



المدرسة التطبيقية للعلوم
التطبيقية - مراكش
ECOLE NATIONALE DES SCIENCES
APPLIQUÉES - MARRAKECH



Rapport du Projet de Fin de Semestre

Mise en place d'un Centre des Opérations de Sécurité de nouvelle génération

Réalisé par :

- Essaleh Yassine
- Stoti Mehdi

Encadré par :

- M. ABOU EL KALAM Anas

Filière : Génie Cyber Défense et Systèmes de
Télécommunications Embarqués

Année Universitaire : 2023 - 2024

Remerciements

Ce projet n'est pas simplement le résultat de nos propres efforts, mais également le fruit des contributions généreuses de nombreuses personnes à qui nous exprimons notre profonde gratitude. Tout d'abord, nous tenons à remercier le Directeur Général de l'ENSA pour sa patience et son soutien tout au long de notre parcours académique. Nos sincères remerciements vont à M. Anas ABOU EL KALAM, responsable de la filière GCDSTE à l'ENSA Marrakech, pour sa constante disponibilité, ses recommandations judicieuses et les informations pertinentes qu'il a partagées. Nous souhaitons également exprimer notre gratitude envers l'ensemble du corps professoral et administratif de l'ENSA Marrakech pour les efforts constants déployés en vue d'assurer et d'améliorer la qualité de notre formation.

Résumé

Ce projet vise à mettre en place un centre opérationnel de sécurité (SOC) afin de permettre aux équipes Blue Team de surveiller et de répondre en continu aux cybermenaces avancées. L'intégration de Wazuh, ELK et TheHive a permis de créer une plateforme de défense complète offrant des fonctionnalités avancées, une collaboration efficace et une visualisation claire des données. Cette implémentation améliore la posture de sécurité de l'entreprise pour faire face aux menaces actuelles et futures. Le projet a rencontré plusieurs défis, notamment des limitations matérielles, des contraintes de temps et un manque de ressources documentaires, en particulier concernant MISP. Malgré ces obstacles, les autres aspects du projet ont été réalisés avec succès, démontrant notre capacité à nous adapter et à maximiser l'utilisation des ressources disponibles..

Abstract

This project aims to establish a Security Operations Center (SOC) to enable Blue Team members to continuously monitor and respond to advanced cyber threats. The integration of Wazuh, ELK, and TheHive has created a comprehensive defense platform offering advanced features, effective collaboration, and clear data visualization. This implementation enhances the company's security posture to address current and future threats. The project faced several challenges, including hardware limitations, time constraints, and a lack of appropriate resources and documentation, particularly concerning MISP. Despite these obstacles, the other aspects of the project were successfully completed, demonstrating our ability to adapt and make the most of the available resources.

Table des Matières

Remerciements.....	3
Résumé.....	4
Abstract.....	5
Table des Matières.....	6
Table des figures.....	9
Listes des abréviations.....	10
Introduction générale.....	11
Chapitre 1 : Contexte Général du projet.....	12
I. Introduction :.....	13
II. Problématique :.....	13
III. Solution : Centre d'Opérations de Cybersécurité :.....	14
1. Définition du SOC :.....	14
2. Objectifs :.....	14
Figure 1 : Fonctions du SOC.....	15
3. Différence entre SOC et CSIRT:.....	16
4. Les composants fondamentaux du SOC:.....	16
5. Les Rôles et responsabilités au sein d'un SOC :.....	17
Figure 2 : Rôles au sein du SOC.....	17
6. Les Outils technologiques dans un SOC :.....	17
Figure 4 : SOAR.....	18
IV. Méthodologie de gestion de projet :.....	20
Figure 6 : Diagramme de Gantt.....	20
V. Conclusion :.....	21
Chapitre 2 : Etat de l'art.....	21
I. Introduction :.....	22
II. La sécurité informatique en général :.....	22
III. Définition générale des risques:.....	23
IV. Les attaques:.....	23
1. Attaque des réseaux.....	23
2. Attaques du système :.....	25
3. Attaques applicatives :	25
V. Les contrôles de sécurité:.....	26
1. Pare-feu (Firewall):.....	27
2. Systèmes de détection et de prévention des intrusions (IDS/IPS) :	27
3. Authentification et contrôle d'accès:.....	27
4. Chiffrement des données:.....	28

5. Virtual Private Network (VPN):.....	28
6. Surveillance du réseau:.....	29
VI. Conclusion :.....	29
Chapitre 3 : ENVIRONNEMENT TECHNIQUE DE TRAVAIL.....	30
Partie 1: SIEM.....	31
I. Introduction :.....	31
II. Les journaux :.....	32
1. Définition :.....	32
2. Journalisation locale :.....	32
3. Centralisation des logs :.....	33
III. Gestion de sécurité des informations et des évènements :.....	33
1. Définition de SIEM:.....	34
2. Solutions SIEM existantes:.....	35
Figure 7 : Elastic logo.....	35
Figure 8 : QRadar logo.....	35
Figure 9 : Splunk logo.....	36
Figure 10 : Wazuhlogo.....	36
3. Étude comparative des différentes solution SIEM :.....	36
Tableau 1 : Tableau comparatif SIEM, Caractéristiques.....	38
Tableau 2 : Tableau comparatif SIEM, Fonctionnement.....	39
4. Choix de solution SIEM.....	39
IV. Wazuh :.....	39
1. Principe :.....	39
Figure 11 : Architecture de ELK/Wazuh.....	40
2. Pourquoi ELK/Wazuh :.....	40
3. Fonctionnement de Wazuh :.....	41
4. Architecture de Déploiement de Wazuh :.....	41
Figure 12 : architecture de Déploiement de Wazuh.....	42
Partie 2: SOAR.....	42
1. Définition de Security Orchestration, Automation and Response :.....	43
Figure 13 : SOAR overview.....	44
2. Les avantages de SOAR :.....	44
3. Analyse comparative de SOAR:.....	45
Figure 14 : TheHive Logo.....	45
Figure 15 : Demisto Logo.....	46
Figure 16 : Swimlane Logo.....	46
4. Choix de solution.....	46
1. Définition:.....	47
2. Les fonctionnalités de TheHive:.....	47
3. Architecture de TheHive:.....	49
Figure 17 : TheHive architecture.....	49
1. Définition:.....	49
2. Les fonctionnalités de Cortex:.....	49
Figure 18 : Architecture de Cortex.....	51

1. Définition de MISP:.....	51
2. Fonctionnalités de MISP:.....	51
Figure 19 : Architecture de Misp.....	53
Partie 3: Autres outils utilisés (IDS, Sandbox).....	54
1. Avantages de Suricata :.....	55
2. Les principales fonctionnalités.....	56
3. Fonctionnement :.....	57
Principales Caractéristiques de Docker :.....	58
Avantages de l'Utilisation de Docker :.....	59
Conception de l'architecture du projet.....	60
Chapitre 4 : IMPLEMENTATION DE LA SOLUTION ET PREUVE DE CONCEPT (POC)..	62
I. Introduction :.....	63
II. Description de l 'environnement de travail :.....	63
Tableau 3. Description de l 'environnement.....	63
III. Déploiement All-in-one :.....	63
IV. Wazuh agent :.....	65
V. Installation de Graylog — Ingestion de Journaux :.....	71
VI. Surveillance du système:.....	86
VII. Configuration de Grafana : Tableaux de bord SIEM open source.....	92
VIII. Surveillance du système:.....	108
IX. Détection d'un malware avec l'intégration de Yara.....	109
X. Intégration de SURICATA.....	114
1. Aperçu général.....	114
2. Résumé du fonctionnement de Suricata avec Wazuh :.....	115
XI. Mise en place de TheHIVE.....	116
1. Installation docker :.....	116
2. Deploiement Cortex et theHive avec docker :.....	117
3. Configuration de Cortex :.....	119
4. Configuration de Cortex avec TheHive :.....	125
XII. Conclusion:.....	126
Conclusion générale.....	127
Références :	129

