```

FIGURE 3.5 : Installation de Sysmon sur Windows10

Nous passons maintenant à l'installation de Sysmon sur la machine Ubuntu, comme montre la figure suivante :

```
ubuntu@Agent-ubuntu01:~$ sudo systemctl status sysmon
[sudo] password for ubuntu:
● sysmon.service - Sysmon event logger
   Loaded: loaded (/etc/systemd/system/sysmon.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-06-03 16:00:34 CET; 1 week 0 days ago
     Main PID: 34103 (sysmon)
        Tasks: 1 (limit: 2207)
       Memory: 76.4M
          CPU: 9min 6.144s
         CGroup: /system.slice/sysmon.service
             └─34103 /opt/sysmon/sysmon -i /opt/sysmon/config.xml -service

18:48:52 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:48:53 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:48:53 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:48:55 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:48:55 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:48:56 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:49:01 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:49:02 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:49:05 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
18:49:05 10 جول Agent-ubuntu01 sysmon[34103]: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}>
lines 1-20/20 (END)
```

**FIGURE 3.6 :** Installation de Sysmon sur Ubuntu

### 3.1.3.3 Configuration de Sysmon pour la collecte des logs

Cette configuration du fichier local de Wazuh permet de surveiller les événements du canal Windows-Sysmon dans le journal Operational de Microsoft. Elle facilite la collecte et l'analyse des journaux système avancés, contribuant ainsi à la détection des menaces sur les endpoints Windows.

```
<localfile>
  <log_format>eventchannel</log_format>
  <location>Microsoft-Windows-Sysmon/Operational</location>
</localfile>
```

**FIGURE 3.7 :** Collecte des logs Sysmon Windows

La configuration suivante de fichier local permet à l'agent Wazuh de collecter les logs Sysmon stockés dans '/var/log/syslog' en utilisant le format syslog standard. Sysmon pour Linux génère des événements détaillés sur les activités système comme les créations de processus, connexions réseau et modifications de fichiers qui sont centralisés dans le journal syslog. Cette surveillance avancée offre une visibilité granulaire sur les comportements suspects et les indicateurs de compromission au niveau du système Linux (Voir les détails de configuration dans l'Annexe A).

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
</localfile>
```

**FIGURE 3.8 :** Collecte des logs Sysmon Linux

### 3.1.4 Configuration des règles personnalisées

Nous avons configurés une règle dans Wazuh (ID 5764) permet de détecter plusieurs tentatives de connexion SSH avec des noms d'utilisateur inexistant. Elle se déclenche si trois événements similaires

(définis par la règle 5710) proviennent de la même adresse IP en moins de 60 secondes. Cela peut indiquer une attaque par force brute. La règle est liée à la technique T1110 du framework MITRE ATT&CK, qui correspond aux attaques par mot de passe.

```
<rule id="5764" level="10" frequency="3" timeframe="60">
<if_matched_sid>5710</if_matched_sid>
<same_source_ip />
<description>Multiple SSH login attempts using non-existent usernames.</description>
<mitre>
<id>T1110</id>
</mitre>
</rule>
```

**FIGURE 3.9 :** Règle Wazuh pour la protection SSH

Nous avons vérifié cette règle en tentant une connexion SSH depuis une autre machine avec un nom d'utilisateur inexistant.

```
PS C:\WINDOWS\system32> ssh amall@144.24.203.214
amall@144.24.203.214: Permission denied (publickey).
PS C:\WINDOWS\system32> ssh amall@144.24.203.214
amall@144.24.203.214: Permission denied (publickey).
PS C:\WINDOWS\system32> ssh amall@144.24.203.214
amall@144.24.203.214: Permission denied (publickey).
PS C:\WINDOWS\system32>
```

**FIGURE 3.10 :** Test de la règle

Nous avons reçu une alerte déclenchée par cette règle comme montre la figure ci-dessous :

timestamp	agent.name	rule.description	rule.level	rule.id
Jun 11, 2025 @ 00:06:47.2...	ubn-cloud	sshd: Attempt to login using a non-existent user	5	5710
Jun 11, 2025 @ 00:06:47.1...	ubn-cloud	sshd: Attempt to login using a non-existent user	5	5710
Jun 11, 2025 @ 00:06:37.1...	ubn-cloud	Multiple SSH login attempts using non-existent usernames.	10	5764

**FIGURE 3.11 :** Validation de l'alerte dans les logs

Nous avons analysé l'alerte générée pour confirmer. Voici le détail de l'alerte :

Document Details		<a href="#">View surrounding documents</a>	<a href="#">View single document</a>
<a href="#">Table</a>	JSON		
t GeoLocation.country_name	Tunisia		
⊕ GeoLocation.location	{ "lon": 9, "lat": 34 }		
t _index	wazuh-alerts-4.x-2025.06.10		
t agent.id	004		
t agent.ip	10.0.0.118		
t agent.name	ubn-cloud		
t data.srcip	154.107.199.122		
t data.srcport	4800		
t data.srcuser	amall		
t decoder.name	sshd		
t decoder.parent	sshd		
t full_log	Jun 10 23:06:35 ubn-cloud sshd[2085825]: Invalid user amall from 154.107.199.122 port 4800		
t id	1749596797.74028505		
t input.type	log		<a href="#">Activate Windows</a>
t location	journald		<a href="#">Go to Settings to activate Windows.</a>
t manager.name	manager-vm.europe-west4-c.c.eighth-study-460002-d3.internal		
t predecoder.hostname	ubn-cloud		

**FIGURE 3.12 :** Description d'une alerte

### 3.1.5 Réponse active (Active Response)

La Réponse Active est une fonctionnalité de Wazuh qui permet d'exécuter automatiquement des actions (par exemple, bloquer une adresse IP, tuer un processus) en réponse à des menaces détectées.

Par exemple :

- Bloquer une adresse IP après plusieurs tentatives de connexion SSH échouées.
- Bloquer une adresse IP après la détection d'un scan de ports.

Nous avons configuré une réponse active, comme illustre la figure 3.13.

```
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5764</rules_id>
  <timeout>no</timeout>
</active-response>
```

**FIGURE 3.13 :** Configuration d'une réponse active dans Wazuh

Cette configuration garantit que lorsqu'une alerte correspondant à la règle 5764 est déclenchée, l'adresse IP à l'origine de l'alerte est bloquée localement sans déblocage automatique.

```
daas_amall@vm-test:~$ curl ifconfig.me
34.90.255.173daas_amall@vm-test:~$ ssh amall@144.24.203.214
amall@144.24.203.214: Permission denied (publickey).
daas_amall@vm-test:~$ ssh amall@144.24.203.214
amall@144.24.203.214: Permission denied (publickey).
daas_amall@vm-test:~$ ssh amall@144.24.203.214
amall@144.24.203.214: Permission denied (publickey).
daas_amall@vm-test:~$ █
```

FIGURE 3.14 : Vérification de la réponse active dans Wazuh

Nous confirmons maintenant en vérifiant les règles du pare-feu sur l'agent testé.

```
ubuntu@ubn-cloud:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP      all  --  173.255.90.34.bc.googleusercontent.com  anywhere
```

FIGURE 3.15 : Affichage des règles iptables sur l'agent

## 3.2 Installation et configuration d'un système de détection d'intrusion (IDS)

### 3.2.1 Mise en place d'un système de détection d'intrusion réseau (NIDS)

Nous avons configuré le NIDS dans le réseau local pour inspecter et détecter les trafics malveillants.

Premièrement, Suricata a été correctement installé.

```
ubuntu@suricata:~$ sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
  Loaded: loaded (/etc/init.d/suricata; generated)
  Active: active (running) since Wed 2025-06-11 11:41:07 CET; 10min ago
    Docs: man:systemd-sysv-generator(8)
 Process: 975 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
   Tasks: 8 (limit: 4545)
  Memory: 51.2M
    CPU: 34.070s
   CGroup: /system.slice/suricata.service
           └─1159 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv

11:41:04 11 ↗ suricata systemd[1]: Starting LSB: Next Generation IDS/IPS...
11:41:07 11 ↗ suricata suricata[975]: Starting suricata in IDS (af-packet) mode... done.
11:41:07 11 ↗ suricata systemd[1]: Started LSB: Next Generation IDS/IPS.
ubuntu@suricata:~$ █
```

FIGURE 3.16 : Installation de Suricata

Maintenant, configurons Suricata comme NIDS pour surveiller le réseau 192.168.219.0/24.

```

vars:
  # more specific is better for alert accuracy and performance
address-groups:
  HOME_NET: "[192.168.219.0/24]"
  #HOME_NET: "[192.168.0.0/16]"
  #HOME_NET: "[10.0.0.0/8]"
  #HOME_NET: "[172.16.0.0/12]"
  #HOME_NET: "any"

```

FIGURE 3.17 : Configuration de Suricata en tant que NIDS

### 3.2.1.1 Configuration des règles personnalisées

Bien que Suricata dispose de règles prédéfinies, nous souhaitons configurer des règles personnalisées afin de surveiller le trafic réseau associé à certains services.

```

alert tcp any any -> $HOME_NET 22 (msg:"SSH brute force login attempt"; flow:established,to_server; content:"SSH"; threshold: type threshold, track_by_src, count 5, seconds 60; classtype:attempted-admin; sid:1000010; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"SSH brute force login attempt - Any Port"; flow:established,to_server; content:"SSH"; pcre:"/failed|failu
re|invalid|error|denied|i"; threshold: type threshold, track_by_src, count 5, seconds 60; classtype:attempted-admin; sid:1000011; rev:1;)
alert http any any -> any any (msg:"ALERT Suspicious User-Agent detected"; content:"User-Agent|3a|"; http_header; content:"sqlmap"; nocase; classt
ype:web-application-attack; sid:1000011; rev:1;)
# Détection d'injection SQL dans les requêtes HTTP
alert http any any -> any any (msg:"SQL Injection attempt detected in HTTP request"; flow:established,to_server; content:"GET"; http_method; pcre:
"/(\%27)|(\')|(\-\-)|(\%23)|(#)|i"; classtype:web-application-attack; sid:1000020; rev:1;)

```

FIGURE 3.18 : Configuration des règles

### 3.2.1.2 Centralisation des logs de Suricata

Nous avons maintenant configuré Suricata pour transférer ses logs vers Wazuh.

```

<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>

```

FIGURE 3.19 : Configuration des logs Suricata vers Wazuh

Tout d'abord, Suricata est ajouté comme agent de Wazuh, aussi comme membre du groupe "Local-network"

Local-Network							<a href="#">Manage agents</a>	<a href="#">Export PDF</a>					
<a href="#">Agents</a>		<a href="#">Files</a>					<a href="#">Refresh</a>	<a href="#">Export formatted</a>					
Agents (3)													
From here you can list and manage your agents													
Id	Name	IP address	Operating system	Version	Status	Actions							
001	Agent-ubuntu01	192.168.219.138	Ubuntu 22.04.5 LTS	v4.12.0	● disconnected ⓘ	<a href="#">Edit</a>							
002	Windows10	192.168.219.132	Microsoft Windows 10 Home 10.0.19045.5854	v4.12.0	● disconnected ⓘ	<a href="#">Edit</a>							
005	suricata	192.168.219.131	Ubuntu 22.04.4 LTS	v4.12.0	● active ⓘ	<a href="#">Edit</a>							
Rows per page: 15							< 1 >						

FIGURE 3.20 : Statut des agents du réseau local

### 3.2.2 Mise en place d'un système de détection d'intrusion réseau (HIDS)

#### 3.2.2.1 Suricata

Nous avons configuré Suricata comme un HIDS pour surveiller les fichiers, les processus et les logs sur nos machines cloud.

```
vars:
# more specific is better for alert accuracy and performance
address-groups:
HOME_NET: "[10.0.0.118/32]"
#HOME_NET: "[192.168.0.0/16]"
```

**FIGURE 3.21 :** Configuration de Suricata en tant que HIDS

Pour centraliser ses logs vers Wazuh, nous avons configuré l'agent Wazuh afin de transférer les journaux, comme décrit dans la partie précédente.

#### 3.2.2.2 Falco

Nous avons maintenant configuré Falco dans la machine ubn-cloud, afin de détecter les comportements anormaux au niveau système et remonter les alertes vers Wazuh (Voir les détails de configuration dans l'Annexe A), comme montre la figure 3.22.

```
<localfile>
<location>/var/log/falco_events.json</location>
<log_format>json</log_format>
</localfile>
```

**FIGURE 3.22 :** Configuration des logs Falco vers Wazuh

Nous avons testé la détection des comportements anormaux par Falco en exécutant, depuis la machine ubn-cloud, la commande suivante : sudo cat /etc/shadow.

↓ timestamp	↓ agent.name	↓ rule.description	rule.level	rule.id
Jun 11, 2025 @ 13:37:08.6...	ubn-cloud	"Falco Alert - " 12:37:08.242236124: Warning Sensitive file opened for reading by non-trusted program   file=/etc/shadow gparent=sudo gparent=bash gggparent=sshd evt_type=openat user=root user_uid=0 user_loginuid=1001 process=:cat proc_exepath=/usr/bin/cat parent=sudo command=cat /etc/shadow terminal=34821 container_id=host container_name=host container_image_repository= container_image_tag=k8s_pod_name=<NA> k8s_ns_name=<NA>"	8	100603

The screenshot shows a log entry from the Falco alert table. The entry details a warning about a sensitive file being opened by a non-trusted program (sudo) on the host system. The log message includes the timestamp, file path, and various process and container details. A tooltip or expanded view of the log message is shown in a separate window, providing a detailed breakdown of the event.

**FIGURE 3.23 :** Alerte générée par Falco

## Conclusion

Ce chapitre a décrit l'installation et la configuration de notre solution SIEM, assurant une collecte et une analyse efficaces des événements de sécurité. Cette base solide prépare la gestion proactive des incidents. La prochaine étape sera l'intégration du SOAR avec l'intelligence artificielle afin de disposer d'un SOC moderne et plus intelligent.

# MISE EN PLACE DE LA SOLUTION SOAR

---

## Plan

Introduction . . . . .	57
1    Les outils choisis SOAR . . . . .	57
2    Mise en place des outils . . . . .	57
Conclusion . . . . .	81

## Introduction

Ce chapitre présente la mise en place de notre solution SOAR. Il décrit les outils choisis, ainsi que leur intégration au sein de notre infrastructure. Chaque phase de déploiement est détaillée, accompagnée des configurations nécessaires pour garantir leur interopérabilité. Enfin, des scénarios de test ont été élaborés afin d'évaluer l'efficacité de la solution face à des incidents de sécurité simulés.

### 4.1 Les outils choisis SOAR

Dans le cadre de notre solution SOAR, nous avons sélectionné un ensemble d'outils complémentaires afin d'automatiser et d'optimiser la réponse aux incidents de sécurité. L'orchestrateur Shuffle constitue le cœur du système, permettant de coordonner les différentes actions entre les outils intégrés. TheHive a été choisi comme plateforme centrale de gestion des incidents, tandis que Cortex permet l'analyse automatique d'indicateurs grâce à ses analyseurs enrichis. Pour le renseignement sur les menaces, nous avons intégré YETI-CTI, qui fournit des informations contextuelles sur les observables. Par ailleurs, nous avons expérimenté l'usage d'un modèle de langage (LLM) afin d'améliorer la compréhension et l'analyse des rapports d'incidents. Enfin, un système de notification via Slack a été mis en place pour assurer une communication rapide et efficace avec les équipes de sécurité.