Table des figures

Figure 1 : Fonctions du SOC.....	15
Figure 2 : Rôles au sein du SOC.....	17
Figure 4 : SOAR.....	18
Figure 6 : Diagramme de Gantt.....	20
Figure 7 : Elastic logo.....	35
Figure 8 : QRadar logo.....	35
Figure 9 : Splunk logo.....	36
Figure 10 : Wazuhlogo.....	36
Tableau 1 : Tableau comparatif SIEM, Caractéristiques.....	38
Tableau 2 : Tableau comparatif SIEM, Fonctionnement.....	39
Figure 11 : Architecture de ELK/Wazuh.....	40
Figure 12 : architecture de Déploiement de Wazuh.....	42
Figure 13 : SOAR overview.....	44
Figure 14 : TheHive Logo.....	45
Figure 15 : Demisto Logo.....	46
Figure 16 : Swimlane Logo.....	46
Figure 17 : TheHive architecture.....	49
Figure 18 : Architecture de Cortex.....	51
Figure 19 : Architecture de Misp.....	53
Tableau 3. Description de l 'environnement.....	63

Listes des abréviations

Abréviation	Signification
SOC	Security Operations Center
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
IDS	Intrusion Detection System
ELK	Elasticsearch, Logstash, Kibana (Elastic Stack)
MISP	Malware Information Sharing Platform
API	Application Programming Interface

Introduction générale

À mesure que la technologie continue de progresser et d'évoluer, elle ouvre de nouvelles portes, offrant des opportunités inédites, des améliorations de productivité et une connectivité accrue. Cependant, cette montée en puissance rapide de la technologie s'accompagne également d'une menace grandissante en matière de sécurité. Les cyberattaques ont connu une croissance exponentielle ces dernières années, devenant toujours plus sophistiquées et ciblées, ce qui place la sécurité des systèmes d'information au cœur des préoccupations dans le monde numérique contemporain.

La détection précoce des menaces et une réponse rapide aux incidents sont désormais des impératifs pour protéger les infrastructures et les données sensibles. Pour ce faire, les entreprises et les organisations doivent adopter une approche holistique de la sécurité, en mettant en place des stratégies et des mesures de protection à plusieurs niveaux. En combinant des technologies de pointe avec une vigilance constante et une culture de sécurité, il est possible de renforcer la résilience face aux attaques potentielles et d'assurer la pérennité des opérations dans un environnement numérique en constante évolution.

De plus, il est crucial de reconnaître que la sécurité informatique ne se limite pas à la mise en place de logiciels et de pare-feu sophistiqués. Elle repose également sur la sensibilisation et la formation des employés pour qu'ils puissent reconnaître les signes d'une tentative d'intrusion ou d'une cyberattaque. La collaboration entre les équipes de sécurité et les autres départements est également essentielle pour garantir une approche coordonnée et efficace face aux menaces émergentes.

En adoptant une approche proactive et en investissant dans des solutions de sécurité robustes, les entreprises peuvent non seulement réduire les risques liés aux cyberattaques, mais aussi renforcer leur compétitivité et leur réputation sur le marché. La sécurité des systèmes d'information n'est plus un simple enjeu technique, mais une composante stratégique fondamentale pour assurer la continuité des activités et la confiance des clients dans un monde numérique en constante évolution.

Chapitre 1 : Contexte Général du projet

I. Introduction :

Ce chapitre fournit un aperçu détaillé du rôle essentiel du SOC Next Gen dans la défense proactive contre les menaces cybernétiques et établit les bases nécessaires pour comprendre les concepts et stratégies discutés tout au long du projet. Il sert de fondation solide pour appréhender les enjeux et les actions à entreprendre dans notre démarche de renforcement de la sécurité des actifs de l'organisation.

II. Problématique :

Les cyberattaques:

Les cyberattaques sont devenues une menace omniprésente et de plus en plus sophistiquée, compromettant la sécurité des systèmes d'information des entreprises. Ces attaques ciblées et complexes peuvent provoquer des interruptions d'activité, des pertes financières importantes et des atteintes à la réputation des organisations. La capacité à détecter rapidement ces menaces et à y répondre efficacement est cruciale pour protéger les infrastructures critiques et les données sensibles.

Cependant, les solutions de sécurité traditionnelles ne sont souvent pas à la hauteur face à l'évolution rapide des techniques d'attaque. Les entreprises doivent donc adopter une approche intégrée et proactive, combinant des outils avancés de gestion des incidents, de détection et de réponse, et d'automatisation de la sécurité, afin de renforcer leur résilience face aux cybermenaces.

La quantité élevée des données:

L'augmentation rapide des volumes de données et la complexité croissante des infrastructures informatiques posent un défi majeur pour la sécurité des entreprises. Gérer et analyser efficacement ces vastes quantités de données pour détecter des anomalies et des menaces potentielles est une tâche ardue. De plus, la diversité des sources de données et la nécessité de les corrélérer en temps réel ajoutent une couche supplémentaire de complexité.

III. Solution : Centre d'Opérations de Cybersécurité :

1. Définition du SOC :

Un SOC (Security Operations Center) est avant tout une équipe d'experts en sécurité qui joue un rôle crucial dans la protection des systèmes d'information. Leur mission principale consiste à surveiller en permanence les activités de sécurité, détecter les menaces potentielles, analyser les incidents et évaluer leur gravité et impact. L'équipe du SOC est responsable de prendre les mesures nécessaires pour réagir aux incidents de sécurité confirmés et minimiser leur durée et leur impact sur les opérations quotidiennes de l'organisation.

En plus de la surveillance et de la détection des menaces, le SOC assume des responsabilités opérationnelles importantes, telles que la gestion des dispositifs de sécurité, le durcissement des systèmes d'exploitation pour renforcer leur sécurité, la gestion des droits d'accès aux ressources, ainsi que la gestion des correctifs et des mises à jour de sécurité.

En collaboration étroite avec les services informatiques, le SOC vise à réduire la durée et l'impact des incidents de sécurité qui exploitent, perturbent, empêchent, dégradent ou détruisent les systèmes utilisés pour les opérations courantes. Cet objectif est atteint grâce à une surveillance efficace et à un suivi complet des incidents.

Les SOC sont généralement composés d'analystes et d'ingénieurs en sécurité, ainsi que de managers supervisant les opérations de sécurité.

2. Objectifs :

On peut résumer les principales fonctions d'un SOC comme suit :



Figure 1 : Fonctions du SOC

Enquête sur les actifs : Pour qu'un SOC puisse efficacement protéger une entreprise, il doit avoir une connaissance exhaustive des ressources à sécuriser. Sans cette compréhension, il risque de ne pas couvrir l'ensemble du réseau. Une étude des actifs doit identifier chaque serveur, routeur, pare-feu sous le contrôle de l'entreprise, ainsi que tout autre outil de cybersécurité en usage.

Collecte de logs : Les données sont essentielles au bon fonctionnement d'un SOC, et les journaux constituent la principale source d'informations sur l'activité du réseau. Le SOC doit établir des flux de données en temps réel à partir des systèmes de l'entreprise. Les humains ne pouvant assimiler de telles quantités d'informations, les outils d'analyse des journaux alimentés par des algorithmes d'intelligence artificielle deviennent indispensables pour les SOC.

Maintenance préventive : Le SOC peut prévenir les cyberattaques en adoptant des processus proactifs, tels que l'installation de correctifs de sécurité et l'ajustement régulier des politiques de pare-feu. Étant donné que certaines cyberattaques peuvent provenir de menaces internes, le SOC doit également identifier les risques au sein de l'organisation.

Surveillance continue : Pour être prêt à réagir à un incident de cybersécurité, le SOC doit maintenir une surveillance constante. Quelques minutes peuvent faire la différence entre bloquer une attaque et voir un système ou un site web entier mis hors service. Les outils du SOC analysent le réseau de l'entreprise pour détecter les menaces potentielles et autres activités suspectes.

Gestion des alertes : Les systèmes automatisés sont excellents pour détecter des schémas et suivre des scripts. Cependant, le personnel du SOC doit savoir comment réagir et vérifier la légitimité des alertes.

Analyse des causes profondes : Une fois l'incident résolu, le travail du SOC continue. Les experts en cybersécurité analysent la cause profonde du problème et diagnostiquent pourquoi il s'est produit. Cela permet une amélioration continue des outils et des règles de sécurité pour éviter que le même incident ne se reproduise à l'avenir.

Audits de conformité : Les entreprises doivent s'assurer que leurs données et systèmes sont sécurisés et conformes aux lois. Les fournisseurs de SOC doivent effectuer des audits réguliers pour vérifier leur conformité dans les régions où ils opèrent. Les équipes SOC ont la responsabilité de déclarer les incidents sur le SI et de mener les opérations nécessaires à leur résolution. Du point de vue opérationnel, c'est le couple SOC et CERT/C-SIRT qui assure la résolution des incidents.

3. Différence entre SOC et CSIRT:

Selon l'ENISA (Agence de l'Union européenne pour la cybersécurité), un CSIRT (Computer Security Incident Response Team) est une équipe d'experts en sécurité informatique dont la principale mission est de répondre aux incidents de sécurité en fournissant les services nécessaires pour traiter les attaques et en aidant les parties prenantes à restaurer les systèmes affectés. La distinction entre un SOC (Security Operations Center) et un CSIRT peut parfois être floue.

Cependant, il est généralement admis que le SOC est responsable de la gestion des vulnérabilités, de la détection et de la qualification des incidents de sécurité, tandis que le CSIRT est responsable de la gestion de crise cyber (qui englobe une notion plus large que la simple réaction à un incident de sécurité) et de la surveillance des cyber menaces, y compris les analyses forensiques.

4. Les composants fondamentaux du SOC:

Le SOC repose sur trois composants essentiels :

- **Ressources humaines (People)** : Les experts en sécurité informatique constituent une partie essentielle du SOC. Ils sont responsables de la surveillance, de la détection et de l'analyse des événements de sécurité.
- **Processus (Process)** : Les processus sont des étapes clairement définies et documentées qui guident les opérations du SOC. Ils incluent la gestion des incidents de sécurité, la détection et l'analyse des menaces, la réponse aux incidents, la remédiation et la récupération après un incident. Ces processus assurent une approche méthodique et cohérente dans la gestion des événements de sécurité. Ils sont conçus pour optimiser l'efficacité et la réactivité du SOC face aux menaces.

- **Les outils techniques (Technology)** : Le SOC utilise une variété d'outils et de technologies pour surveiller et analyser les événements de sécurité. Cela comprend généralement un Security Information and Event Management (SIEM) qui permet de collecter, d'agréger et de corrélérer les données de sécurité provenant de diverses sources.

5. Les Rôles et responsabilités au sein d'un SOC :



Figure 2 : Rôles au sein du SOC

6. Les Outils technologiques dans un SOC :

Un Centre des Opérations de Sécurité (SOC) est constitué d'un ensemble d'outils regroupés dans des piles technologiques distinctes, permettant ainsi aux analystes de la cybersécurité de surveiller en continu l'activité de sécurité au sein de l'infrastructure informatique d'une organisation.

a. SIEM (Security Information and Event Management) :

Le SIEM est un système qui collecte, corrèle et analyse les informations de sécurité provenant de différents éléments du système d'information. Il permet de détecter les menaces et les incidents de sécurité en temps réel en analysant les journaux, les événements et les alertes générés par les systèmes, les applications et les périphériques du réseau.

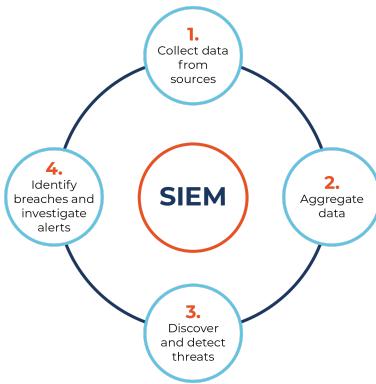


Figure 3 : SIEM

b. XDR (Extended Detection and Response)

Le XDR est une évolution du SIEM qui élargit la portée de la détection et de la réponse aux incidents de sécurité. Contrairement au SIEM traditionnel, qui se concentre principalement sur les journaux et les événements, le XDR intègre des données provenant de différentes sources de sécurité, telles que les endpoints (terminaux), le réseau, les applications cloud, etc. Il offre une visibilité plus large et une détection plus précise des menaces, ainsi qu'une réponse coordonnée.

c. SOAR (Security Orchestration, Automation, and Response)

Le SOAR est une plateforme qui automatise et orchestre les processus de sécurité. Il permet aux équipes du SOC de gérer efficacement les incidents en automatisant les tâches répétitives et en intégrant les outils de sécurité existants. Le SOAR facilite également la collaboration entre les équipes et améliore les délais de réponse aux incidents.

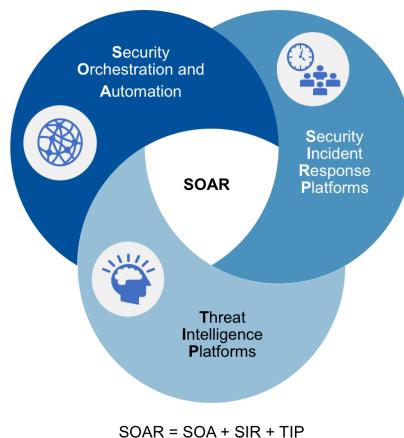


Figure 4 : SOAR

d. TIP (Threat Intelligence Platform)

Les plateformes de renseignement sur les menaces sont chargées d'agréger et d'analyser les renseignements sur les menaces afin d'en tirer des informations utiles. Voici quelques-unes des étapes clés de ce processus :

Collecte et agrégation des données : Les organisations ont généralement accès à des renseignements sur les menaces provenant de nombreuses sources internes et externes. Un TIP recueille des données provenant de toutes ces sources afin de fournir une image plus complète et contextuelle du paysage des cybermenaces.

Normalisation et déduplication : renseignements sur les menaces Les données peuvent se présenter sous différents formats et inclure des données redondantes. La normalisation permet de convertir les données collectées dans un format commun, ce qui permet de supprimer les données en double.

Traitement : Les TIP traitent les données qu'ils ont collectées pour les transformer en renseignements et rapports utiles à l'organisation. Par exemple, les TIP peuvent générer des indicateurs de compromission (IoC) qui permettent à une organisation d'identifier plus rapidement les menaces potentielles.

Intégration : Les TIP peuvent être intégrés au reste de l'architecture de sécurité d'une organisation, y compris les Pare-feu de nouvelle génération (NGFW), les systèmes de poste de détection et de réponse (EDR), de **détection et de réponse étendues** (XDR) et de gestion de l'information et des événements de sécurité (SIEM). Cette intégration permet de distribuer rapidement les IoC aux systèmes qui peuvent les utiliser pour bloquer les attaques et informer le personnel de sécurité des menaces pressantes.