### 4.2 Mise en place des outils

#### 4.2.1 Installation de Docker

Docker a été utilisé pour déployer efficacement les différents composants de notre solution SOAR, notamment Shuffle, TheHive, Cortex, MISP et YETI. Chaque outil fonctionne dans un conteneur dédié, assurant une isolation, une portabilité et une facilité de maintenance. Grâce à Docker Compose, nous avons pu orchestrer et automatiser le démarrage de l'ensemble des services de manière cohérente.

```

daas_amall@shuffle-vm:~$ sudo systemctl status docker.service
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-06-15 11:06:58 UTC; 10min ago
   TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
      Main PID: 169812 (dockerd)
        Tasks: 74
       Memory: 336.5M (peak: 1.4G)
         CPU: 1min 54.616s
        CGroup: /system.slice/docker.service
                └─169812 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
                  ├─170201 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 9200 -container-ip 172.18.0.2
                  ├─170207 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 9200 -container-ip 172.18.0.2 -con>
                  ├─171203 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 5001 -container-ip 172.18.0.4
                  ├─171211 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 5001 -container-ip 172.18.0.4 -con>
                  ├─171248 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 3001 -container-ip 172.18.0.5
                  ├─171259 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 3001 -container-ip 172.18.0.5 -con>
                  ├─171269 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 3443 -container-ip 172.18.0.5
                  └─171277 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 3443 -container-ip 172.18.0.5 -con>

Jun 15 11:15:40 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:40 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:41 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:41 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:41 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:49 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:49 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:50 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:15:50 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:16:55 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
Jun 15 11:16:55 shuffle-vm.europe-west4-b.c.eighth-study-460002-d3.internal dockerd[169812]: time="2025-06-15T11>
daas_amall@shuffle-vm:~$ docker compose version
Docker Compose version v2.36.2 ←
daas_amall@shuffle-vm:~$ █

```

FIGURE 4.1 : Installation de docker et docker compose

#### 4.2.2 Mise en place de YETI

Nous avons déployé YETI à l'aide de Docker Compose, ce qui nous a permis de bénéficier d'un déploiement modulaire, rapide et facile à maintenir. Cette installation comprend plusieurs services essentiels tels que l'API, le frontend, la base de données ArangoDB ainsi que le service de cache Redis. Grâce à cette approche containerisée, la mise à jour des composants et l'intégration avec d'autres outils de sécurité sont grandement simplifiées.

NAME	IMAGE	COMMAND	SERVICE	CREATED	STATUS	PORTS
bloomcheck	yetiplatform/bloomcheck:dev	"/app/bloomcheck -se..."	bloomcheck	2 days ago	Up About an hour	
yeti-api	yetiplatform/yeti:latest	"/docker-entrypoint..."	api	2 days ago	Up About an hour	0.0.0.0:8000->8000/tcp, :::8000->8000/tcp
yeti-arangodb	arangodb:3.11	"/entrypoint.sh aran..."	arangodb	2 days ago	Up 2 hours	8529/tcp
yeti-events-tasks	yetiplatform/yeti:latest	"/docker-entrypoint..."	events-tasks	2 days ago	Up About an hour	
yeti-frontend	yetiplatform/yeti-frontend:latest	"/docker-entrypoint..."	frontend	2 days ago	Up About an hour	0.0.0.0:80->80/tcp, :::80->80/tcp
yeti-redis	redis:latest	"/docker-entrypoint..."	redis	2 days ago	Up About an hour	6379/tcp
yeti-tasks	yetiplatform/yeti:latest	"/docker-entrypoint..."	tasks	2 days ago	Up About an hour	
yeti-tasks-beat	yetiplatform/yeti:latest	"/docker-entrypoint..."	tasks-beat	2 days ago	Up About an hour	

FIGURE 4.2 : Conteneurs de YETI

L'interface web de Yeti est désormais accessible via un navigateur, ce qui permet aux utilisateurs d'interagir facilement avec la plateforme pour consulter, analyser et enrichir les observables, comme illustré dans la figure suivante :

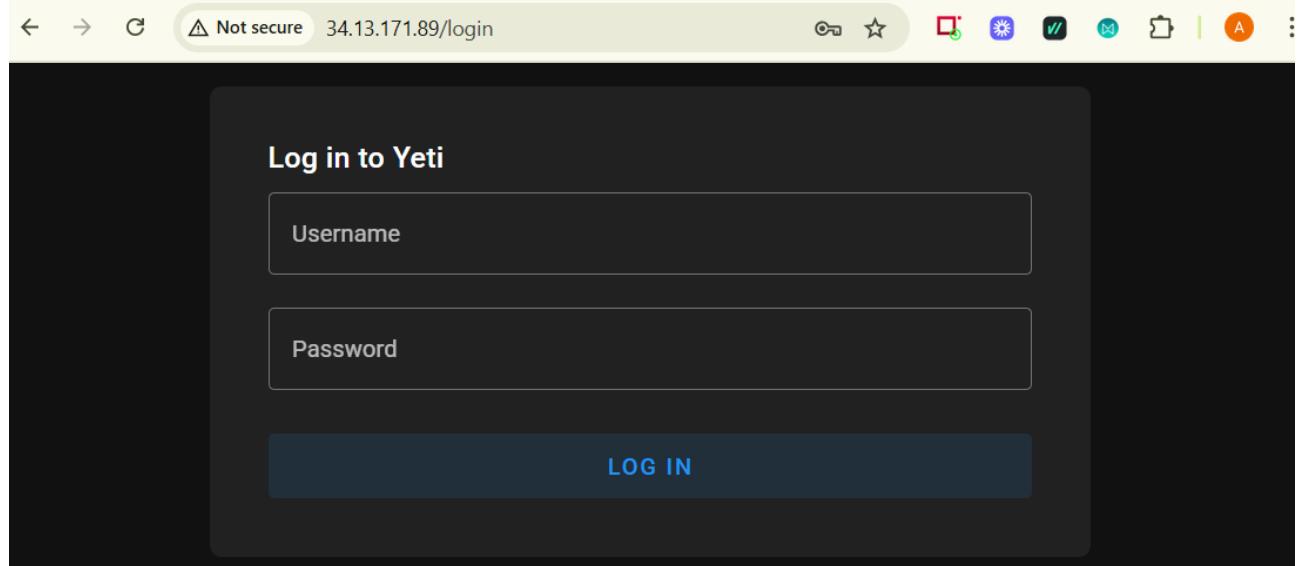


FIGURE 4.3 : Interface graphique de YETI

#### 4.2.2.1 Activation les flux dans YETI

Nous avons configuré plusieurs flux de renseignements sur les menaces dans YETI. Ces flux, tels que AbuseIPDB, AlienVaultIPReputation ou encore BlocklistdeBruteforceLogin, s'exécutent automatiquement à des intervalles réguliers pour alimenter la base de données en indicateurs de compromission (IOCs). Comme montre la figure 4.4.

Name	Runs every	Last run	Description	Status	Toggle
AbuseIPDB	5 hours	2025-06-15 13:14:03	Black List IP generated by AbuseIPDB	Completed	<input checked="" type="checkbox"/> <a href="#">C</a>
AlienVaultIPReputation	4 hours	2025-06-15 15:23:30	Reputation IP generated by AlienVault	Completed	<input checked="" type="checkbox"/> <a href="#">C</a>
AbuseIPDB	5 hours	2025-06-15 18:55:55	Black List IP generated by AbuseIPDB	Completed	<input checked="" type="checkbox"/> <a href="#">C</a>
AlienVaultIPReputation	4 hours	2025-06-15 19:23:30	Reputation IP generated by AlienVault	Completed	<input checked="" type="checkbox"/> <a href="#">C</a>
BlocklistdeBruteforceLogin	an hour	2025-06-15 19:28:12	All IPs which attacks Joomlas, Wordpress and other Web-Logins with Brute-Force Logins.	Completed	<input checked="" type="checkbox"/> <a href="#">C</a>
BlocklistdeBruteforceLogin	an hour	2025-06-15 20:28:16	All IPs which attacks Joomlas, Wordpress and other Web-Logins with Brute-Force Logins.	Completed	<input checked="" type="checkbox"/> <a href="#">C</a>

FIGURE 4.4 : Les flux de YETI

#### 4.2.2.2 Test de recherche d'un observable dans YETI

Nous avons soumis une adresse IP suspecte afin de l'identifier comme un observable de type IPv4. Les résultats affichent son origine à partir de différentes sources, telles qu'AbuseIPDB et BlocklistdeAll, ce qui permet d'évaluer sa réputation. Comme montre le résultat de la figure ci-dessous :

The screenshot shows the Yeti web interface with the URL 34.13.171.89/search. The top navigation bar includes tabs for SEARCH, OBSERVABLES, ENTITIES, INDICATORS, DFIQ, AUTOMATION, SYSTEM, and ADMIN. A search bar at the top contains the value 51.210.243.91. Below the search bar are several input fields: 'LAUNCH SEARCH', 'Regex search (expensive)', 'Tag and add missing observables', 'Guess type' dropdown, and 'Optional tags' input field. Below these are buttons for 'Related entities' (0) and 'Indicator matches' (0). The main content area is titled 'Known observables' and shows a table with one row. The table columns are Value, Type, Tags, Context, and Created (UTC). The single entry is 51.210.243.91, ipv4, with 0 tags, context showing AbuseIPDB, BlocklistdeAll, and AbuseIPDB, and created on 2025-06-08 at 01:32:14.

**FIGURE 4.5** : Résultat de la recherche d'un observable dans Yeti

#### 4.2.3 Mise en place de Cortex

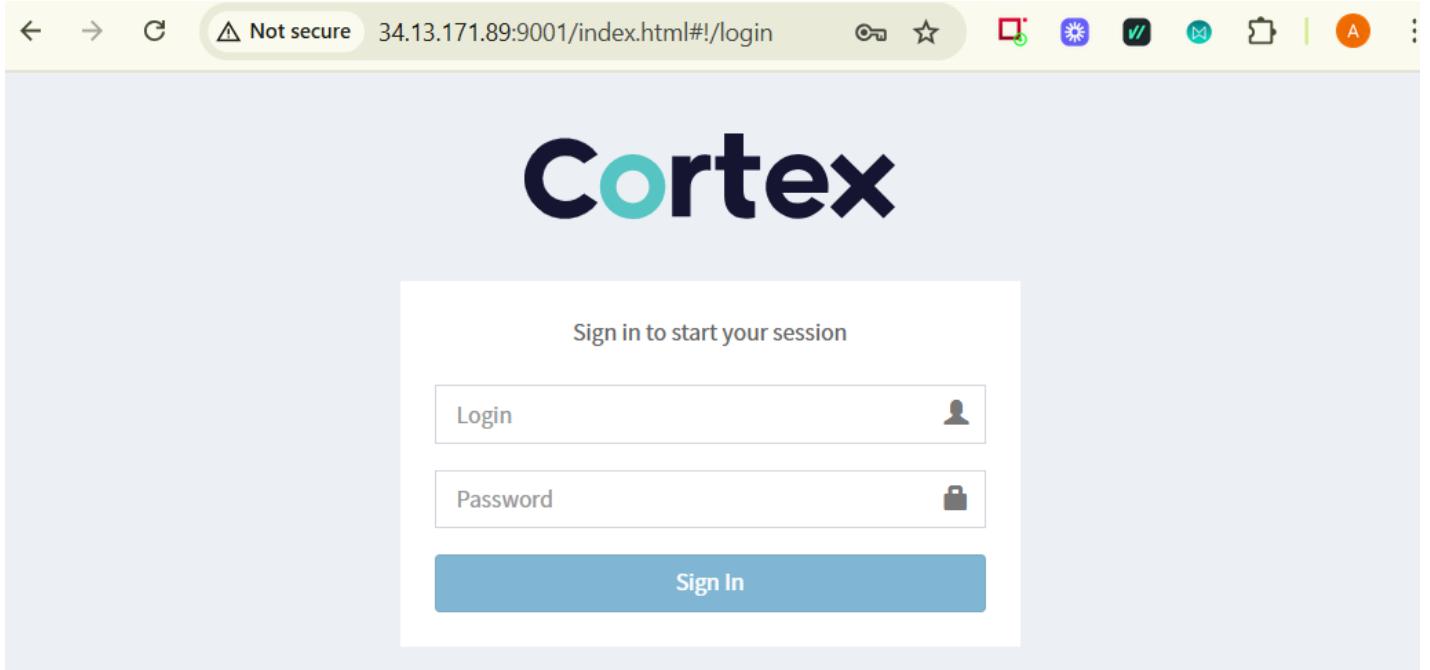
Nous avons installé Cortex en utilisant Docker pour bénéficier d'un déploiement rapide et simplifié. Cette installation containerisée facilite la gestion des mises à jour et l'intégration avec d'autres outils de sécurité. Nous avons déployé Cortex via Docker Compose en intégrant Elasticsearch afin d'assurer l'indexation des données indispensables à son bon fonctionnement.

```
daas_amall@SOAR:~/cortex$ docker compose ps
WARN[0000] /home/daas_amall/cortex/docker-compose.yml: `version` is obsolete
NAME                IMAGE               COMMAND             SERVICE            CREATED           STATUS
PORTS
cortex              thehiveproject/cortex:latest   "/opt/cortex/entrypo..."   cortex            2 weeks ago      Up 3 hours
  0.0.0.0:9001->9001/tcp
elasticsearch        elasticsearch:7.11.1       "/bin/tini -- /usr/l..."   elasticsearch    2 weeks ago      Up 3 hours
  0.0.0.0:9200->9200/tcp, 9300/tcp
```

**FIGURE 4.6** : Conteneurs de Cortex

L'interface graphique de Cortex est désormais accessible depuis un navigateur, comme illustre

la figure suivante :



**FIGURE 4.7** : Interface graphique de Cortex

#### 4.2.3.1 Configuration d'une organisation

Nous avons maintenant créé une organisation et ajouté les utilisateurs associés. Comme illustre la figure 4.8.

Status	Organization	Edit	Disable
Active	SOC_ORG		
Active	cortex		

**FIGURE 4.8** : Configuration d'une organisation dans Cortex

#### 4.2.3.2 Configuration des analyseurs

En utilisant le compte qui nous avons crée dans l'organisation SOC\_ORG, nous avons configuré plusieurs analyseurs afin de traiter différents types d'IOC. Comme présenté dans la figure suivante, nous avons sélectionné les analyseurs AbuseIPDB\_1\_0, VirusTotal\_GetReport\_3\_1 et Yeti\_1\_0, dans le but d'enrichir les données collectées et de renforcer l'efficacité de la détection des menaces.

The screenshot shows the Cortex Analyzers interface. At the top, there are tabs for 'Jobs History', 'Analyzers' (which is selected), 'Responders', and 'Organization'. A user profile icon 'SOC\_ORG/amal' is also at the top right. Below the tabs, the title 'Analyzers (3)' is displayed. There are filters for 'Data Types (6)' (Select dropdown, Search input, Search button, Clear button, Page size dropdown set to '50 / page') and a search bar ('Search for analyzer description'). Three analyzers are listed:

- AbuseIPDB\_1\_0**: Version: 1.0, Author: Matteo Lodi, License: AGPL-v3. Description: Determine whether an IP was reported or not as malicious by AbuseIPDB. Applies to: ip. Run button.
- VirusTotal\_GetReport\_3\_1**: Version: 3.1, Author: CERT-BDF, StrangeBee, License: AGPL-V3. Description: Get the latest VirusTotal report for a file, hash, domain or an IP address. Applies to: file, hash, domain, fqdn, ip, url. Run button.
- Yeti\_1\_0**: Version: 1.0, Author: CERT-BDF, License: AGPL-V3. Description: Fetch observable details from a YETI instance. Applies to: domain, fqdn, ip, url, hash. Run button.

FIGURE 4.9 : Analyseurs de Cortex

#### 4.2.4 Mise en place de TheHive

##### 4.2.4.1 Installation de TheHive

Nous avons mis en place TheHive sous forme d'un conteneur Docker afin de faciliter son déploiement et sa gestion. En utilisant l'image officielle, nous avons configuré les volumes pour assurer la persistance des données et défini les variables d'environnement nécessaires au bon fonctionnement. Cette approche nous a permis d'obtenir une installation rapide, flexible et facilement maintenable.

```
daas_amall@manager-vm:~$ docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED      STATUS      PORTS
                   NAMES
8ace9c6b6efb   strangebee/thehive:5.4.4-1   "/opt/thehive/entryp..."   2 weeks ago   Up 2 days   0.0.0.0:9000->9000
/tcp, [::]:9000->9000/tcp   thehive
```

FIGURE 4.10 : Conteneur de TheHive

L'interface de TheHive dans la figure ci-dessous :

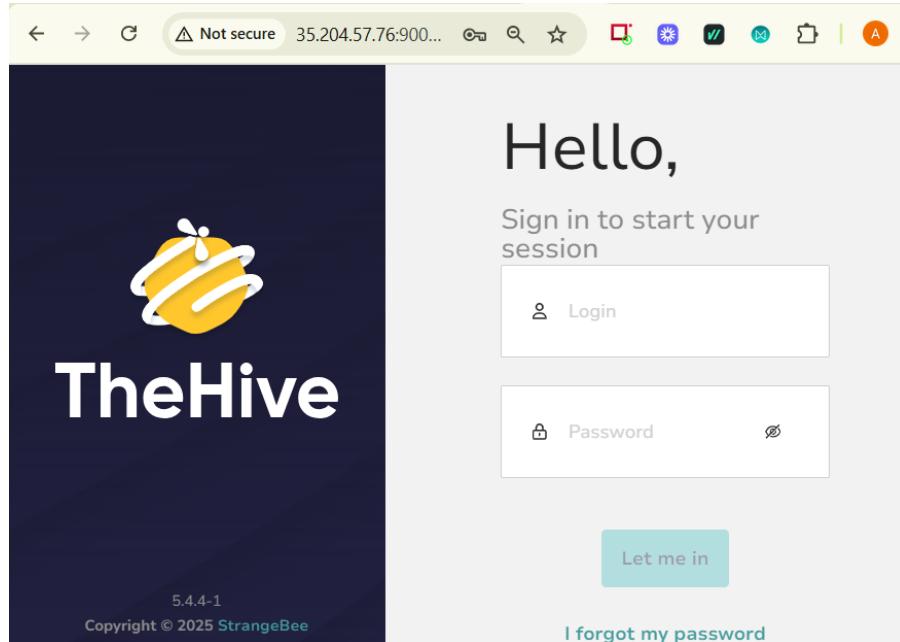


FIGURE 4.11 : Interface de TheHive

Nous avons maintenant crée une organisation comme montre la figure suivante :

	Name	Created by	Created date
<input type="checkbox"/>	admin	TheHive system user	29/05/2025 11:05
<input type="checkbox"/>	SOC_ORG	admin@thehive.local	29/05/2025 13:07

FIGURE 4.12 : Crédation d'une organisation dans TheHive

Ensuite, nous avons crée un utilisateur avec le profil "org\_admin" pour cette organisation.