Analyse : Un TIP doit permettre aux utilisateurs d'accéder aux données et de les visualiser de manière conviviale. Un TIP doit permettre des requêtes et peut avoir la capacité de générer des rapports prédéfinis ou personnalisés pour répondre aux besoins des différentes parties prenantes.

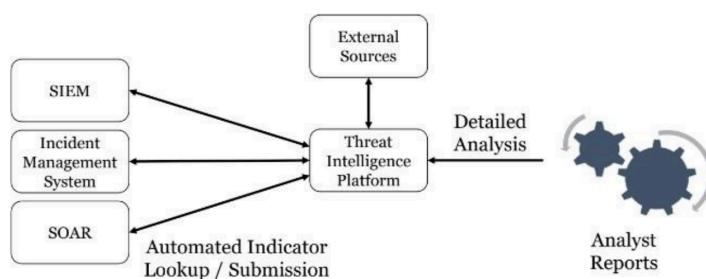


Figure 5 : TIP

e. Incident Management System

Les systèmes de gestion des incidents sont des plateformes ou des outils utilisés par les équipes de sécurité (Blue Teams) pour enregistrer, suivre et gérer les enquêtes et actions liées aux incidents. Ces systèmes offrent un espace centralisé où sont documentées les informations pertinentes sur les incidents, facilitant ainsi une meilleure collaboration et une gestion efficace des problèmes de sécurité.

En général, les équipes se procurent une solution à partir de trois sources principales : un fournisseur proposant un logiciel de gestion des tickets généralisé, similaire à ceux utilisés par les services d'assistance technique ; une solution intégrée à l'un de leurs outils tels qu'un SIEM ; ou un système de gestion des tickets spécifiquement axé sur la sécurité. Les systèmes dédiés à la sécurité sont généralement les plus adaptés, car ils sont conçus pour répondre aux besoins spécifiques des équipes de sécurité. Ils incluent souvent toutes les fonctionnalités typiques d'un système de gestion des tickets, mais comportent également des fonctionnalités supplémentaires cruciales pour les professionnels de la sécurité, telles que la possibilité d'enregistrer des indicateurs de compromission (IOCs) associés à une enquête et des intégrations avec des plateformes de renseignement sur les menaces.

IV. Méthodologie de gestion de projet :

La planification du projet est une phase importante avant d'entamer la phase de réalisation. Elle consiste à prévoir le déroulement de ce dernier tout au long des phases du cycle de développement.

Le diagramme de Gantt est le moyen idéal pour coordonner les tâches entre les membres de l'équipe et de visualiser le temps consacré à la réalisation de chaque tâche. Voici ci-dessous le diagramme de Gantt de notre projet :

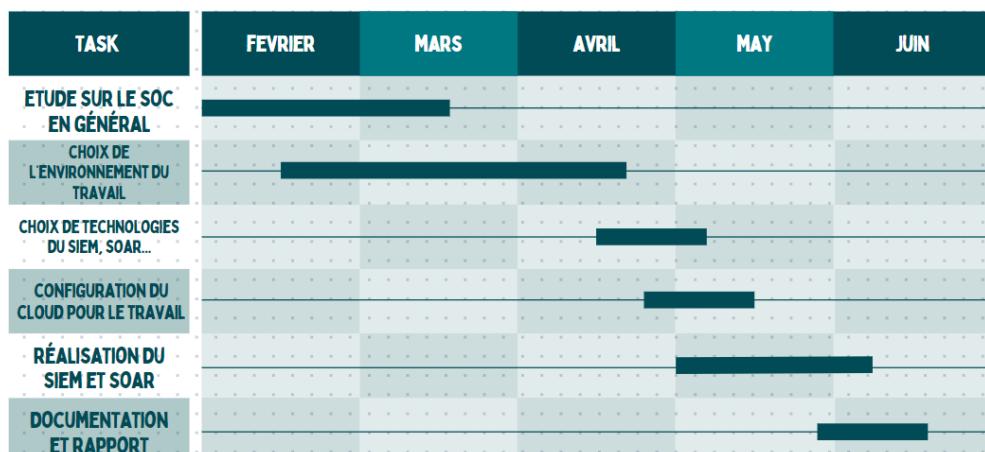


Figure 6 : Diagramme de Gantt

V. Conclusion :

D'après tous ce qu'on a élaboré dans ce chapitre, on peut conclure que la réalisation d'un centre opérationnel de sécurité nécessite la présence d'un SIEM pour la collection des logs et génération des alertes et puis un SOAR pour l'analyse de ces alertes d'une façon automatisée et la création des cases etc.

Chapitre 2 : Etat de l'art

I. Introduction :

Ce chapitre propose une analyse approfondie du rôle essentiel du SOC Next Gen dans la défense proactive contre les menaces cybernétiques, et fournit les bases nécessaires pour comprendre les concepts et les stratégies développés tout au long du projet. Il constitue un socle solide pour une compréhension complète des enjeux et des mesures à mettre en œuvre afin de renforcer la sécurité des actifs de l'organisation. En abordant les défis actuels et les solutions innovantes, ce chapitre prépare le lecteur à apprécier les actions cruciales pour améliorer la résilience de l'infrastructure numérique de l'entreprise.

II. La sécurité informatique en général :

La sécurité informatique englobe toutes les activités visant à protéger la fonctionnalité et l'intégrité de votre réseau et de vos données, les applications, les appareils et les systèmes qui sont connectés au réseau. Et à empêcher et surveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'un réseau informatique et des ressources accessibles sur le réseau. La sécurité informatique vise généralement 5 principaux objectifs :

- **L'intégrité** : Garantir que les données sont bien celles que l'on croit être.
- **La disponibilité** : Ce principe vise à maintenir le bon fonctionnement du système d'information, en s'assurant que les ressources sont accessibles et utilisables lorsque nécessaire, en minimisant les interruptions et les pannes.

- **La confidentialité** : Rendre les données inintelligibles et inaccessibles à des personnes non autorisées, garantissant ainsi que seuls les acteurs autorisés peuvent y accéder.
- **Authenticité** : S'assurer que l'identité des utilisateurs, des systèmes et des données peut être vérifiée avec certitude.
- **Non-répudiation** : Garantir qu'une transaction ne peut être niée

III. Définition générale des risques:

Les risques peuvent être définis comme la probabilité d'occurrence d'un événement indésirable combinée à son impact potentiel, alors le risque fait référence aux menaces potentielles qui pourraient compromettre l'intégrité, la confidentialité et la disponibilité des systèmes informatiques, des réseaux et des données. Ces risques peuvent provenir d'une multitude de sources, notamment des cybercriminels, des erreurs humaines, des failles de sécurité, des vulnérabilités logicielles ou matérielles, des attaques ciblées et des incidents imprévus.