	Details	Full Name	Login	Profile	MFA	Dates
<input type="checkbox"/>	A	amal	amal	org-admin	off	C. 29/05/2025 13:08 U. 29/05/2025 13:08

FIGURE 4.13 : Crédation d'un utilisateur dans TheHive

#### 4.2.4.2 Intégration avec Cortex

#### 4.2.5 Mise en place de Shuffle

Nous avons créé un fichier Docker Compose définissant une architecture multi-services pour déployer la plateforme Shuffle. Ce déploiement comprend plusieurs services essentiels, notamment le backend, le frontend, le gestionnaire de workflows Orborus, ainsi qu'un moteur de recherche OpenSearch utilisé pour l'indexation et la recherche des données. Chaque service est conteneurisé et exposé sur les ports nécessaires afin de garantir une communication fluide entre les composants et un accès depuis l'extérieur de la machine.

NAME	IMAGE	COMMAND	SERVICE	CREATED
STATUS	PORTS			
shuffle-backend	ghcr.io/shuffle/shuffle-backend:latest	"/webapp"	backend	2 weeks ago
Up 16 minutes	0.0.0.0:5001->5001/tcp, [::]:5001->5001/tcp			
shuffle-frontend	ghcr.io/shuffle/shuffle-frontend:latest	"/entrypoint.sh nginx..."	frontend	2 weeks ago
Up 16 minutes	0.0.0.0:3001->80/tcp, [::]:3001->80/tcp, 0.0.0.0:3443->443/tcp, [::]:3443->443/tcp			
shuffle-opensearch	opensearchproject/opensearch:2.19.1	"/opensearch-docker..."	opensearch	2 weeks ago
Up 16 minutes	9300/tcp, 9600/tcp, 0.0.0.0:9200->9200/tcp, [::]:9200->9200/tcp, 9650/tcp			
shuffle-orborus	ghcr.io/shuffle/shuffle-orborus:latest	"/orborus"	orborus	2 weeks ago
Up 16 minutes				

FIGURE 4.14 : Conteneurs de Shuffle

#### 4.2.5.1 Configuration du nom de domaine

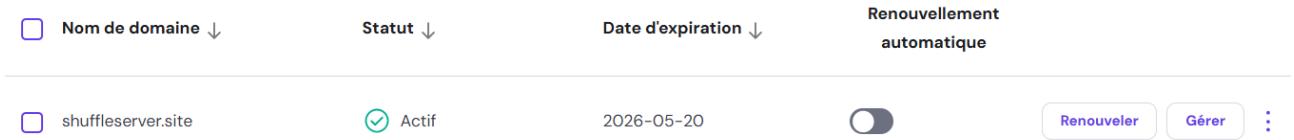


FIGURE 4.15 : Association d'un nom de domaine

Pour rendre notre plateforme Shuffle accessible depuis Internet, nous avons associé une adresse IP publique à un nom de domaine personnalisé : shuffleserver.site. Cette configuration permet aux utilisateurs d'accéder facilement à l'orchestrateur via une URL dédiée, plutôt qu'une simple adresse IP, facilitant ainsi l'intégration dans un environnement sécurisé et professionnel.

#### 4.2.5.2 Reverse proxy

Un reverse proxy est un serveur intermédiaire qui reçoit les requêtes des clients et les redirige vers les serveurs internes appropriés. Il agit comme point d'entrée unique, masquant la structure interne du réseau. Il permet également de gérer le chiffrement SSL, la répartition de charge, la sécurité et le contrôle d'accès.

```
server {
    server_name shuffleserver.site;

    location / {
        proxy_pass https://localhost:3443;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_ssl_verify off;
    }

    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/shuffleserver.site/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/shuffleserver.site/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}

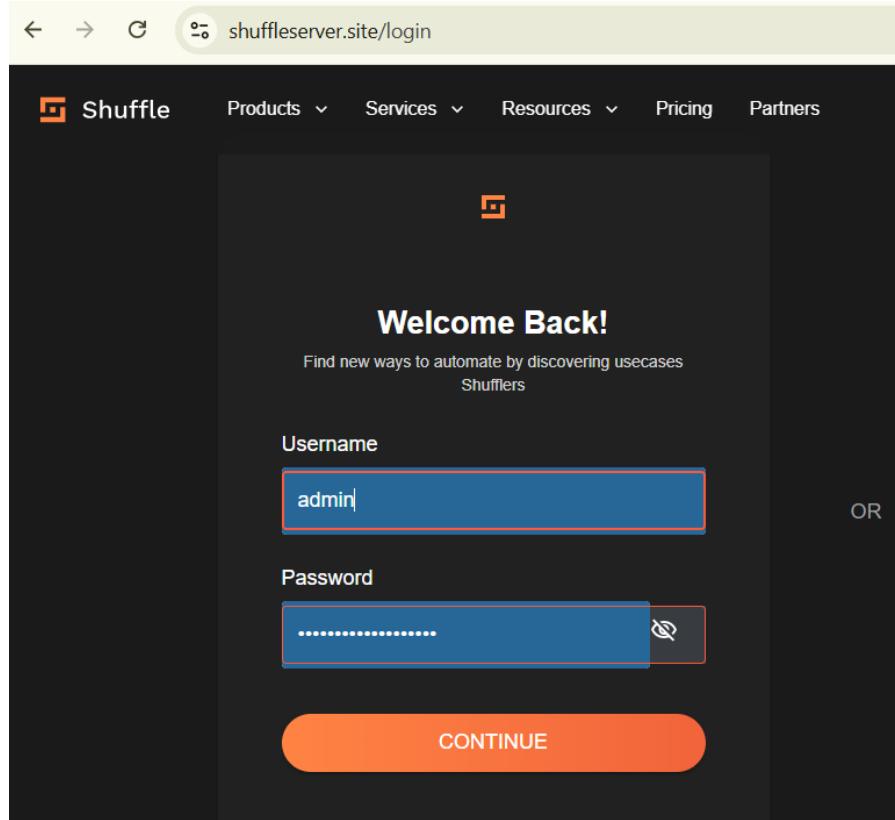
server {
    if ($host = shuffleserver.site) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    listen 80;
    server_name shuffleserver.site;
    return 404; # managed by Certbot
}
```

FIGURE 4.16 : Reverse proxy Nginx

Cette figure montre une configuration NGINX utilisant un reverse proxy pour sécuriser l'accès à Shuffle via le domaine shuffleserver.site, en redirigeant les requêtes HTTPS vers le service local sur le port 3443.

L'interface de Shuffle :

**FIGURE 4.17 :** Interface de Shuffle

#### 4.2.5.3 Intégration avec Wazuh

Dans notre solution, les alertes générées par le SIEM Wazuh déclenchent automatiquement des workflows dans Shuffle grâce à l'utilisation de webhooks configurés sur mesure. Chaque webhook est associé à une règle spécifique de Wazuh, permettant d'envoyer uniquement les alertes pertinentes vers l'URL dédiée de Shuffle. Cette intégration assure une automatisation ciblée et un traitement rapide des incidents détectés. Comme illustre la figure ci-dessous :

```
<integration>
<name>shuffle</name>
<hook_url>https://shuffleserver.site/api/v1/hooks/webhook_41cc823d-dee2-4a35-b6e1-a77e687aebc2</hook_url>
<rule_id>86601</rule_id>
<alert_format>json</alert_format>
</integration>
```

**FIGURE 4.18 :** Intégration de Wazuh avec Shuffle

#### 4.2.5.4 Intégration avec ZohoMail

Mes configurations	Aide	
Nom du webhook	URL de webhook	
Outgoing Webhook Bot	https://shuffleserver.site/api/v1/hoo...	
	<input type="button" value="Copier"/>	<input checked="" type="checkbox"/>

**FIGURE 4.19 :** Intégration avec ZohoMail

Cette Figure montre l'intégration d'un webhook Sortant dans Zoho Mail, utilisé pour connecter la messagerie à la plateforme Shuffle.

#### 4.2.5.5 Intégration avec TheHive

Pour connecter Shuffle à TheHive, nous avons configuré l'authentification en renseignant la clé API, l'URL de l'instance. Cela permet à Shuffle d'interagir avec TheHive pour automatiser la gestion des incidents via ses workflows. La figure suivante montre l'intégration de Shuffle avec TheHive :

**Authentication for TheHive**

**What is app authentication?**  
These are required fields for authenticating with TheHive

**Label for you to remember**

TheHive

**apikey**

.....

**url**

http://35.204.57.76:9000/

**SUBMIT**

**FIGURE 4.20 :** Intégration avec TheHive

#### 4.2.5.6 Intégration avec YETI

L'intégration de Yeti avec Shuffle permet d'automatiser l'enrichissement des indicateurs de menace au sein des workflows. En connectant l'API de Yeti à Shuffle, ce dernier peut interroger la base CTI pour récupérer des informations contextuelles sur les observables. Cette automatisation renforce l'analyse des alertes et améliore la prise de décision en réponse aux incidents.

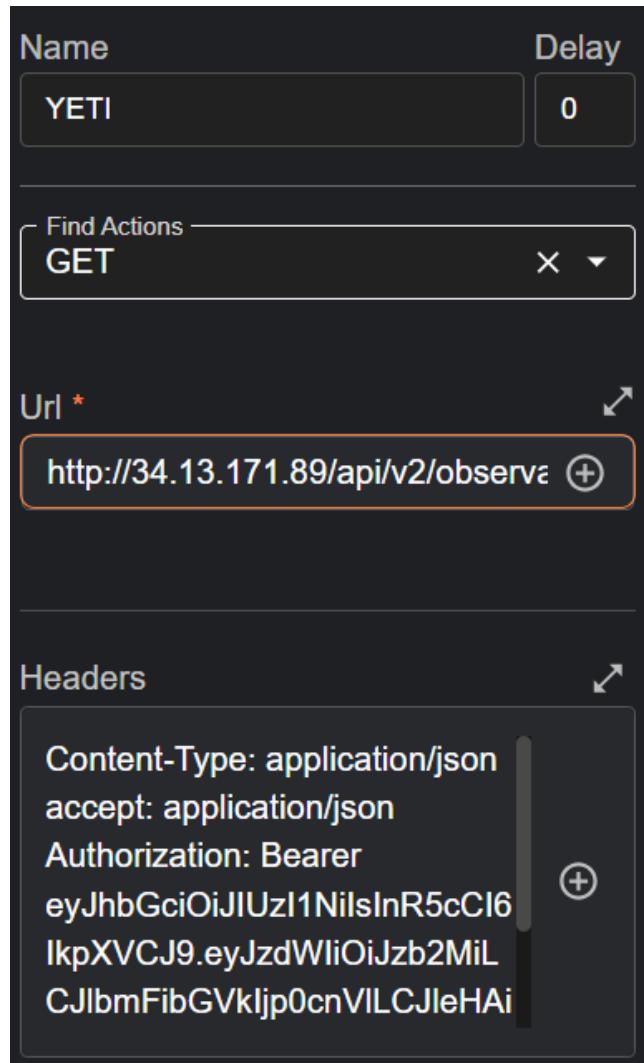


FIGURE 4.21 : Intégration avec YETI

#### 4.2.5.7 Intégration avec LLM

L'intégration d'un LLM (Large Language Model) avec Shuffle permet d'analyser et résumer automatiquement les alertes ou les rapports de sécurité dans les workflows. Grâce à des appels API vers le modèle, Shuffle peut générer des réponses contextualisées, des classifications ou des suggestions d'actions. Cette automatisation améliore l'efficacité de la réponse aux incidents et réduit la charge d'analyse manuelle.

Dans notre cas, nous avons opté pour l'utilisation du LLM LLAMA3.

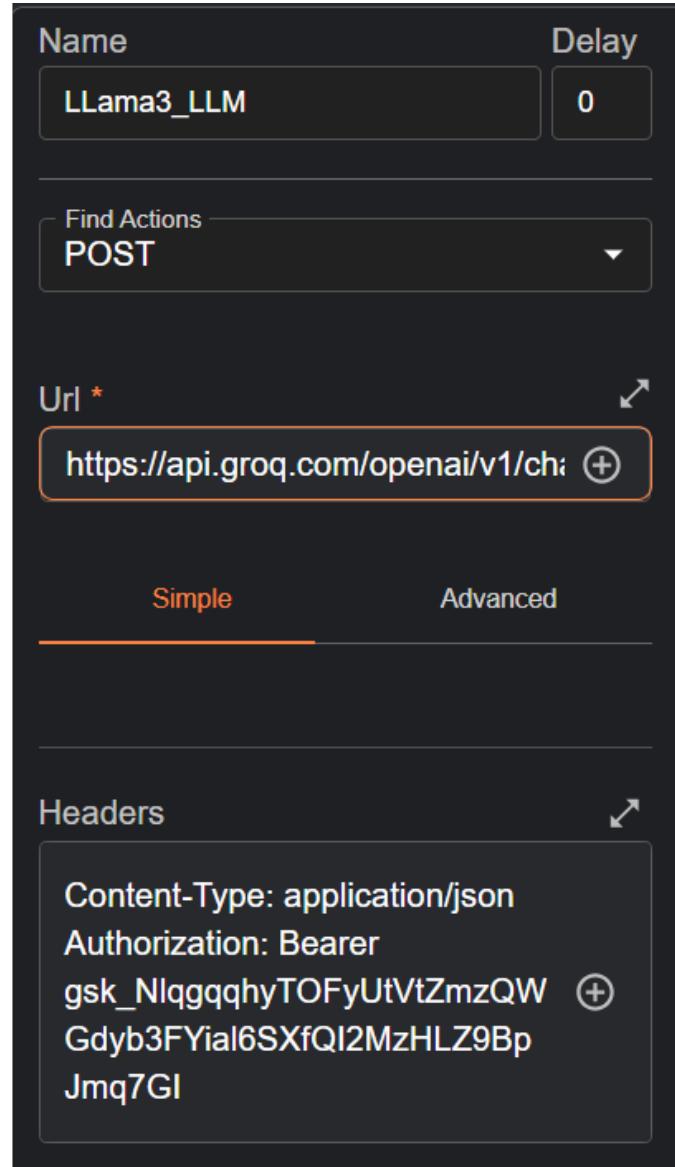


FIGURE 4.22 : Intégration avec LLM

Nous avons maintenant créé un prompt via l’application HTTP, en utilisant une requête POST pour l’envoyer vers LLAMA3\_LLM. Le contenu de la requête est illustré dans la figure ci-dessous :

```
{"model":"llama-3.3-70b-versatile","messages": [{"role":"user","content":"You are an expert security analyst specializing in Suricata IDS/IPS alert analysis and incident response. Your task is to analyze Suricata security alerts and provide clear, concise, and actionable intelligence to security teams.\n\nWhen presented with a Suricata alert, you will:\n1. THOROUGHLY analyze all fields within the alert, paying special attention to:\n  - Suricata rule signature and SID\n  - Source/destination IPs and ports\n  - Protocol information and payload data\n  - Alert classification and category\n  - Flow information and packet details\n  - Rule logic and detection method\n  - Any additional context provided in the alert\n2. Provide an analysis with the following structure:\n**Alert Summary**\n  - Provide a clear, concise explanation of what happened in non-technical language\n  - Identify the type of security event detected by Suricata rule\n  - Highlight the most critical aspects of the alert\n  - Explain what the Suricata rule is designed to detect\n**Security Implications**\n  - Assess the potential severity (Critical, Medium, Legitimate)\n  - Explain possible attacker motivations or attack chain positioning\n  - Detail potential impact to systems, data, or operations\n  - Note if this appears to be part of a larger attack pattern\n  - Identify any known CVEs or attack techniques (MITRE ATT&CK) being leveraged\n  - Describe the rule logic and detection method\n**Recommended Actions**\nBased on the severity assessment:\nFOR CRITICAL ALERTS:\n  - BLOCK THIS IP ADDRESS IMMEDIATELY - High priority security threat\n  - Provide specific firewall/blocking commands\n  - List exact commands to run for verification\n  - Specify files to check and their locations\n  - Suggest immediate containment or remediation steps\n  - Recommend urgent escalation to security team\nFOR MEDIUM ALERTS:\n  - Analyze and provide mitigation solutions\n  - RECOMMEND BLOCKING THIS IP ADDRESS if you want additional security\n  - List exact commands to run for verification\n  - Specify files to check and their locations\n  - Enhanced monitoring and logging recommended\n  - Recommend whether escalation is needed\nFOR LEGITIMATE ALERTS:\n  - Acknowledge the traffic may be legitimate business activity\n  - Explain why this triggered the detection rule\n  - YOU ARE NOT OBLIGATED TO BLOCK THIS ADDRESS for normal operations\n  - However, if this IP address appears in international threat intelligence databases or known malicious IP lists, RECOMMEND BLOCKING IT anyway as a precautionary measure\n  - List exact commands to run for verification\n  - Check threat intelligence sources before making final decision\n\nYour analysis should be thorough but prioritize actionable intelligence over theory. Be specific with your recommendations and include exact commands when helpful. All advice should follow security best practices"}]
```

FIGURE 4.23 : Prompt LLM – Attaque réseau

```
{"model":"llama-3.3-70b-versatile","messages": [{"role":"user","content":"Analyse cet email pour détecter uniquement les vraies menaces de phishing.\n\nUn email est MALVEILLANT seulement si:\n- Expéditeur usurpe une identité connue\n- Demande des mots de passe ou données bancaires\n- Liens vers des domaines suspects ou raccourcis malveillants\n- Pièces jointes exécutables suspectes\n- Headers montrent une falsification\n\nUn email est LEGITIME si:\n- Expéditeur correspond au domaine\n- Liens vers des sites officiels ou connus\n- Contenu cohérent avec l'expéditeur\n- Pas de demande d'informations sensibles\n\nNe considère PAS comme malveillant:\n- Emails commerciaux normaux\n- Liens vers des sites légitimes\n- Newsletters\n- Notifications de services\n\nRéponds :\n\nSTATUS: MALVEILLANT ou LEGITIME\nRAISON: [Pourquoi en une phrase]\nSCORE: [1-10 où 1=très sûr, 10=très suspect]\nEmail:\n$message"}]}
```

FIGURE 4.24 : Prompt LLM – Attaque Phishing

#### 4.2.5.8 Intégration avec Slack

L'intégration de Slack avec Shuffle permet d'automatiser la communication et la gestion des alertes de sécurité directement via les canaux Slack. Grâce à cette connexion, Shuffle peut envoyer des notifications et orchestrer des workflows en temps réel, améliorant ainsi la collaboration entre les équipes. Cette intégration facilite une réponse rapide et coordonnée face aux incidents.

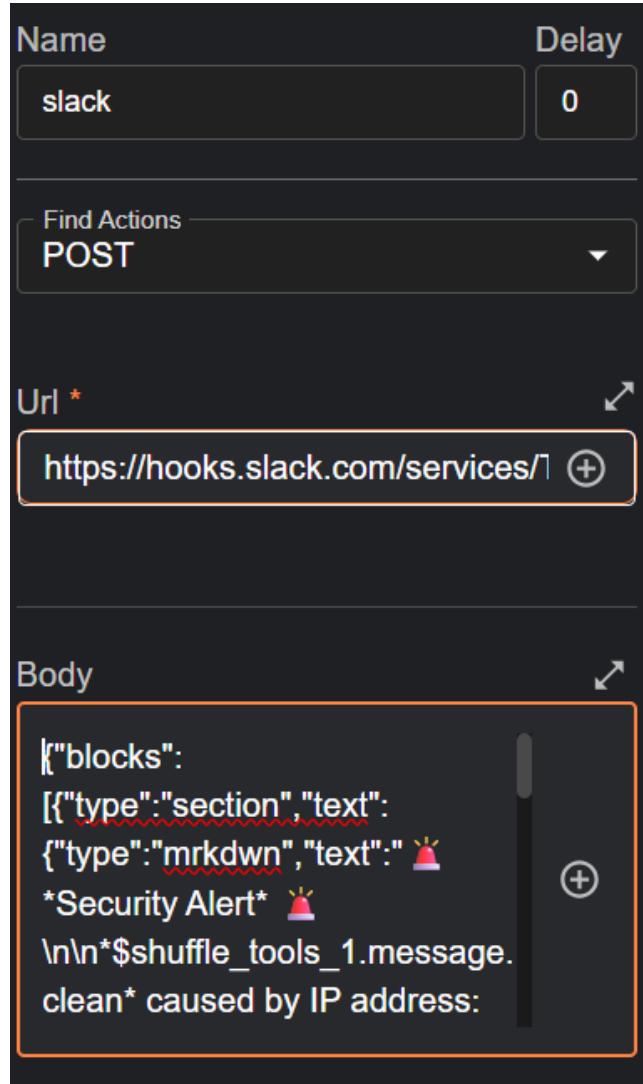


FIGURE 4.25 : Intégration avec Slack

Voici le message que Slack envoie lorsqu'une attaque est détectée dans le réseau.

```
{"blocks": [{"type": "section", "text": {"type": "mrkdwn", "text": "*Security Alert* 🚨\n\n*$shuffle_tools_1.message.clean* caused by IP address: '$shuffle_tools_1.message.ip`\n\nWould you like to ban this IP address ?"}}, {"type": "actions", "elements": [{"type": "button", "text": {"type": "plain_text", "text": "✓ Continue"}, "style": "primary", "url": "https://shuffleserver.site$frontend_continue.value"}, {"type": "button", "text": {"type": "plain_text", "text": "🚫 Abort"}, "style": "danger", "url": "https://shuffleserver.site$frontend_abort.value"}]}, {"type": "section", "text": {"type": "mrkdwn", "text": ":link: *Related CTI Report*: \n<https://app.slack.com/client/T085KNY1491/C090ZFU9ECW| View full YETI CTI Report>"}]}]
```

FIGURE 4.26 : Contenu de la notification Slack - Attaque réseau

Ainsi le contenu du message Slack lorsqu'une alerte de phishing est détectée.

```
{"blocks": [{"type": "header", "text": {"type": "plain_text", "text": "⚠️ Phishing Alert - TheHive Case"}}, {"type": "section", "text": {"type": "mrkdwn", "text": "* ⚡ Case link: *\n\n<http://35.204.57.76:9000/cases/$create_case_from_alert.body._id|Voir le cas dans TheHive>"}]}]
```

FIGURE 4.27 : Contenu de la notification Slack - Attaque de Phishing

#### 4.2.5.9 Intégration de la réponse active de Wazuh

Nous avons intégré l'action de Wazuh (Active Response) pour bloquer une adresse malveillante en utilisant la commande firewall-drop.

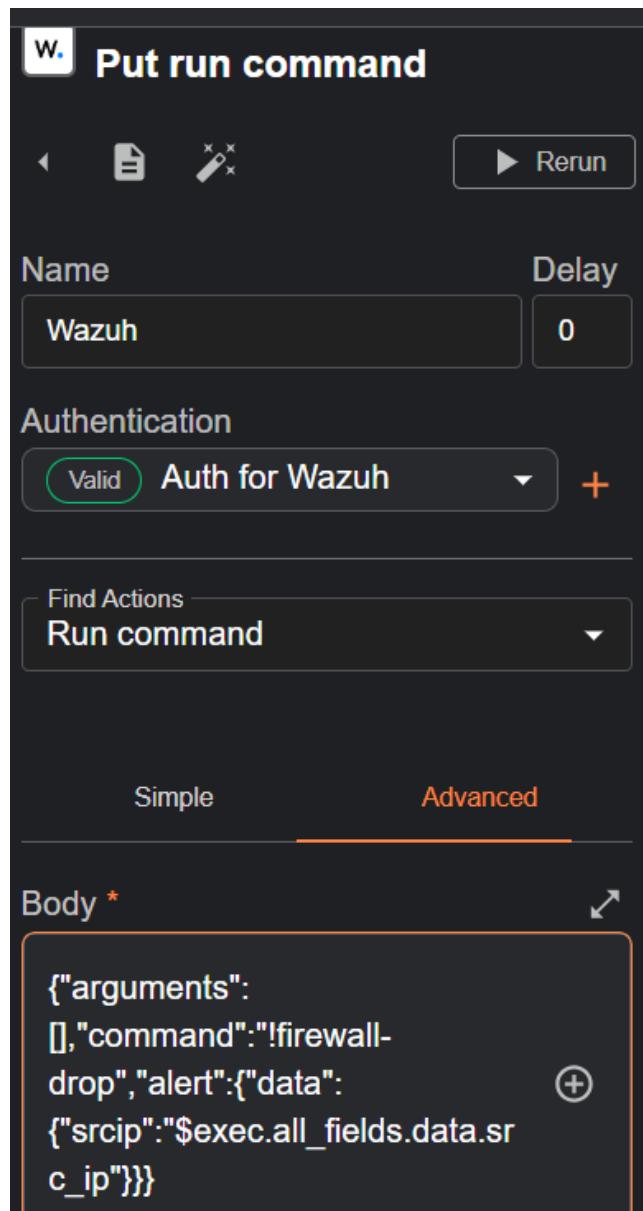
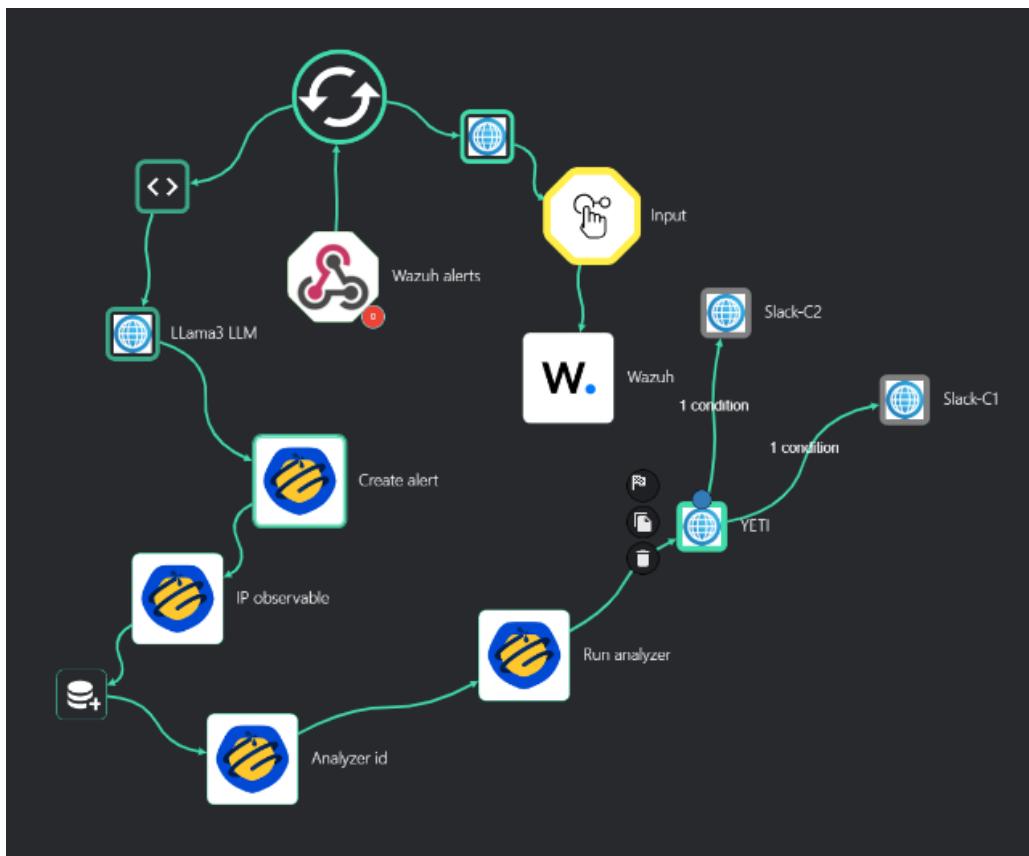


FIGURE 4.28 : Réponse Active de Wazuh

#### 4.2.6 Scénario de test 1 : Attaque sur le réseau

Le workflow présenté ci-dessous permet d'automatiser le traitement des alertes générées par Wazuh, en particulier celles issues de Suricata. Lorsqu'une alerte est détectée, elle est transmise à LLAMA3\_LLM via un prompt configuré par un script Python, afin de produire une description claire et compréhensible. Cette description est ensuite utilisée pour créer une alerte dans TheHive. L'adresse IP concernée est extraite comme observable, puis analysée à l'aide des analyseurs Cortex intégrés à TheHive. Pour un enrichissement supplémentaire, l'adresse est transmise à YETI afin d'évaluer sa réputation à travers différentes bases de données de Threat Intelligence. Si l'adresse est jugée malveillante, un rapport est automatiquement envoyé vers Slack, indiquant la source de détection. Ensuite, l'application User Input permet à l'utilisateur de décider s'il souhaite bloquer ou ignorer cette adresse. En cas de décision de blocage, Wazuh déclenche une réponse active à l'aide de la commande firewall-drop.



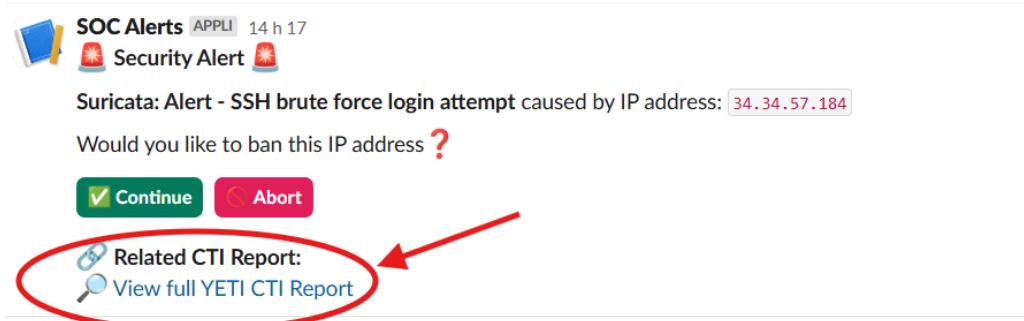
**FIGURE 4.29 :** Workflow pour la détection des attaques dans le réseau

Nous passons à la phase de simulation de l'attaque par Brute Force à l'aide de la boucle for de la commande ssh, comme illustre la figure ci-dessous :

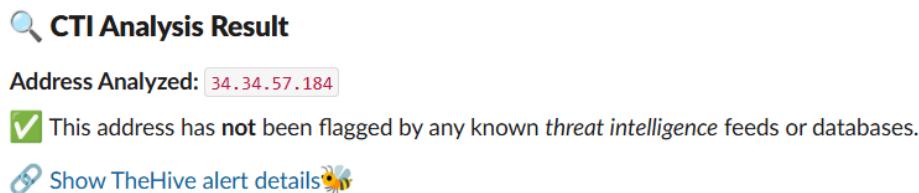
```
daas_amall@test-vm:~$ for i in {1..6}; do ssh kk@34.13.171.89 ; done
kk@34.13.171.89: Permission denied (publickey).
```

**FIGURE 4.30 :** Attaque par Brute Force

Une alerte générée via Slack indique l'adresse IP de l'attaquant ainsi que la décision prise concernant le blocage ou l'ignorance de cette adresse, comme la figure 4.31.

**FIGURE 4.31 :** Notification de Slack

Un simple clic sur le lien permet d'accéder aux informations relatives à cette adresse dans les bases de données de Threat Intelligence. Comme le montre la figure 4.31, aucune source de Threat Intelligence n'a identifié cette adresse IP comme malveillante.