IV. Les attaques:

Dans un monde où le progrès technologique avance à grande vitesse, où les gens, les entreprises, les organismes, les pays et même les objets sont de plus en plus connectés, les attaques informatiques sont de plus en plus fréquentes. Une attaque informatique est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. Les attaques touchent généralement trois composantes du système à savoir la couche réseau, le système d'exploitation et la couche applicative. La question de la cybersécurité se pose à tous les niveaux et tend à devenir un enjeu essentiel ces prochaines années. Pour mieux se protéger, il est primordial de savoir à quoi s'attendre, et donc de connaître les attaques informatiques les plus courantes. En voici une liste des types d'attaques :

1. Attaque des réseaux

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. La sécurité informatique est devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les infrastructures de télécommunication modernes. Les attaques sur les réseaux informatiques peuvent être menées de différentes manières et peuvent avoir des conséquences graves. Parmi ces attaques :

a. Man in the middle (MITM)

Encore connus sous le nom de « l'attaque de l'homme du milieu », dans cette attaque, une machine malveillante intercepte les paquets envoyés entre deux parties, sans que ni l'un ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

L'attaquant modifie les paquets et les envoie ensuite à la destination prévue, les machines d'origine et de réception ignorant que leur communication a été altérée. Généralement, ce type d'attaque est utilisé pour amener les cibles à révéler des informations sécurisées et à poursuivre ces transmissions pendant un certain temps, tout en ignorant que la machine au milieu de la transmission écoute tout le temps.

b. Denial of service (DoS)

Denial of Service ou DoS attack (L'attaque de déni de service) est une technique d'attaque informatique visant à rendre inaccessible un système ou un service, en inondant le serveur de trafic ou de demandes de connexion, ce qui entraîne une surcharge du système et une incapacité à répondre aux demandes légitimes Il s'agit de :

- L'inondation d'un réseau afin d'empêcher son fonctionnement ;
- La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier.
- L'obstruction d'accès à un service à une personne en particulier.
- Également le fait d'envoyer des millions de kilooctets à une box Wi-Fi.

L'attaquant n'a pas forcément besoin de matériel sophistiqué. Ainsi, certaines attaques DoS peuvent être exécutées avec des ressources limitées contre un réseau beaucoup plus grand et moderne. Un hacker avec un ordinateur obsolète et un modem lent peut ainsi neutraliser des machines ou des réseaux beaucoup plus importants.

c. Phishing attack

Une attaque de phishing ou (Attaque par hameçonnage) est une technique d'ingénierie sociale utilisée par les cybercriminels pour tromper les utilisateurs et les inciter à divulguer des informations confidentielles telles que des noms d'utilisateur, des mots de passe, des numéros de carte de crédit ou des informations bancaires, ou à cliquer sur des liens malveillants. Les attaquants utilisent souvent des courriels ou des messages texte qui semblent provenir d'une source légitime, telle qu'une banque ou un service de messagerie, pour inciter les utilisateurs à fournir des informations sensibles telles que des noms d'utilisateur, des mots de passe ou des numéros de carte de crédit. Les attaquants peuvent également utiliser des sites Web malveillants pour piéger les utilisateurs et leur faire télécharger des logiciels malveillants ou leur faire saisir des informations sensibles, les attaquants de phishing peuvent aussi envoyer des messages contrefaits à partir de comptes de réseaux sociaux piratés.

2. Attaques du système :

Les systèmes d'exploitation sont des programmes qui permettent à l'appareil informatique de fonctionner en faisant l'interface entre l'utilisateur et le matériel informatique. Ils fournissent une interface entre le matériel informatique et les applications, permettant ainsi aux utilisateurs d'interagir avec leur ordinateur. Malheureusement, les systèmes d'exploitation sont également vulnérables aux attaques. Les attaquants peuvent exploiter ces vulnérabilités pour compromettre un système, accéder à des informations sensibles ou effectuer des activités malveillantes.

a. Blue screen of death (BSOD)

L'attaque de l'écran bleu de la mort, également connue sous le nom d'attaque BSOD, est une attaque qui vise à planter un système d'exploitation Windows en provoquant un écran bleu de la mort. Cette attaque est généralement utilisée par l'injection d'un code malveillant dans un pilote de périphérique, l'envoi de paquets réseau malformés, ou l'exploitation de vulnérabilités connues dans le système d'exploitation. Lorsqu'un système d'exploitation Windows plante en raison d'une attaque BSOD, l'écran bleu de la mort s'affiche, ce qui rend le système d'exploitation inutilisable jusqu'à ce qu'il soit redémarré. Cette attaque peut être utilisée pour dégrader les performances d'un système, pour empêcher l'accès à des ressources critiques ou pour perturber les opérations d'un réseau.

b. Attaque par force brute

Brute-force attack ou attaque par force brute est une tentative visant à craquer un mot de passe ou un nom d'utilisateur, ou encore à trouver une page Web cachée ou la clé utilisée pour chiffrer un message, via un processus d'essais et d'erreurs pour, au bout du compte, espérer deviner juste. Ensuite, ils ont le champ libre pour récupérer les données, propager des malwares et ransomwares, ou encore détourner le trafic de sites Web. C'est une vieille méthode d'attaque, mais elle reste efficace et répandue parmi les pirates. En fonction de la longueur et de la complexité du mot de passe, le craquage peut prendre entre quelques secondes et plusieurs années. En théorie la complexité d'une attaque par force brute est une fonction exponentielle de la longueur du mot de passe, la rendant virtuellement impossible pour des mots de passe de longueur moyenne. Les attaques par force brute peuvent être utilisées pour attaquer des systèmes d'authentification tels que les comptes utilisateur, les serveurs FTP, les réseaux Wi-Fi, les systèmes de cryptage de fichiers, et même des algorithmes de hachage de mots de passe.

3. Attaques applicatives :

L'augmentation de la complexité des applications et la diversité des plateformes sur lesquelles elles sont déployées, les attaques applicatives sont devenues une préoccupation de plus en plus importante pour les entreprises et les organisations qui utilisent des

applications pour stocker des informations sensibles et des données confidentielles. Les attaques applicatives sont des méthodes malveillantes utilisées pour exploiter les vulnérabilités des applications.

a. Attaque par injection SQL

Une attaque par injection SQL est une technique d'attaque informatique qui consiste à insérer du code SQL malveillant dans les champs de saisie d'une application, qui peut ensuite être exécuté par la base de données de l'application. Les attaquants injectent des commandes SQL malveillantes dans les entrées de l'application Web, dans le but de compromettre les données stockées dans la base de données. Les attaques par injection SQL sont souvent utilisées pour accéder ou modifier des données sensibles, telles que des mots de passe, des détails de carte de crédit ou des informations personnelles sur l'utilisateur. Les attaquants peuvent également utiliser cette technique pour modifier ou supprimer des données, affectant ainsi l'intégrité des données stockées dans la base de données.

b. Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) est une attaque qui force les utilisateurs authentifiés à soumettre une requête à une application Web contre laquelle ils sont actuellement authentifiés. Les attaques CSRF exploitent la confiance qu'une application Web accorde à un utilisateur authentifié. (Inversement, les attaques de script intersites (XSS) exploitent la confiance qu'un utilisateur a dans une application Web particulière). Une attaque CSRF exploite une vulnérabilité dans une application Web si elle ne peut pas faire la différence entre une requête générée par un utilisateur individuel et une requête générée par un utilisateur sans son consentement.

c. Cross-Site Scripting (XSS)

Cross-Site Scripting se produisent lorsque des attaquants ou des utilisateurs malveillants peuvent manipuler un site Web ou une application Web pour renvoyer du code JavaScript malveillant aux utilisateurs. Lorsque ce JavaScript malveillant est exécuté dans le navigateur de l'utilisateur, toutes les interactions de l'utilisateur avec le site (y compris, mais sans s'y limiter, l'authentification et le paiement) peuvent être compromises par l'attaquant.

V. Les contrôles de sécurité:

Les contrôles de sécurité sont des paramètres mis en œuvre pour protéger diverses formes de données et d'infrastructure importantes pour une organisation. Tout type de sauvegarde ou de contre-mesure utilisé pour éviter, détecter, contrer ou réduire les risques de sécurité pour les biens physiques, les informations, les systèmes informatiques ou d'autres actifs est considéré comme un contrôle de sécurité. Il existe plusieurs types de contrôles d'accès, Voici quelques exemples :

1. Pare-feu (Firewall):

Un firewall, ou pare-feu, est un système de sécurité pour réseaux informatiques qui régule le trafic Internet entrant, sortant, ou interne à un réseau privé. Ce dispositif, qu'il soit logiciel ou une combinaison matériel-logiciel dédiée, fonctionne en filtrant sélectivement les paquets de données, bloquant ou autorisant leur passage. Son objectif principal est de prévenir les activités malveillantes et d'empêcher toute personne, tant à l'intérieur qu'à l'extérieur du réseau privé, de s'engager dans des activités Web non autorisées.