**FIGURE 4.32 :** Résultat de YETI

Lorsqu'une adresse est reconnue comme malveillante, par exemple une adresse identifiée dans une base de Threat Intelligence, le rapport de YETI la marque comme telle dans la blocklist. Comme la figure suivante :

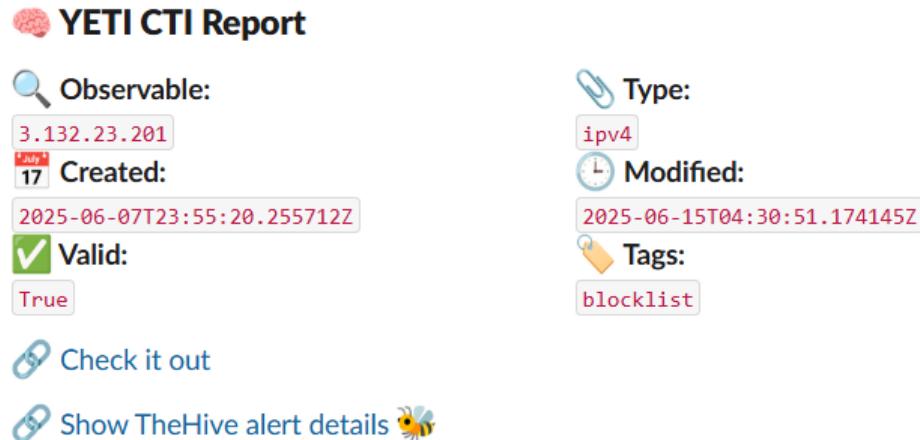


FIGURE 4.33 : Rapport de YETI

Dans ce cas, l'alerte générée peut être consultée dans TheHive en cliquant sur le lien "Show TheHive alert details" pour voir La description de l'alerte générée par le LLAMA3\_LLM, comme montre la figure 4.34.

The screenshot shows the TheHive alert details page for an SSH Brute Force attack. The alert ID is 88965232. The alert summary states: "A Suricata alert was triggered for a potential SSH Brute Force attack detected from source IP address 51.210.243.91 to destination IP address 10.164.0.5 on port 22. The Suricata rule with ID 86601 and signature ID 1000001 detected this activity, which falls under the category of Misc activity. This rule is designed to detect brute force attempts on SSH servers, indicating potential malicious activity aimed at guessing login credentials. The most critical aspect of this alert is the repeated attempts to access the SSH server, suggesting a potential security threat." The security implications section notes that the severity is Critical and describes the potential impact. The recommended actions section provides instructions to block the IP address. The comments section has a placeholder "Type a comment...".

Suricata: Alert - SSH Brute Force detected	
id ~88965232	
Created by amal	
Created at 15/06/2025 16:53	
SEVERITY:MEDIUM	
TLP:AMBER	PAP:AMBER
Assignee <a href="#">Assign to me</a>	
Unassigned	
Source Wazuh	
Reference 1750002789.5246152	
Type ip	
Occurred date 15/06/2025 16:53	
Status Pending	
Time metrics	
Detection < 1 second	Triage < 1 second

FIGURE 4.34 : Description de l'alerte

Cette alerte inclut la création de l'observable, où les résultats des analyseurs de Cortex sont accessibles, l'adresse est considérée comme légitime dans notre cas, comme représenté par la figure 4.31

The screenshot shows the Cortex interface with the 'Observables (1)' tab selected. A single observable is listed: an IP address (34.34.57.184) with flags TLP:AMBER and PAP:AMBER. The data type is 'ip'. Below the IP address, several analysis results are shown in colored boxes: AbuseIPDB:Records=0 (green), AbuseIPDB:Abuse Confidence Score... (green), AbuseIPDB:Usage Type="Data Cente..." (green), VT:GetReport="0/94" (blue), and VT:GetReport="1 resolution(s)" (orange). The timestamp for the alert is S. 16/06/2025 20:25, and the creation timestamp is C. 16/06/2025 20:25.

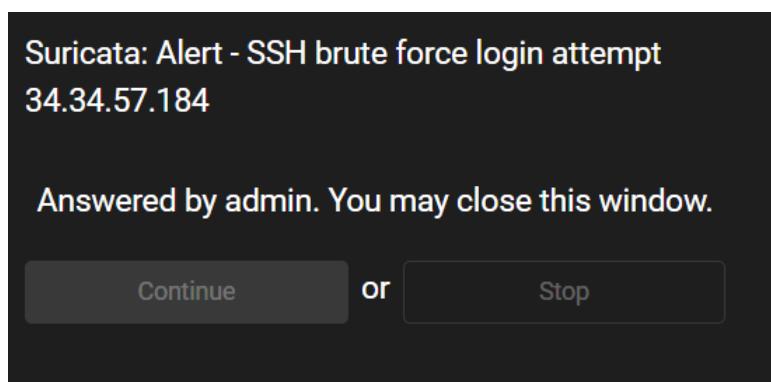
**FIGURE 4.35 :** Observables de l'alerte d'une adresse légitime

Si une adresse est considérée comme malveillante, Voici les résultats des analyseurs exécutés via Cortex.

The screenshot shows the Cortex interface with the 'Observables (1)' tab selected. A single observable is listed: an IP address (3.132.23.201) with flags TLP:AMBER and PAP:AMBER. The data type is 'ip'. Below the IP address, several analysis results are shown in colored boxes: AbuseIPDB:Abuse Confidence Score... (orange), AbuseIPDB:Records="2242" (red), AbuseIPDB:Usage Type="Data Cente..." (green), VT:GetReport="5 resolution(s)" (red), and VT:GetReport="9/94" (red). The timestamp for the alert is S. 16/06/2025 20:25, and the creation timestamp is C. 16/06/2025 20:25.

**FIGURE 4.36 :** Observables de l'alerte d'une adresse malveillante

Comme illustré dans la figure 4.37, une règle a été mise en place au niveau du Wazuh pour bloquer l'adresse IP de l'attaquant.



**FIGURE 4.37 :** Action de blocage d'une adresse IP malveillante

Comme nous pouvons le constater, l'adresse a été ajoutée aux règles iptables.

```
daas_amall@web-cloud:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP      all  --  184.57.34.34.bc.googleusercontent.com  anywhere
```

FIGURE 4.38 : Liste des règles iptables

#### 4.2.7 Scénario de test 2 : Attaque de Phishing

Le workflow traite automatiquement les e-mails suspects de phishing reçus via Zoho Mail. Lorsqu'un nouveau message est reçu, son contenu est analysé par LLAMA3 afin de détecter toute intention malveillante ou la présence de données sensibles, à l'aide d'un prompt configuré par un script Python. En cas de menace, une alerte est générée dans TheHive, enrichie par l'analyse de LLAMA3 pour mieux comprendre le contenu du message, avec la création d'un cas contenant l'e-mail comme observable. Si des URL sont détectées, elles sont analysées par Cortex ; si elles sont jugées malveillantes, une alerte est envoyée via Slack et le message est marqué comme spam.

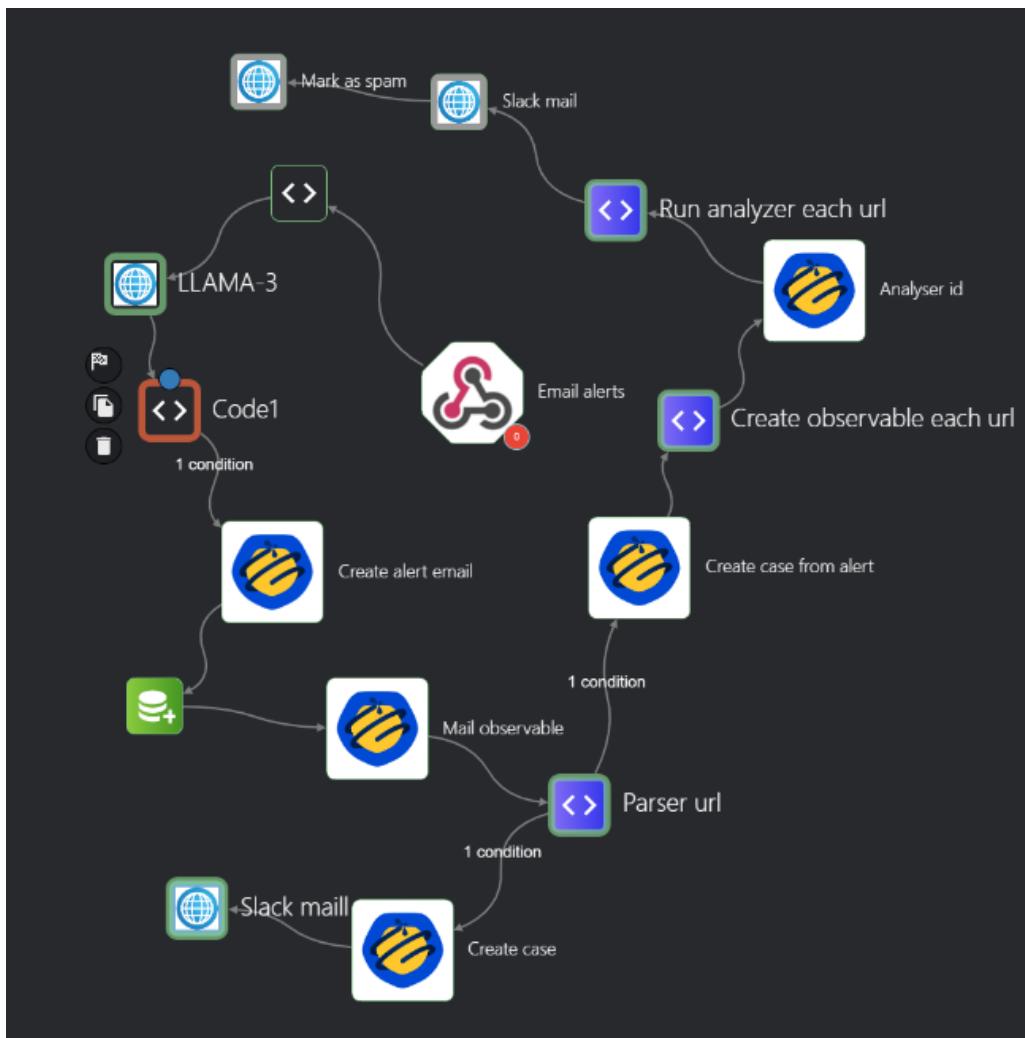
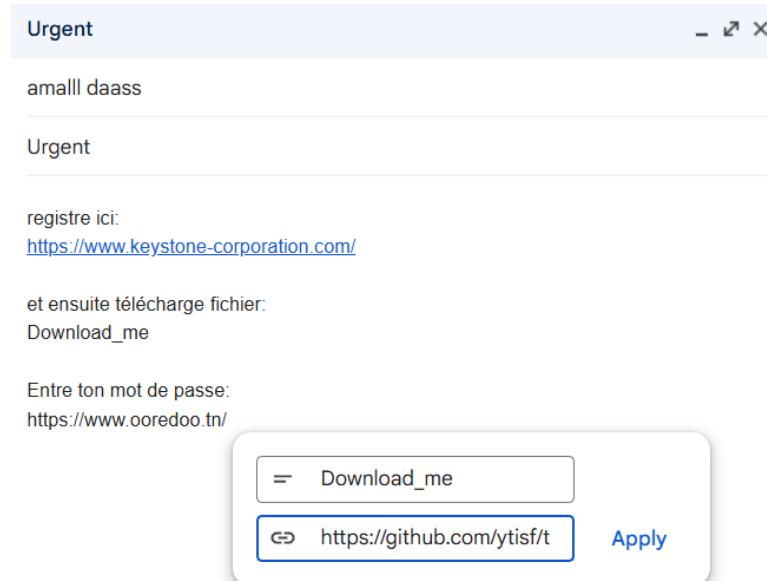


FIGURE 4.39 : Workflow pour la détection des attaques de Phishing

Nous passons maintenant à la phase d'envoi d'un e-mail malveillant, dans lequel une URL malveillante est dissimulée sous le nom « Download\_me », afin de vérifier si le LLM détecte correctement son contenu, voici la figure ci-dessous :



**FIGURE 4.40 :** Envoi un nouveau mail

Nous avons reçu une alerte dans TheHive contenant l'analyse générée par LLAMA3, comme le montre dans la figure 4.41.

**\* Title**  
Phising\_email

**Tags**

**Description**

STATUS: MALVEILLANT  
RAISON: L'email demande d'entrer un mot de passe sur un lien fourni et propose de télécharger un fichier suspect, ce qui sont des indicateurs de phishing.  
SCORE: 8  
Raisonnement détaillé :

- L'expéditeur demande d'entrer un mot de passe sur un lien fourni, ce qui est un indicateur de phishing.
- Le lien 'Download\_me' pointe vers un dépôt GitHub contenant des binaires de malware, ce qui est suspectif.
- L'email demande des informations sensibles (le mot de passe).
- Le fait que l'email demande de télécharger un fichier suspect et d'entrer un mot de passe sur un lien fourni sont des indicateurs de phishing.
- Le lien vers le site de Keystone Corporation semble légitime, mais le contexte dans lequel il est utilisé (en combinaison avec la demande de mot de passe et le téléchargement d'un fichier suspect) le rend suspect.
- Le lien vers le site d'Ooredoo Tunisia semble également légitime, mais la demande d'entrer un mot de passe sur ce site est anormale et constitue un indicateur de phishing.

**Summary**  
urgent

**FIGURE 4.41 :** Alert de TheHive

Le contenu de l'e-mail contient des URLs. Un cas lié à l'alerte a été créé avec les observables correspondants (voir figure 4.42).

Tasks	0
Observables	4
TTPs	0
Linked Alerts	1

**FIGURE 4.42 :** Crédit d'un cas dans TheHive

Les observables de type URL sont analysés par Cortex, comme illustré dans la figure suivante :

URL	VT:GetReport Result
hxps://www[.]keystone-corporation[.]com	0/96
hxps://github[.]com/ytisf/theZoo/tree/master/malware/Binaries/Keylogger[.]Ardamax	3/89
hxps://www[.]ooredoo[.]tn	0/96
daas[.]jamall@gmail[.]com	No report(s) available

**FIGURE 4.43 :** Analyse des URLs par Cortex

Nous avons maintenant une notification dans Slack contenant le lien vers le cas dans TheHive, comme montré dans la figure ci-dessous :



**FIGURE 4.44 :** Notification de Slack

D'après l'analyse des URLs, le message sera marqué comme spam.

## Conclusion

L'intégration de TheHive, Cortex, YETI, LLAMA3 et Shuffle dans notre solution SOAR a permis d'automatiser l'ensemble du cycle de gestion des incidents. YETI fournit une base de renseignement sur les menaces, tandis que LLAMA3 interprète les alertes et en génère des descriptions claires pour faciliter leur traitement. Grâce à Shuffle, les différents outils communiquent efficacement, assurant une réponse structurée et rapide face aux incidents. Cette approche améliore significativement notre capacité de détection et de remédiation tout en réduisant la charge opérationnelle.

# MISE EN PLACE D'UNE SOLUTION D'AUTOMATISATION DES TESTS DE SÉCURITÉ

---

## Plan

Introduction . . . . .	83
1    Mise en place de Caldera . . . . .	83
2    Simulations des scénarios de tests dans le SOC . . . . .	87
3    Simulation de tests automatiques sur le workflow . . . . .	92
Conclusion . . . . .	95

## Introduction

Ce chapitre présente la mise en œuvre de notre solution d'automatisation des tests de sécurité, ainsi que son intégration dans l'architecture du SOC. Des tests simulés ont ensuite été réalisés afin d'évaluer l'efficacité des mécanismes de détection et de réponse aux incidents.

### 5.1 Mise en place de Caldera

Nous avons déployé Caldera à l'aide du dépôt GitHub officiel, ce qui nous a permis d'installer la plateforme de manière flexible et de disposer de l'ensemble des plugins et modules nécessaires pour simuler différents scénarios d'attaque dans notre environnement de test.

```
root@manager-vm:~# git clone https://github.com/mitre/caldera.git
Cloning into 'caldera'...
remote: Enumerating objects: 24841, done.
remote: Counting objects: 100% (246/246), done.
remote: Compressing objects: 100% (109/109), done.
remote: Total 24841 (delta 193), reused 137 (delta 137), pack-reused 24595 (from 3)
Receiving objects: 100% (24841/24841), 25.81 MiB | 13.54 MiB/s, done.
Resolving deltas: 100% (16760/16760), done.
root@manager-vm:~#
```

FIGURE 5.1 : Installation de Caldera

Ensuite, nous avons déployé Caldera afin d'accéder à son interface web, comme montre dans la figure suivante :

```
root@manager-vm:~/caldera# source venv/bin/activate
(venv) root@manager-vm:~/caldera# python3 server.py --build --insecure
2025-06-17 15:23:18 WARNING --insecure flag set. Caldera will use the default user accounts in
                           default.yml config file.
                           INFO Using main config from conf/default.yml
2025-06-17 15:23:19 INFO     Building VueJS front-end.
                                             server.py:219
                                             server.py:228
                                             server.py:255

up to date, audited 774 packages in 6s

100 packages are looking for funding
  run `npm fund` for details

25 vulnerabilities (1 low, 14 moderate, 9 high, 1 critical)

To address issues that do not require attention, run:
  npm audit fix

The logo consists of two stylized, blocky letters 'C' and 'A' formed by a grid of colored squares. The top row of squares is blue, the middle row is purple, and the bottom row is red. They are arranged side-by-side with some internal connections between them.

2025-06-17 15:24:45 INFO Docs built successfully.
```

FIGURE 5.2 : Déploiement de Caldera

Notre serveur Caldera est accessible via l'URL : <http://35.204.57.76:8888/>.

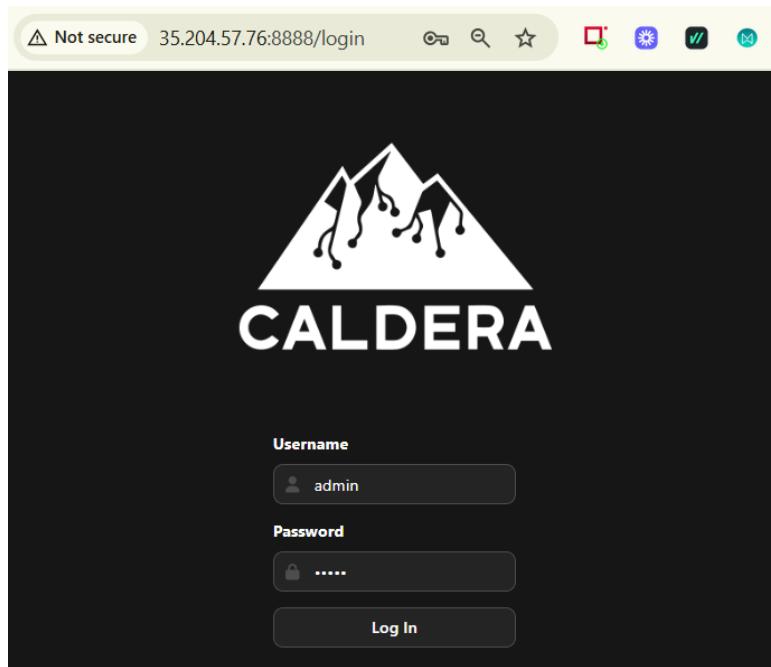


FIGURE 5.3 : Interface graphique de Caldera

Nous accédons à notre instance à l'aide d'un compte administrateur appartenant à l'équipe rouge. Voici le tableau de bord de Caldera :

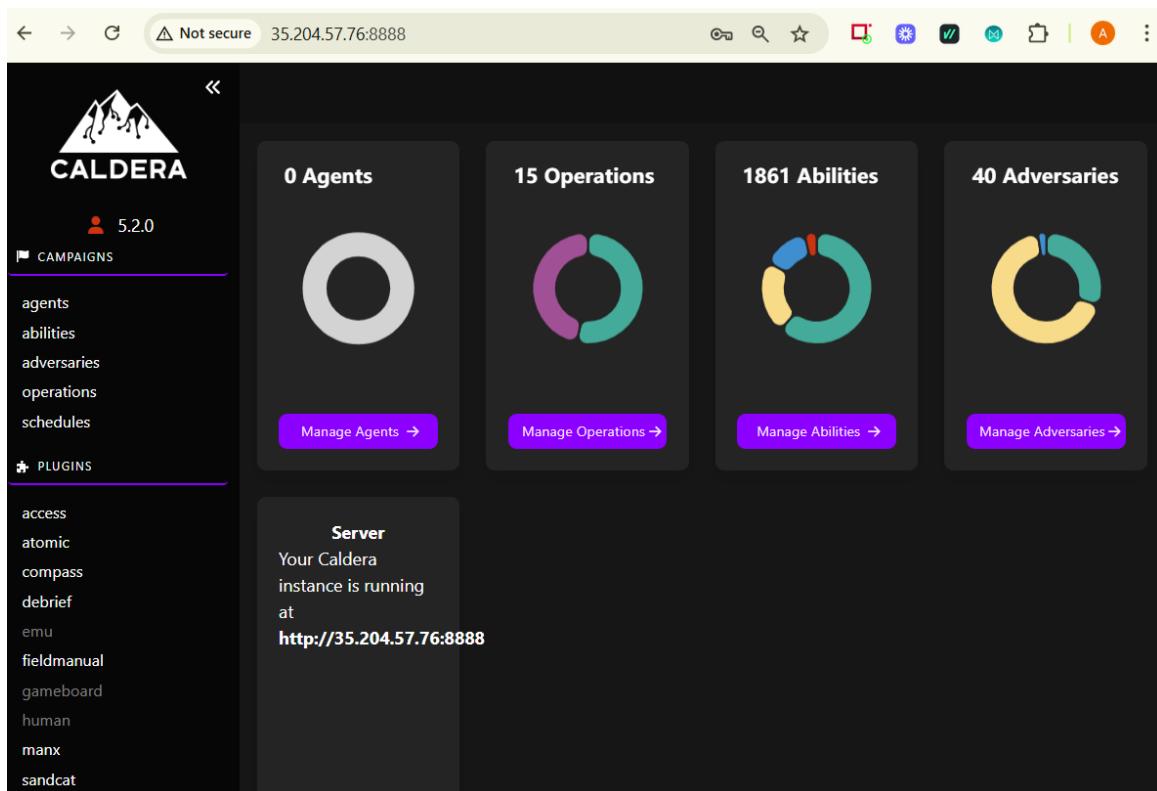


FIGURE 5.4 : Le tableau de board de Caldera

### 5.1.1 Déploiement des agents

Nous procédons à la configuration des agents Caldera dans notre infrastructure (Voir les détails de la création des agents Caldera dans l'Annexe B). Les agents que j'utilise pour effectuer les tests dans la figure 5.5.

Agents							
You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.							
<a href="#">+ Deploy an agent</a>		<a href="#">Configuration</a>		3 alive 3 trusted 3 agents 0 dead 0 untrusted		Bulk Actions ▾	
<b>id (paw)</b>	<b>host</b>	<b>group</b>	<b>platform</b>	<b>contact</b>	<b>pid</b>	<b>privilege</b>	<b>status</b>
mnnqfwr	ubn-cloud	Cloud-Endpoints	linux	HTTP	114154	User	alive, trusted
zufuyv	suricata	Local-Network	linux	HTTP	4183	Elevated	alive, trusted
revabl	Windows10	Local-Network-win	windows	HTTP	8712	Elevated	alive, trusted

FIGURE 5.5 : Les agents de Caldera

### 5.1.2 Les capacités (Abilities)

Caldera offre notamment la possibilité de simuler diverses méthodes d'attaque, y compris les TTPs, ce qui en fait un outil essentiel pour l'évaluation de la posture de sécurité. Voici un aperçu des 1 861 capacités prédéfinies dans Caldera, auxquelles s'ajoute la possibilité de créer des capacités personnalisées.

## Abilities

An ability is a specific ATT&CK tactic/technique implementation which can be executed on running agents. Abilities will include the command(s) to run, the platforms / executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the Caldera server.

The screenshot shows the Caldera Abilities interface. On the left, there is a sidebar with a search bar containing "cred", a "Tactic" dropdown set to "All", a "Technique" dropdown set to "All", and a "Platform" dropdown set to "All". Below these are "Clear Filters" and "53 / 1861 abilities" buttons. The main area displays four cards representing different abilities:

- Access Saved Credentials via VaultCmd**: credential-access T1555.004 - Credentials from Password Stores: Windows Credential Manager. Description: List credentials currently stored in Windows Credential Manager via the native Windows utility vaultcmd.exe. Credential Manager stores credentials for signing into websites, applications, and/or devices that request authentication through NTLM or Kerberos. References: <https://blog.malwarebytes.com/101/2016/01/the-windows-vaults/> and [https://medium.com/threatpunter/detecting-adversary-tradcrafc-with-image-load-event-logging-and-eql-8de9338c16](https://medium.com/threatpunter/detecting-adversary-tradcрафc-with-image-load-event-logging-and-eql-8de9338c16).
- AppleScript - Spoofing a credential prompt using osascript**: multiple T1056.002 - Input Capture: GUI Input Capture. Description: Prompt user for password without requiring permissions to send Apple events to System Settings. Reference: <https://embraceethered.com/blog/posts/2021/spoofing-credential-dialogs/>.
- Brute Force Credentials of single Active Directory domain user via LDAP against domain controller (NTLM or Kerberos)**: credential-access T1110.001 - Brute Force: Password Guessing. Description: Attempt to brute force Active Directory domain user on a domain controller, via LDAP, with NTLM or Kerberos.
- Brute Force Credentials of single Azure AD user**: credential-access T1110.001 - Brute Force: Password Guessing. Description: Attempt to brute force Azure AD user via AzureAD powershell module.

FIGURE 5.6 : Les capacités de Caldera

### 5.1.3 Le profil d'adversaire (Adversaries)

Caldera propose 36 adversaires prédéfinis, dont les profils représentent différentes approches d'attaque et permettent l'exécution des capacités correspondantes. Il est également possible de créer un profil d'adversaire personnalisé. Voici un exemple de profil d'adversaire, nommé Discovery, qui présente plusieurs capacités (abilités) et s'exécute sur différents agents.

The screenshot shows the Caldera Adversary profile interface for a "Discovery" profile. At the top, there are buttons for "+ Add Ability", "+ Add Adversary", "Fact Breakdown", "Objective: default", "Export", "Save", and "Delete". The main area is a table with the following columns:

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Identify active user	discovery	System Owner/User Discovery	mac, windows		key		x
2	Find local users	discovery	Account Discovery: Local Account	mac, windows		key		x
3	Identify local users	discovery	Account Discovery: Local Account	mac, windows				x
4	Snag broadcast IP	discovery	System Network Configuration Discovery	mac				x
5	Find user processes	discovery	Process Discovery	mac, windows	lock			x
6	View admin shares	discovery	Network Share Discovery	windows		key		x
7	Discover domain controller	discovery	Remote System Discovery	windows				x
8	Discover antivirus programs	discovery	Software Discovery: Security Software Discovery	mac, windows		key		x
9	Permission Groups Discovery	discovery	Permission Groups Discovery: Local Groups	mac, windows				x
10	Identify Firewalls	discovery	Software Discovery: Security Software Discovery	windows				x
11	Discover Mail Server	discovery	Remote System Discovery	mac, windows		key		x
12	Get Chrome Bookmarks	discovery	Browser Bookmark Discovery	mac		key		x

FIGURE 5.7 : Exemple de profil d'adversaire Caldera

### 5.1.4 Les opérations (operations)

Les opérations dans Caldera permettent de simuler des attaques en exécutant les profils d'adversaires sur les agents déployés. Chaque opération suit une séquence définie des capacités (Abilitie) selon les TTPs associées à l'adversaire sélectionné. Cet exemple dans la figure 5.8 montre une opération qui utilise le profil d'adversaire Discovery.

The screenshot shows the Caldera Operations interface. At the top, there's a header bar with the title 'Operations', a dropdown menu showing 'Discovery-operation (2025-06-18T09:42:28.927Z) - 15 decisions | 3 min ago', a 'New Operation' button, and 'Download Report' and 'Delete Operation' buttons. Below the header is a sub-header for 'Discovery-operation (2025-06-18T09:42:28.927Z)' with a 'Download Graph SVG' button. The main area contains a table of operation details and a timeline visualization.

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
6/18/2025, 10:42:26 AM GMT+1	success	Identify active user	discovery	mnnfwr	ubn-cloud	125008	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:42:26 AM GMT+1	success	Identify active user	discovery	zufuyv	suricata	13719	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:42:26 AM GMT+1	success	Identify active user	discovery	qstugt	Windows10	2144	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:43:07 AM GMT+1	success	Find local users	discovery	mnnfwr	ubn-cloud	125211	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:43:07 AM GMT+1	success	Find local users	discovery	zufuyv	suricata	13722	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:43:07 AM GMT+1	success	Identify local users	discovery	qstugt	Windows10	6044	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:43:42 AM GMT+1	success	Find user processes	discovery	mnnfwr	ubn-cloud	125390	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:43:42 AM GMT+1	success	Find user processes	discovery	zufuyv	suricata	13726	<button>View Command</button>	<button>View Output</button>
6/18/2025, 10:43:42 AM GMT+1	success	Find user processes	discovery	qstugt	Windows10	2572	<button>View Command</button>	<button>View Output</button>

At the bottom right of the table, there is a button labeled 'Activate Windows'.

FIGURE 5.8 : Opération simulée

## 5.2 Simulations des scénarios de tests dans le SOC

### 5.2.1 Tests des agents Windows

#### 5.2.1.1 Crédation des capacités

Nous avons créé une capacité nommée Mimikatz en identifiant les TTPs qui lui correspondent.

Voici la figure ci-dessous.

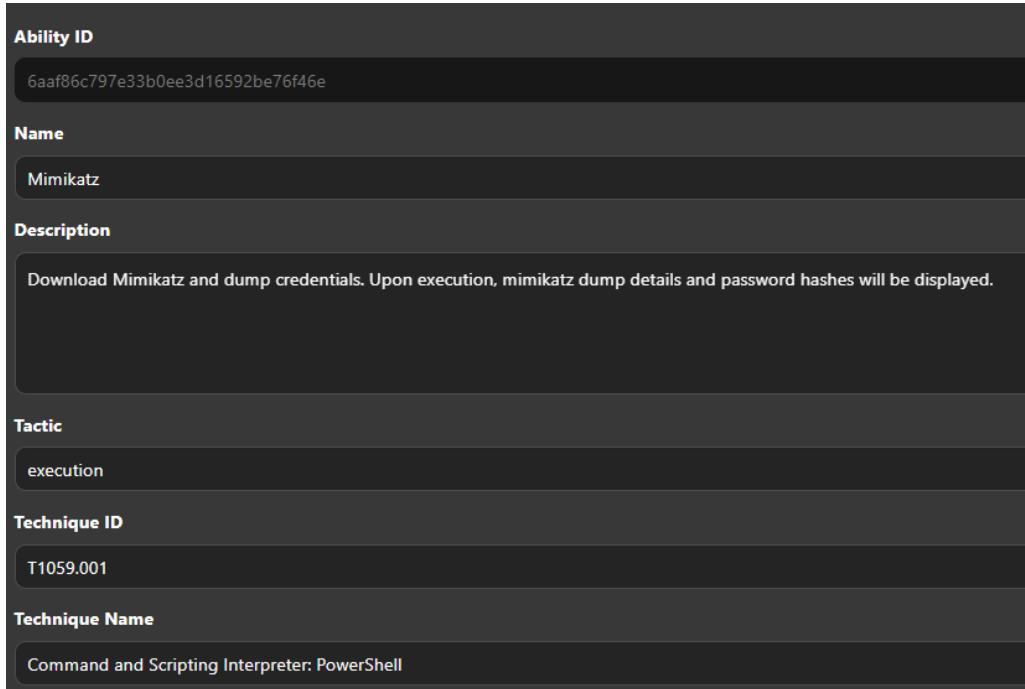


FIGURE 5.9 : Création d'une capacité - Mimikatz

La figure 5.10 présente l'exécuteur ainsi que les commandes utilisées dans cette capacité.



FIGURE 5.10 : Commandes utilisées - Mimikatz

### 5.2.1.2 Cration de profil d'adversaire

Nous procons maintenant  la cration d'un profil d'adversaire nomm Mimikatz, contenant deux capacits bases sur celles que nous avons crees.

The screenshot shows the 'Mimikatz Adversary' profile creation interface. At the top, there are buttons for '+ Add Ability', '+ Add Adversary', and 'Fact Breakdown'. To the right are buttons for 'Objective: default', 'Save' (highlighted in green), 'Export', and 'Delete'. Below this is a table with the following data:

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Mimikatz	execution	Command and Scripting Interpreter: PowerShell	Windows				x
2	PowerShell Invoke-Mimikatz	execution	Command and Scripting Interpreter: PowerShell	Windows				x

FIGURE 5.11 : Cration d'un adversaire - Mimikatz

### 5.2.1.3 Simulation d'operation

Une fois l'adversaire cr, nous le simulons en excutant l'operation. Voici la cration d'une operation qui slectionne l'agent Windows du groupe "Local-Network-win".