2. Systèmes de détection et de prévention des intrusions (IDS/IPS) :

Un système de détection d'intrusion (IDS) est utilisé pour identifier les attaques contre un réseau ou un système informatique à un stade précoce. Le logiciel IDS nécessaire peut être installé sur le système informatique à surveiller ou sur un appareil distinct. Ces systèmes surveillent et analysent toutes les activités du réseau pour détecter un trafic inhabituel et avertir l'utilisateur en cas de détection. Cela permet à l'utilisateur de réagir aux tentatives d'accès au système par des intrus et de prévenir ainsi une attaque.

Après avoir détecté une attaque potentielle, les systèmes de prévention d'intrusion (IPS) non seulement informent l'administrateur, mais mettent également en place des contre-mesures appropriées immédiatement. Cela évite un délai trop long entre la détection d'un problème et la réaction, contrairement aux logiciels IDS.

Un système de prévention d'intrusion doit généralement être configurable de manière individuelle pour éviter que les actions courantes de l'utilisateur ne soient classées comme dangereuses et bloquées par le détecteur d'anomalies.

3. Authentification et contrôle d'accès:

Les systèmes d'authentification et de gestion des sessions sont des fonctionnalités critiques des applications web. L'authentification permet de s'assurer que seuls des utilisateurs légitimes peuvent accéder à l'application tandis que le mécanisme des sessions assure le suivi des diverses actions réalisées par les utilisateurs sur l'application. Ils incluent l'utilisation de mots de passe forts, d'authentification à deux facteurs, de certificats numériques, de contrôles de permissions et de politiques d'accès.

Souvent ciblées lors d'attaques, les vulnérabilités exploitées sur ces mécanismes permettent aux attaquants d'usurper ou de détourner des comptes ou des sessions utilisateurs. Il est donc nécessaire de concevoir des systèmes sécurisés pour contrer ces attaques et garantir l'intégrité de vos données.

4. Chiffrement des données:

En cryptographie, le cryptage est le processus de codage d'un message ou d'une information de manière que seules les parties autorisées puissent y accéder et que celles qui ne sont pas autorisées ne le puissent pas. Le cryptage est divisé en deux types :

- **Chiffrement symétrique** : Également appelé chiffrement à clé privée. La clé utilisée pour encoder est la même que celle utilisée pour décoder, ce qui convient parfaitement pour les utilisateurs individuels et les systèmes fermés. Autrement, la clé doit être envoyée au destinataire, ce qui augmente le risque de compromission si elle est interceptée par un tiers (un cybercriminel, par exemple). Cette méthode est plus rapide que la méthode asymétrique.
- **Chiffrement asymétrique** : cette méthode utilise deux clés différentes (publique et privée) mathématiquement liées. Concrètement, les clés se composent uniquement de grands nombres qui ont été couplés entre eux mais ne sont pas identiques, d'où le terme asymétrique. La clé privée est tenue secrète par le propriétaire et la clé publique est soit partagée parmi les destinataires autorisés, soit mise à disposition du public à grande échelle.

Le chiffrement permet de protéger les données sensibles en les rendant illisibles pour les personnes non autorisées. Il est utilisé pour sécuriser les communications réseau, les fichiers et les sauvegardes.

5. Virtual Private Network (VPN):

Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel » .

La technique consiste à utiliser Internet comme support de transmission en utilisant un protocole de « tunnelling » (en anglais tunneling), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de VPN pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

Le VPN permet donc d'obtenir une liaison sécurisée à moindre coût. Le VPN vise à apporter certains éléments essentiels dans la transmission de données :

- L'authentification (et donc l'identification) des interlocuteurs,

- La confidentialité des données (le chiffrement vise à les rendre inutilisables par quelqu'un d'autre que le destinataire).

6. Surveillance du réseau:

La surveillance constante du réseau permet de détecter les anomalies, les comportements suspects ou les activités malveillantes. Des outils de surveillance tels que les systèmes de gestion des informations et des événements de sécurité (SIEM) sont utilisés pour analyser les journaux d'événements et les alertes de sécurité.

VI. Conclusion :

En conclusion, la prévention des cyberattaques reste primordiale dans un environnement professionnel. Bien que la mise en place de contrôles de sécurité soit cruciale, il est tout aussi important de reconnaître qu'aucune méthode n'est infaillible malgré les efforts déployés. C'est pourquoi la détection proactive des cyberattaques devient indispensable.

Pour y parvenir, il est nécessaire de collecter les logs de tous les appareils présents sur notre réseau et de développer une approche de détection et de réponse active. Cette approche nous permettra d'anticiper les intrusions potentielles et de les identifier rapidement avant qu'elles ne causent des dommages significatifs. C'est pour cette raison que nous avons choisi de mettre en place un système de collecte de logs (SIEM) et un système de surveillance, de détection et de réponse aux menaces au niveau des terminaux (SOAR).

Chapitre 3 : ENVIRONNEMENT TECHNIQUE DE TRAVAIL

Partie 1: SIEM

I. Introduction :

Presque toutes les applications exécutées dans un environnement serveur génèrent automatiquement des journaux. Ces journaux sont une partie vitale de tout système car ils fournissent des informations essentielles sur le fonctionnement actuel d'un système et également sur son fonctionnement dans le passé. En effectuant une recherche dans les données du journal, vous pouvez identifier les problèmes, les erreurs et les tendances. Cependant, il peut être extrêmement fastidieux et frustrant de rechercher manuellement une erreur particulière sur des centaines, voire des milliers de serveurs, dans des milliers de fichiers journaux. Dans ce chapitre, nous nous concentrerons sur la mise en œuvre d'une solution de centralisation et gestion des journaux.

II. Les journaux :

1. Définition :

Les Logs, les événements ou les journaux ne sont que des notifications d'événements plus ou moins importants envoyés par des services, des systèmes, des éléments de réseau ou des applications. Les journaux d'événements permettent aux administrateurs système, réseau et sécurité de suivre le fonctionnement et le cycle de vie d'un système. Les logs ont une grande signification et importance en sécurité car il s'agit de savoir ce qui se passe sur un ensemble d'applications ou de systèmes afin de pouvoir :

- Expliquer les erreurs, les comportements anormaux, les pannes de services (tels que les services Web) ;
- Retracer la vie d'un utilisateur, d'une application, d'un paquet sur un réseau sur les logs d'un proxy et des éléments réseau par exemple ;
- Comprendre le fonctionnement d'une application, d'un protocole et d'un système, comme les étapes pour démarrer un service SSH sous Linux ;
- Recevoir des notifications sur les actions, les opérations, les modifications (telles que les arrêts ou les démarrages du système.

2. Journalisation locale :

Les journaux locaux, également appelés journaux système ou journaux des événements, sont des fichiers qui enregistrent les événements et les activités qui se produisent sur le système informatique local. Ils sont utilisés pour diagnostiquer les problèmes, suivre l'activité et assurer la sécurité du système. Les journaux locaux contiennent des informations telles que les erreurs système, les avertissements, les connexions des utilisateurs, l'activité du réseau et d'autres événements pertinents. Cependant, les journaux locaux peuvent avoir certaines limites.

- **Fragmentation des données :** dans les environnements comportant de nombreux systèmes, chaque machine possède ses propres journaux locaux, ce qui rend difficile la corrélation des événements et l'obtention d'une vue d'ensemble de l'infrastructure.
- **Difficulté de gestion :** la gestion et l'analyse des journaux pour chaque système individuellement peuvent être fastidieuses et inefficaces. Des connexions individuelles à chaque machine sont nécessaires pour accéder aux journaux et les surveiller.