**Start New Operation**

<b>Operation Name</b>	Operation-Mimikatz
<b>Adversary</b>	Mimikatz Adversary
<b>Fact Source</b>	basic
<b>Group</b>	All groups Local-Network Local-Network-win Cloud-Endpoints
<b>Planner</b>	atomic
<b>Obfuscators</b>	base64 base64jumble base64noPadding caesar cipher plain-text steganography
<b>Autonomous</b>	<input checked="" type="radio"/> Run autonomously <input type="radio"/> Require manual approval
<b>Parser</b>	<input checked="" type="radio"/> Use Default Parser <input type="radio"/> Don't use default learning parsers
<b>Auto Close</b>	<input checked="" type="radio"/> Keep open forever <input type="radio"/> Auto close operation
<b>Run State</b>	<input checked="" type="radio"/> Run immediately <input type="radio"/> Pause on start
<b>Jitter (sec/sec)</b>	2 / 8
<input type="button" value="Cancel"/> <input type="button" value="Start"/>	

**FIGURE 5.12 :** Créeation d'une opération

L'exécution de l'opération est terminée, dans la figure suivante :

Operation-Mimikatz		Download Graph SVG		
				+ <span style="float: right;">Autonomous</span>
<input type="button" value="+ Manual Command"/> <input type="button" value="+ Potential Link"/> <input type="button" value="Operation Details"/> <input type="button" value="▼ Filters"/>		<span style="border: 1px solid black; padding: 2px;">running</span> <span style="border: 1px solid black; padding: 2px;">■</span> <span style="border: 1px solid black; padding: 2px;">  </span> <span style="border: 1px solid black; padding: 2px;">▶</span> <sub>1</sub>		Obfuscator: plain-text <span style="float: right;">▼</span>
Time Ran	Status	Ability Name	Tactic	Agent
6/18/2025, 12:59:43 PM GMT+1	<input checked="" type="radio"/> success	Mimikatz	execution	revabl
6/18/2025, 1:00:18 PM GMT+1	<input checked="" type="radio"/> success	PowerShell Invoke MimiKatz	execution	revabl
				Host pid Link Command Link Output
				Windows10 9868 <input type="button" value="View Command"/> <input type="button" value="View Output"/> C
				Windows10 11688 <input type="button" value="View Command"/> <input type="button" value="View Output"/> C

**FIGURE 5.13 :** Opération accomplie - Mimikatz

### 5.2.1.4 Alerte de Wazuh

Voici comment Wazuh détecte l'exécution de Mimikatz après la configuration par des règles spécifiques.

	Jun 18, 2025 @ 13:00:35.3...	Windows10	Invoke-Mimikatz Detected via PowerShell	12	100004
	Jun 18, 2025 @ 13:00:00.1...	Windows10	Download Mimikatz and dump credentials. Upon execution, mimikatz dump details and password hashes will be displayed	15	100003
	Jun 18, 2025 @ 12:56:48.3...	Windows10	Suspicious Windows cmd shell execution	3	92032

**FIGURE 5.14 :** Alerte de Wazuh - Mimikatz

### 5.2.2 Tests des agents Cloud

Un serveur de base de données MySQL est déployé sur notre machine cloud. Ainsi, nous avons créé un adversaire qui simule des attaques par commandes SQL à l'aide de capacités spécifiques. Cet adversaire est présenté dans la figure suivante.

Ordering	Name	Tactic	Technique	Executors
1	Create Database	impact	Database Manipulation	
2	Create DB User	impact	Database Manipulation	
3	Delete DB User	impact	Database Manipulation	
4	Delete Database	impact	Database Manipulation	

**FIGURE 5.15 :** Création d'un adversaire - MySQL \_ Manipulation

Maintenant, nous passons à l'exécution de l'opération.

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
6/18/2025, 2:05:00 PM GMT+1	success	Create Database	impact	mnqfwr	ubn-cloud	167515	<button>View Command</button>	No output
6/18/2025, 2:05:41 PM GMT+1	success	Create DB User	impact	mnqfwr	ubn-cloud	167714	<button>View Command</button>	No output
6/18/2025, 2:06:36 PM GMT+1	success	Delete DB User	impact	mnqfwr	ubn-cloud	167815	<button>View Command</button>	No output
6/18/2025, 2:07:11 PM GMT+1	success	Delete Database	impact	mnqfwr	ubn-cloud	167984	<button>View Command</button>	No output

**FIGURE 5.16 :** Opération accomplie - MySQL \_ Manipulation

Une fois cette étape terminée, la détection est effectuée via Wazuh (Voir les détails dans l'Annexe

A)

	Jun 18, 2025 @ 14:05:40.9...	ubn-cloud	'CREATE DATABASE secret_data CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci' is critical at MYSQL Command Detected	11	100151
	Jun 18, 2025 @ 14:06:37.0...	ubn-cloud	'CREATE USER 'spy_user'@localhost' IDENTIFIED BY <secret> is critical at MYSQL Command Detected	11	100151
	Jun 18, 2025 @ 14:06:37.0...	ubn-cloud	'ALTER USER 'spy_user'@localhost' IDENTIFIED WITH 'mysql_native_password' BY <secret> is critical at MYSQL Command Detected	3	100153
	Jun 18, 2025 @ 14:07:55.0...	ubn-cloud	'DROP DATABASE IF EXISTS secret_data' is critical at MYSQL Command Detected	12	100152

**FIGURE 5.17 :** Alerte de wazuh - MySQL\_Manipulation

### 5.3 Simulation de tests automatiques sur le workflow

Nous avons une application web hébergée sur notre serveur dans le réseau local, par ailleurs, un adversaire a été créé pour simuler des attaques sur l'application.

#### web-application-test

Simulation of attacks on a web application to identify vulnerabilities and test its security

			Objective: default			
<b>Ordering</b>	<b>Name</b>		<b>Tactic</b>	<b>Technique</b>		<b>Execu</b>
☰ 1	SQL Injection via curl		execution	Server Software Component		⚠
☰ 2	XSS attempt - Script tag injection		execution	Command and Scripting Interpreter		⚠

**FIGURE 5.18 :** Crédation d'un adversaire - web-application-test

Ensuite, nous avons simulé l'opération sur la machine locale afin de tester la capacité de détection de Suricata, qui identifie les requêtes d'injection SQL ainsi que les attaques XSS sur le réseau.

web-application-operation (2025-06-18T13:53:59.690Z)								+	
					Obfuscator: plain-text	Autonomous			
6/18/2025, 2:53:57 PM GMT+1		SQL Injection via curl	execution	zufuyv	suricata	14438			C
6/18/2025, 2:54:18 PM GMT+1		XSS attempt - Script tag injection	execution	zufuyv	suricata	14441			C

**FIGURE 5.19 :** Opération accomplie - web-application-test

Nous avons reçu deux alertes dans Slack suite à cette opération.

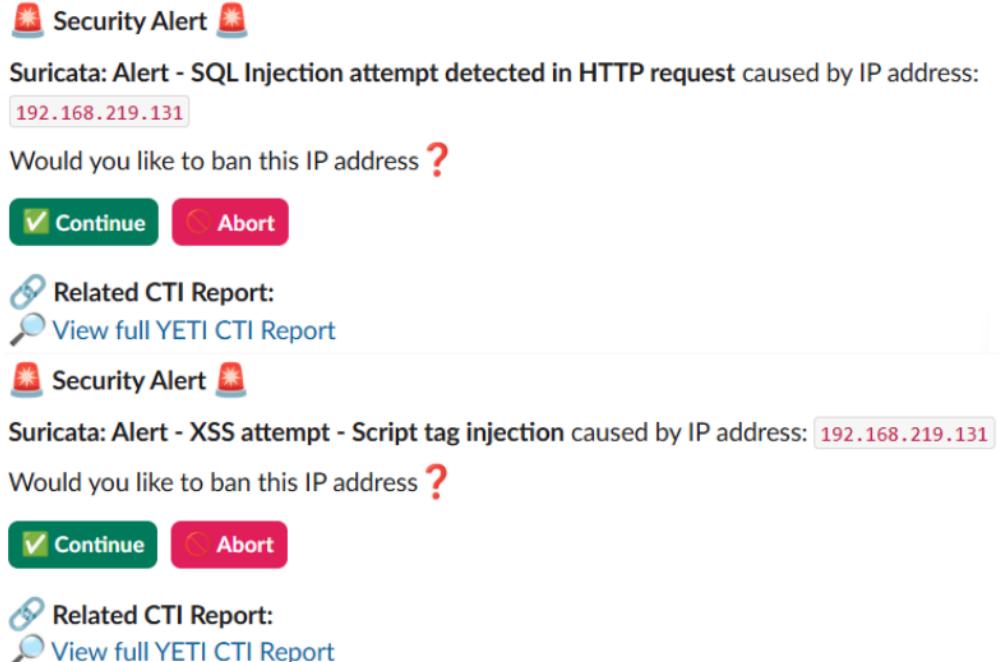


FIGURE 5.20 : Alerte Slack

Ensuite, nous cliquons sur le lien fourni dans l'alerte afin d'afficher le rapport généré par YETI, comme illustre dans la figure suivante :



FIGURE 5.21 : Résultat de YETI

Un clic sur le lien redirige vers les informations détaillées de l'alerte dans TheHive. Celle-ci contient une description générée par le LLM.

General Observables (1) TTPs (0) Attachments Similar Cases Similar Alerts Responders History

Suricata: Alert - SQL Injection attempt detected in HTTP request

**Tags**

**Description**

**Alert Summary**

A SQL injection attempt was detected in an HTTP request from source IP 192.168.219.131 to destination IP 192.168.219.138 on port 80. The Suricata rule with signature ID 1000020 and category Web Application Attack triggered this alert, indicating a potential attack on the web application. The alert shows a GET request with a suspicious URL containing SQL injection characters. The Suricata rule is designed to detect SQL injection attempts in HTTP requests, which can lead to unauthorized access to sensitive data or system compromise.

**Security Implications**

The severity of this alert is critical as it indicates a potential SQL injection attack, which can have severe consequences such as unauthorized data access, modification, or deletion. The attacker's motivation may be to exploit vulnerabilities in the web application to gain access to sensitive data or disrupt system operations. The potential impact on systems, data, or operations can be significant, and this could be part of a larger attack pattern. The rule logic and detection method are based on the signature ID 1000020, which is designed to detect SQL injection attempts in HTTP requests. The alert is related to the MITRE ATT&CK technique T1190, which involves exploiting software vulnerabilities.

**Recommended Actions**

Based on the severity assessment, this is a critical alert, and immediate action is required.

BLOCK THIS IP ADDRESS IMMEDIATELY - High priority security threat.

The specific firewall/blocking command to run is iptables -A INPUT -s 192.168.219.131 -j DROP.

To verify, run the command iptables -nvL.

Check the file /var/log/suricata/eve.json for additional information.

Immediate containment or remediation steps include isolating the affected system, analyzing logs, and updating the web application to patch vulnerabilities.

Urgent escalation to the security team is recommended to ensure prompt response and mitigation.

Additional steps include monitoring system logs, analyzing network traffic, and performing a thorough incident response to identify and contain the threat.

**FIGURE 5.22 : Alerte TheHive - SQL Injection**

Ainsi, le rapport présente l'observable IP analysé par Cortex.

Summary			
Malicious	0/94	Last analysis date	2024-09-14 06:53:57
Suspicious	0/94		
Undefined	94/94		
SHA-256 192.168.219.131			
VirusTotal Report <a href="https://www.virustotal.com/gui/search/192.168.219.131">https://www.virustotal.com/gui/search/192.168.219.131</a>			

**FIGURE 5.23 : Rapport d'analyse de l'adresse IP**

Enfin, nous prenons la décision de bloquer ou d'aborder l'adresse selon la norme de sévérité,

par un simple clic sur le bouton dans l'alerte Slack.

## Conclusion

Dans ce chapitre, nous avons présenté la mise en œuvre de tests automatiques d'attaques, permettant de simuler divers comportements adversaires au sein de notre infrastructure. Ces simulations ont offert une évaluation dynamique et réaliste des capacités de détection et de réaction de notre SOC. Grâce à l'intégration d'agents variés et à la création de profils d'adversaires personnalisés, nous avons pu tester efficacement la robustesse des outils de sécurité. Ces expérimentations démontrent l'importance d'un SOC proactif et adaptable, capable de faire face à des menaces évolutives grâce à des tests continus et automatisés.

# Conclusion générale

Ce projet de fin d'études réalisé au sein du SOC de KEYSTONE-Group m'a permis de développer des compétences techniques avancées en cybersécurité, notamment dans la conception, la mise en place et l'automatisation d'un centre opérationnel de sécurité. En combinant SIEM et SOAR, nous avons mis en place une solution automatisée permettant la détection, l'analyse et la réponse rapide aux incidents, renforçant ainsi la capacité du SOC à protéger efficacement les systèmes d'information face à des menaces de plus en plus complexes.

L'intégration d'un modèle de langage large (LLM) au sein de la plateforme SOAR du SOC a enrichi le traitement des alertes grâce à des analyses contextuelles intelligentes, améliorant la qualité des investigations et la pertinence des réponses. Par ailleurs, la mise en œuvre de simulations d'attaques automatisées a permis de tester et d'optimiser la résilience du SOC face aux cybermenaces réelles.

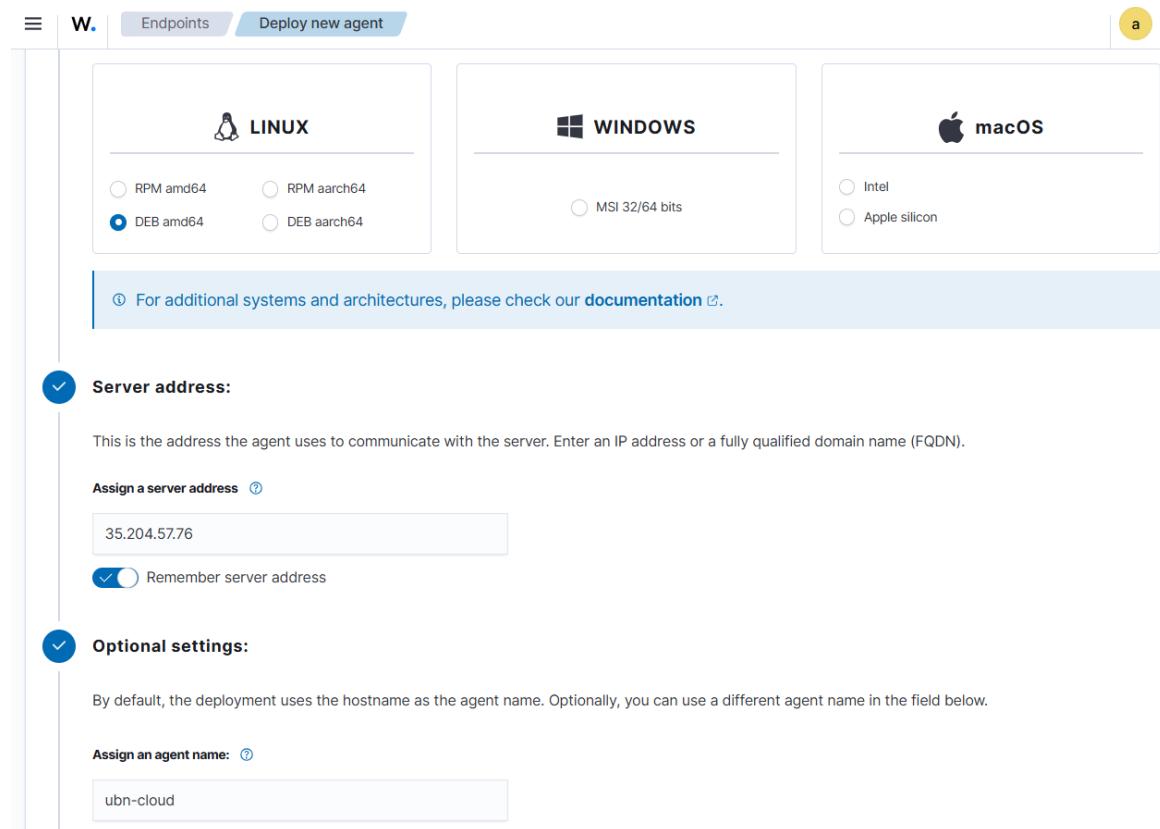
Ce stage a constitué une expérience professionnelle clé, me permettant d'appréhender les enjeux opérationnels d'un SOC moderne, tout en développant mes compétences en automatisation, intelligence artificielle et gestion des incidents. Il m'a également sensibilisé à l'importance d'une veille continue et d'une innovation constante pour maintenir l'efficacité des dispositifs de sécurité.

Enfin, les perspectives d'évolution que j'ai identifiées montrent ma capacité à anticiper les besoins futurs du SOC, notamment par le renforcement des mécanismes d'intelligence artificielle et d'apprentissage automatique, ce qui constitue un atout majeur pour ma carrière dans le domaine de la cybersécurité.

# Annexes

## Annexe A : Agent des agents Wazuh

Nous avons ajouté un agent Ubuntu nommé "ubn-cloud", en spécifiant son système d'exploitation, son architecture, l'adresse IP du serveur Wazuh ainsi que son groupe d'appartenance, comme illustré dans la figure ci-dessous :



**FIGURE 6.1 :** Ajout d'un agent Ubuntu sur Wazuh

Pour permettre la liaison entre l'agent et le serveur, nous avons générée des commandes destinées à être exécutées sur la machine cible.

Select one or more existing groups: [?](#)

cloud-endpoints [X](#)

[X](#) [▼](#)

**4 Run the following commands to download and install the agent:**

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER='35.204.57.76' WAZUH_REGISTRATION_PASSWORD='*****' WAZUH_AGENT_GROUP='cloud-endpoints' WAZUH_AGENT_NAME='ubn-cloud' dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb
```

[X](#) Show password

[?](#) Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

**5 Start the agent:**

```
sudo systemctl daemon-reload  
sudo systemctl enable wazuh-agent  
sudo systemctl start wazuh-agent
```

**FIGURE 6.2 :** Commandes d'installation de l'agent Wazuh

## Annexe B : Configuration des décodeurs et des règles de détection

- **Configuration de Sysmon pour Linux**

Nous avons créé des décodeurs Sysmon pour Linux afin que le serveur Wazuh puisse interpréter les logs provenant des machines Linux.

```

<decoder name="sysmon-linux">
  <program_name>sysmon</program_name>
</decoder>

<!-- system -->
<!-- EventID -->
<decoder name="sysmon-linux-child">
  <parent>sysmon-linux</parent>
  <regex offset="after_parent">\pEventID\p(\d+) \p/EventID\p</regex>
  <order>system.eventId</order>
</decoder>

<!-- keywords -->
<decoder name="sysmon-linux-child">
  <parent>sysmon-linux</parent>
  <regex offset="after_parent">\pKeywords\p(.+) \p/Keywords\p</regex>
  <order>system.keywords</order>
</decoder>

<!-- level -->
<decoder name="sysmon-linux-child">
  <parent>sysmon-linux</parent>
  <regex offset="after_parent">\pLevel\p(\d+) \p/Level\p</regex>
  <order>system.level</order>
</decoder>

<!-- channel -->
<decoder name="sysmon-linux-child">
  <parent>sysmon-linux</parent>
  <regex offset="after_parent">\pChannel\p(.+) \p/Channel\p</regex>
  <order>system.channel</order>
</decoder>

<!-- opcode -->
<decoder name="sysmon-linux-child">
  <parent>sysmon-linux</parent>
  <regex offset="after_parent">\pOpcode\p(\d+) \p/Opcode\p</regex>
  <order>system.opcode</order>
</decoder>

```

FIGURE 6.3 : Configuration des décodeurs Sysmon pour Wazuh

Nous avons également configuré des règles spécifiques à Sysmon dans le serveur Wazuh.

```

<group name="linux,sysmon">
    <rule id="200150" level="3">
        <decoded_as>sysmon-linux</decoded_as>
        <field name="system.eventId">\.+</field>
        <group>sysmon_event1</group>
        <description>Sysmon For Linux Event</description>
        <mitre>
            <id>T1204</id>
        </mitre>
        <options>no_full_log</options>
    </rule>
    <rule id="200151" level="3">
        <if_sid>200150</if_sid>
        <field name="system.eventId">^1$</field>
        <description>Sysmon - Event 1: Process creation $(eventdata.image)</description>
        <group>sysmon_event1</group>
        <mitre>
            <id>T1204</id>
        </mitre>
        <options>no_full_log</options>
    </rule>
    <rule id="200152" level="3">
        <if_sid>200150</if_sid>
        <field name="system.eventId">^3$</field>
        <description>Sysmon - Event 3: Network connection by $(eventdata.image)</description>
        <group>sysmon_event3</group>
        <mitre>
            <id>T1043</id>
        </mitre>
        <options>no_full_log</options>
    </rule>
    <rule id="200153" level="3">
        <if_sid>200150</if_sid>
        <field name="system.eventId">^5$</field>
        <description>Sysmon - Event 5: Process terminated $(eventdata.image)</description>
        <group>sysmon_event5</group>
        <mitre>
            <id>T1204</id>
        </mitre>
        <options>no_full_log</options>
    </rule>

```

FIGURE 6.4 : La configuration de règles dédiées à Sysmon

- Configuration de Falco

Nous avons d'abord créé un fichier de configuration personnalisé sur l'agent Wazuh afin de définir des paramètres qui remplacent ceux de la configuration par défaut.

```

#Enable logs in json format
json_output: true

#Adds extra information to the logs. This will serve as a base to trigger alerts on Wazuh
append_output:
  - extra_fields:
      - wazuh_integration: "falco"

#Save the logs to /var/log/falco_events.json file
file_output:
  enabled: true
  keep_alive: false
  filename: /var/log/falco_events.json

```

FIGURE 6.5 : Fichier de configuration de Falco

Nous avons intégré des règles Falco personnalisées dans la configuration du serveur Wazuh.

```

<group name="falco">
  <rule id="100600" level="0">
    <decoded_as>json</decoded_as>
    <field name="output_fields.wazuh_integration">falco</field>
    <description>Falco: run-time security logs.</description>
    <options>no_full_log</options>
  </rule>
  <rule id="100601" level="4">
    <if_sid>100600</if_sid>
    <field name="priority">Info</field>
    <description>"Falco Alert - " $(output)</description>
    <options>no_full_log</options>
  </rule>
  <rule id="100602" level="6">
    <if_sid>100600</if_sid>
    <field name="priority">Notice</field>
    <description>"Falco Alert - " $(output)</description>
    <options>no_full_log</options>
  </rule>
  <rule id="100603" level="8">
    <if_sid>100600</if_sid>
    <field name="priority">Warning</field>
    <description>"Falco Alert - " $(output)</description>
    <options>no_full_log</options>
  </rule>
  <rule id="100604" level="10">
    <if_sid>100600</if_sid>
    <field name="priority">Error</field>
    <description>"Falco Alert - " $(output)</description>
    <options>no_full_log</options>
  </rule>

  <rule id="100605" level="12">
    <if_sid>100600</if_sid>
    <field name="priority">Critical</field>
    <description>"Falco Alert - " $(output)</description>
    <options>no_full_log</options>
  </rule>

```

FIGURE 6.6 : La configuration de règles dédiées à Falco

- Configuration des MYSQL

Nous avons modifié le fichier "ossec.conf" de l'agent Wazuh pour envoyer les logs MySQL au serveur Wazuh.

```

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/mysql/query.log</location>
</localfile>

```

FIGURE 6.7 : Collecte des logs MySQL

Nous avons créé des décodeurs pour les requêtes SQL exécutées afin que le serveur Wazuh puisse interpréter ces logs.

```
<decoder name="local_decoder_example">
    <program_name>local_decoder_example</program_name>
</decoder>
<decoder name="custom_mysql">
    <prematch>^Query\t\w</prematch>
    <regex>^\w+\t(.*)$</regex>
    <order>_action, command</order>
</decoder>
```

FIGURE 6.8 : Configuration des décodeurs MySQL

Nous avons intégré des règles personnalisées pour MySQL dans la configuration du serveur Wazuh.

```

<group name="mysql">
  <rule id="100151" level="11">
    <decoded_as>custom_mysql</decoded_as>
    <field name="command">CREATE</field>
    <description>'$(command)' is critical at MYSQL Command Detected</description>
  </rule>

  <rule id="100152" level="12">
    <decoded_as>custom_mysql</decoded_as>
    <field name="command">DROP</field>
    <description>'$(command)' is critical at MYSQL Command Detected</description>
  <mitre>
    <id>T1485</id>
  </mitre>
  </rule>

  <rule id="100153" level="3">
    <decoded_as>custom_mysql</decoded_as>
    <field name="command">ALTER</field>
    <description>'$(command)' is critical at MYSQL Command Detected</description>
  <mitre>
    <id>T1132</id>
  </mitre>
  </rule>

  <rule id="100154" level="12">
    <decoded_as>custom_mysql</decoded_as>
    <field name="command">UPDATE</field>
    <description>'$(command)' is critical at MYSQL Command Detected</description>
  </rule>

  <rule id="100156" level="12">
    <decoded_as>custom_mysql</decoded_as>
    <field name="command">DELETE</field>
    <description>'$(command)' is critical at MYSQL Command Detected</description>
  <mitre>
    <id>T1485</id>
  </mitre>
  </rule>

```

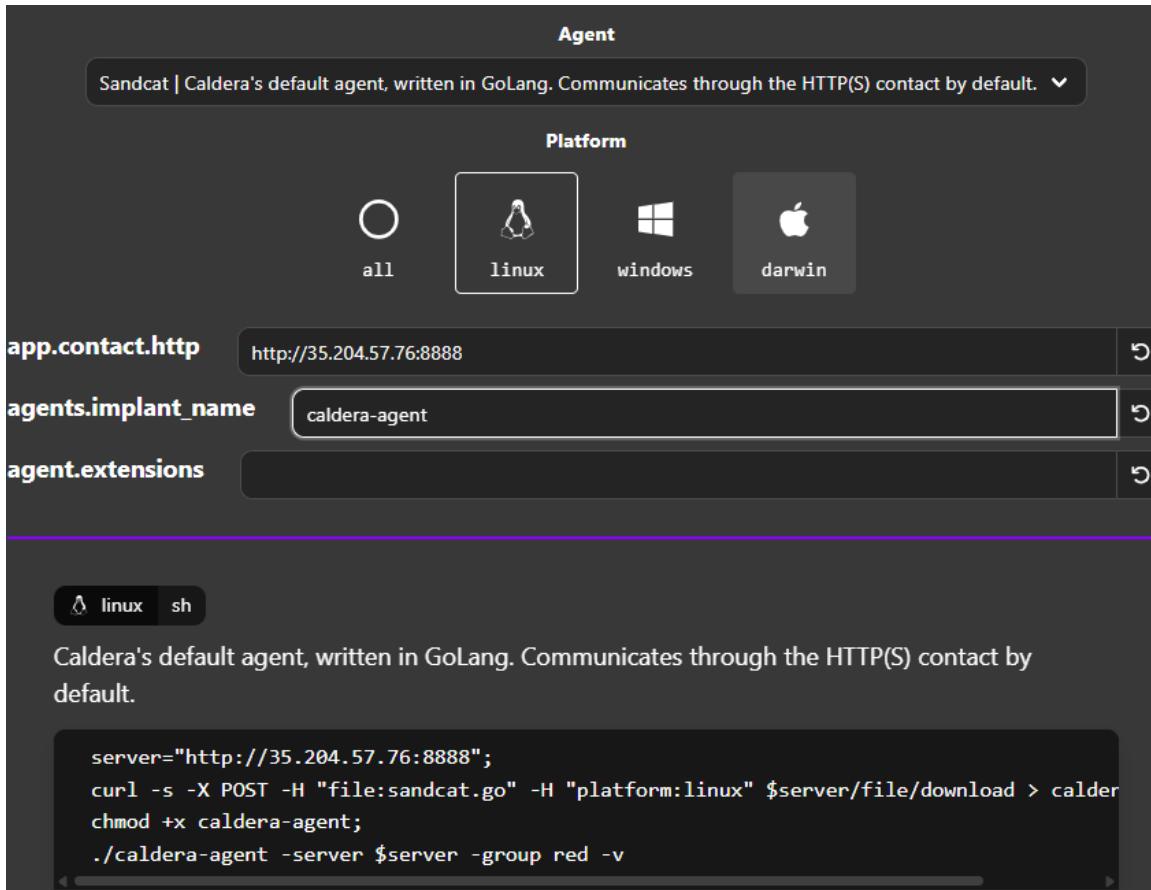
FIGURE 6.9 : Configuration des règles MYSQL

## Annexe B : Configuration des agents Caldera

Nous avons commencé par déployer un agent Caldera en utilisant Sandcat, l'agent le plus utilisé et fourni par la plateforme.



**FIGURE 6.10 :** Crédit de l'agent Sandcat



**FIGURE 6.11 :** Déploiement de l'agent Caldera sur Ubuntu

# Bibliographie

- [1] <https://www.keystone-corporation.com> (Accédé le 03/02/2025)
- [2] <https://www.appvizer.fr/magazine/operations/gestion-de-projet/methode-agile> (Accédé le 15/02/2025)
- [3] <https://www.nutcache.com/fr/blog/comment-planifier-projet-avec-diagramme-de-gantt> (Accédé le 20/02/2025)
- [4] <https://www.logpoint.com/fr/blog/security-operations-center-soc> (Accédé le 23/02/2025)
- [5] [https://www.splunk.com/fr\\_fr/blog/learn/siem-security-information-event-management.html](https://www.splunk.com/fr_fr/blog/learn/siem-security-information-event-management.html) (Accédé le 01/03/2025)
- [6] <https://blog.alphorm.com/choisir-meilleur-outil-siem-securite-informatique> (Accédé le 05/03/2025)
- [7] <https://wazuh.com> (Accédé le 07/03/2025)
- [8] <https://www.objetconnecte.com/hids-definition> (Accédé le 17/03/2025)
- [9] <https://tehtris.com/fr/glossaire/nids-network-intrusion-detection-system> (Accédé le 20/03/2025)
- [10] <https://suricata.io> (Accédé le 20/03/2025)
- [11] <https://falco.org> (Accédé le 22/03/2025)
- [12] <https://www.elastic.co/fr/what-is/soar> (Accédé le 01/04/2025)
- [13] <https://geekflare.com/fr/best-soar-tools> (Accédé le 02/04/2025)
- [14] <https://strangebee.com> (Accédé le 04/04/2025)
- [15] <https://tehtris.com/fr/glossaire/cti-cyber-threat-intelligence> (Accédé le 07/04/2025)
- [16] <https://yeti-platform.io> (Accédé le 08/04/2025)
- [17] <https://shuffler.io> (Accédé le 10/04/2025)
- [18] <https://www.picussecurity.com/resource/glossary/what-is-adversary-emulation> (Accédé le 15/04/2025)
- [19] <https://caldera.readthedocs.io/en/latest> (Accédé le 20/04/2025)
- [20] <https://aws.amazon.com/fr/what-is/virtualization> (Accédé le 01/05/2025)
- [21] <https://docs.docker.com> (Accédé le 02/05/2025)
- [22] <https://cloud.google.com/?hl=fr> (Accédé le 05/05/2025)
- [23] <https://www.oracle.com/fr/cloud/soc-security-operations-center> (Accédé le 06/05/2025)
- [24] <https://www.netapp.com/fr/artificial-intelligence/what-is-artificial-intelligence> (Accédé le 17/05/2025)
- [25] <https://www.cloudflare.com/fr-fr/learning/ai/what-is-large-language-model> (Accédé le 18/05/2025)

## Résumé

Ce rapport présente le travail réalisé dans le cadre du projet de fin d'études chez KEYSTONE-Group. Il traite de la mise en place d'un SOC intégrant une solution combinant SIEM et SOAR, l'utilisation d'un modèle LLM pour enrichir l'analyse des alertes, ainsi que l'automatisation de simulations d'attaques afin de tester la robustesse du dispositif. L'objectif principal était de renforcer la sécurité de l'entreprise grâce à une surveillance continue, une détection précise des menaces et une réponse rapide aux incidents.

**Mots clés :** SOC, SIEM, SOAR, LLM

## Abstract

This report presents the work carried out as part of the final year project at KEYSTONE-Group. It focuses on the implementation of a SOC integrating a solution combining SIEM and SOAR, the use of an LLM model to enhance alert analysis, as well as the automation of attack simulations to test the robustness of the system. The main objective was to strengthen the company's security through continuous monitoring, precise threat detection, and rapid incident response.

**Keywords :** SOC, SIEM, SOAR, LLM