- **Manque de centralisation :** Les journaux locaux sont stockés sur chaque système, ce qui signifie qu'en cas de panne de la machine ou de perte de données, les journaux correspondants peuvent ne pas être récupérables. De plus, la centralisation des informations pour l'analyse et le reporting peut être complexe.

3. Centralisation des logs :

Pour atténuer ces limitations, la centralisation des logs est une solution recommandée. Cela implique de collecter les journaux de tous les systèmes et de les stocker dans un emplacement centralisé. Voici quelques avantages de la journalisation centralisée :

- **Visibilité globale :** en centralisant les journaux, il devient plus facile d'avoir une visibilité sur votre infrastructure informatique. Les événements peuvent être corrélés, les tendances identifiées et les problèmes diagnostiqués plus rapidement.
- **Gestion simplifiée :** la centralisation simplifie la gestion des journaux. Au lieu de se connecter à chaque machine, les administrateurs peuvent accéder à un emplacement centralisé pour analyser et surveiller les journaux.
- **Résilience et sécurité améliorées :** en stockant les journaux dans un emplacement centralisé, des mécanismes de sauvegarde et de récupération des données peuvent être mis en œuvre. Cela réduit le risque de perte de données en cas de panne.
- **Analyse approfondie :** les journaux centralisés facilitent l'analyse des données à grande échelle. Les outils analytiques peuvent être utilisés pour détecter les tendances, les anomalies et les modèles de comportement qui peuvent indiquer des problèmes ou des menaces potentiels.

Donc, la journalisation centralisée offre un moyen plus efficace de gérer, d'analyser et d'utiliser les journaux système. Cela permet une meilleure visibilité, une gestion simplifiée, une plus grande résilience et des capacités d'analyse approfondies. Cela est fait par la mise en œuvre d'un système de gestion des événements « SIEM ».

III. Gestion de sécurité des informations et des événements :

1. Définition de SIEM:

Le principal outil constituant le SOC se nomme le SIEM. L'abréviation SIEM (Security Information and Event Management) est une combinaison des concepts SIM (Security Information Management) et SEM (Security Event Management). Ensemble, ces deux concepts couvrent l'ensemble de la sécurité informatique.

Un SIEM, ou système de gestion des informations et des événements de sécurité, prend en compte les exigences spécifiques de l'entreprise en définissant de manière claire et individuelle les processus et les événements liés à la sécurité, ainsi que les réactions appropriées et leur ordre de priorité. Il peut également être considéré comme un ensemble de règles pour les normes de sécurité applicables et comme un guide visant à maintenir la qualité dans le fonctionnement informatique d'une entreprise, voici les composantes du SIEM:

SEM (Security Event Management), permet : L'analyse en temps réel (ou quasi réel) des journaux. Cela permet au personnel de sécurité de prendre des mesures défensives plus rapidement.

- Gestion des événements de sécurité,
- Les corrélations d'événements,
- Les réponses aux incidents liés aux menaces internes et externes,
- L'analyse en temps réel pour prendre des mesures défensives rapides.

SIM (Security Information Management), fournit des rapports conformes à la réglementation et surveille les menaces internes. Il gère les journaux, génère des rapports et effectue des analyses différées.

Il est important de noter que SEM se concentre sur l'analyse en temps réel des événements de sécurité, tandis que SIM se concentre sur la gestion des informations de sécurité, la génération de rapports et l'analyse différée pour une meilleure compréhension des menaces et des tendances.

Les solutions SIEM modernes peuvent être déployées localement, dans le cloud ou dans un environnement hybride, et sont conçues pour évoluer avec l'entreprise et sa croissance. Elles incluent également des technologies telles que le SOAR pour automatiser la réponse aux menaces.

Les équipes SOC cherchent en permanence à être moins sollicitées pour être plus performantes. Elles ont donc besoin de clarté. Sans un SIEM, les analystes en sécurité doivent parcourir des millions de données hétérogènes et cloisonnées pour chaque application et source de sécurité. Pour résumer, le SIEM peut accélérer la détection et la

réponse aux cybermenaces, rendant ainsi les analystes en sécurité plus efficaces et précis lors de leurs investigations.

2. Solutions SIEM existantes:

2.1. Elastic Stack:

Elastic Stack, également connu sous le nom d'ELK Stack, est une suite d'outils open-source développée par Elastic. Elle comprend Elasticsearch, Logstash, Beats et Kibana. Elasticsearch est utilisé pour l'indexation et la recherche de données, Logstash pour l'ingestion et la transformation des logs, Beats pour la collecte des données et Kibana pour la visualisation et l'analyse des données. Elastic Stack offre une flexibilité et une extensibilité élevées, ainsi qu'une puissante capacité de recherche et d'analyse en temps réel.



Figure 7 : Elastic logo

2.2. QRadar:

QRadar est une solution SIEM développée par IBM. Elle offre une gamme complète de fonctionnalités pour la collecte, la corrélation, l'analyse et la gestion des événements de sécurité. QRadar intègre également d'autres sources de données, telles que les journaux, les flux réseau, les informations sur les menaces et les vulnérabilités. La solution utilise des algorithmes d'analyse avancés pour détecter les anomalies, les menaces potentielles et les comportements malveillants. QRadar fournit également des fonctionnalités de gestion des incidents et de génération de rapports de conformité.



Figure 8 : QRadar logo

2.3. Splunk:

Splunk est une plateforme de gestion de données qui propose des solutions pour la gestion des événements de sécurité et l'analyse des logs. Elle permet la collecte, l'indexation, la

corrélation et l'analyse en temps réel des événements de sécurité provenant de diverses sources. Splunk offre une interface conviviale et puissante pour la visualisation des données, la création de tableaux de bord personnalisés et l'extraction de renseignements exploitables. Elle prend en charge l'analyse prédictive et offre des fonctionnalités avancées pour la détection des menaces et la réponse aux incidents.



Figure 9 : Splunk logo

2.4. Wazuh:

La plateforme Wazuh offre des fonctionnalités XDR (Extended Detection and Response) et SIEM (Security Information and Event Management) pour protéger vos charges de travail dans le cloud, les conteneurs, et les serveurs. Parmi ses fonctionnalités, on trouve l'analyse des données de logs, la détection d'intrusions et de malwares, le contrôle de l'intégrité des fichiers, l'évaluation des configurations, la détection des vulnérabilités, ainsi que le support pour la conformité réglementaire.

Wazuh est basé sur la stack ELK (Elasticsearch, Logstash, Kibana), ce qui permet une collecte, une analyse, et une visualisation efficaces des données de sécurité. L'utilisation de la stack ELK permet à Wazuh de bénéficier de la robustesse et de l'évolutivité de ces outils, offrant ainsi une solution puissante et flexible pour la gestion de la sécurité de vos infrastructures.



Figure 10 : Wazuh logo

3. Étude comparative des différentes solution SIEM :

Voici une étude comparative sur les caractéristiques entre les différentes solutions SIEM :

Critères	Elastic Stack	QRadar	Splunk	Wazuh
Modèle de licences	Open-source	Propriétaire	Propriétaire	Open-source
Extensibilité	Très élevée	Élevée	Élevée	Très élevée
Collecte des logs	Elasticsearch, Logstash, Beats	Collecteurs QRadar	Collecteurs Splunk	Wazuh agents, Filebeat, syslog
Fonctionnalités avancées	Recherche, analytique, visualisation	Analyse avancée, gestion des incidents, génération de rapports	Analyse des logs, recherche, tableaux de bord	Détection des intrusions, surveillance de l'intégrité des fichiers, gestion des vulnérabilités, analyse des logs
Évolutivité	Très élevée	Élevée	Élevée	Très élevée
Prise en charge des sources de données	Large gamme de sources	Large gamme de sources	Large gamme de sources	Large gamme de sources
Analyse en temps réel	Oui	Oui	Oui	Oui
Flexibilité	Élevée	Moyenne	Élevée	Élevée
Interface utilisateur	Kibana	Console QRadar	Interface Splunk	Wazuh Dashboard (Kibana)
Communauté et support	Grande communauté open-source	Support IBM	Support Splunk	Grande communauté open-source
Coût	Gratuit (version open source) et version payante disponible	Tarification basée sur les besoins et la taille de l'infrastructure	Tarification basée sur les besoins et la taille de l'infrastructure	Gratuit (version open source) et version payante disponible
Stockage	Elastic search	Elastic search, MongoDB	Elastic search	Elasticsearch, Opensearch

Tableau 1 : Tableau comparatif SIEM, Caractéristiques

Voici une étude comparative sur le fonctionnement entre les différentes solutions SIEM :

Critères	Elastic Stack	QRadar	Splunk	Wazuh
Installation	Généralement plus complexe en raison de la configuration requise des différents composants de la pile ELK (Elasticsearch, Logstash, Beats, Kibana)	Complexité moyenne, nécessitant des connaissances techniques pour l'installation des composants QRadar et des collecteurs associés	Installation relativement simple et guidée, avec des options de déploiement sur site ou cloud	Installation relativement simple, avec des options pour une mise en place sur site ou dans le cloud
Configuration	Configuration modulaire et personnalisable à travers les différents composants de la pile ELK	Configuration avancée, nécessitant une bonne compréhension des politiques et des règles de sécurité pour optimiser les fonctionnalités de QRadar	Configuration intuitive avec des options de configuration avancées pour répondre aux besoins spécifiques	Configuration flexible et intuitive avec des options avancées pour répondre aux besoins spécifiques de l'environnement
Recherche	Puissante capacité de recherche en temps réel avec Elasticsearch, permettant des recherches complexes et des filtres avancés	Capacité de recherche avancée avec des options de recherche et de requête flexibles, y compris des recherches personnalisées basées sur des champs spécifiques	Recherche rapide et efficace avec une syntaxe de recherche robuste et des options de filtrage étendues	Capacité de recherche robuste avec des fonctionnalités avancées pour l'analyse en temps réel des données de sécurité
Tableau de bord	Utilisation de Kibana pour créer des tableaux de bord personnalisés	Interface de tableau de bord QRadar permettant de créer des tableaux de bord	Tableaux de bord personnalisables avec une interface	Utilisation de Wazuh Dashboard pour la création de tableaux de

	avec une interface conviviale et des visualisations interactives	personnalisés avec des widgets et des graphiques	conviviale et la possibilité de créer des visualisations interactives	bord personnalisés avec des visualisations interactives et une interface conviviale
--	--	--	---	---

Tableau 2 : Tableau comparatif SIEM, Fonctionnement

4. Choix de solution SIEM

Après avoir minutieusement évalué les différentes options de SIEM à travers des tableaux comparatifs détaillés, notre choix s'est arrêté sur Wazuh. En tant que seule solution SIEM open-source disponible sur le marché et reposant sur l'architecture fiable de la pile ELK, elle répond parfaitement à nos exigences spécifiques. Sa scalabilité illimitée accompagnera notre croissance organisationnelle sans contraintes. Les fonctionnalités complètes de détection d'intrusions, d'analyse de journaux et de gestion des vulnérabilités offrent une approche holistique de la sécurité, simplifiant nos opérations. De plus, la communauté open-source dynamique qui entoure Wazuh assure un soutien et des ressources précieuses pour une mise en œuvre réussie de notre projet.

IV. Wazuh :

1. Principe :

Wazuh/ELK est une solution puissante pour la gestion des logs et l'analyse de la sécurité. Il s'agit d'une combinaison de Wazuh, un logiciel de surveillance de la sécurité open-source populaire, et de l'Elastic Stack, qui est composé d'ElasticSearch, Logstash et Kibana (ELK). **Wazuh** est utilisé pour collecter, surveiller et analyser les événements de sécurité provenant de différentes sources, telles que les fichiers journaux, le trafic réseau et le registre Windows. Wazuh traite ensuite les données et les envoie à la pile Elastic Stack pour le stockage et la visualisation.

L'Elastic Stack est le cœur de l'architecture de Wazuh/ELK. Il est responsable du stockage, de l'analyse et de la visualisation des données. ElasticSearch est utilisé pour indexer et stocker les données, Logstash est utilisé pour traiter les données et Kibana est utilisé pour visualiser et analyser les données.

Wazuh/ELK fournit une plateforme centralisée pour la collecte, la surveillance et l'analyse des logs en temps réel. Il offre également des capacités d'analyse et de rapports détaillés, ce qui en fait un excellent choix pour la gestion des événements de sécurité.

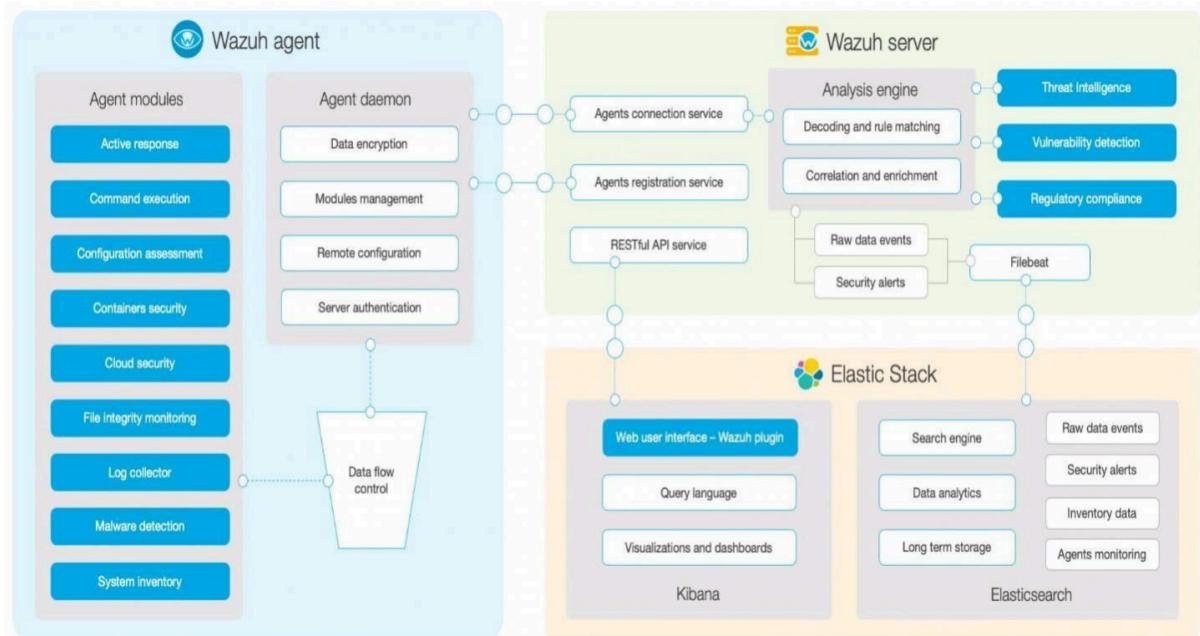


Figure 11 : Architecture de ELK/Wazuh

2. Pourquoi ELK/Wazuh :

ELK et Wazuh sont deux outils open source qui peuvent être utilisés ensemble pour la gestion des logs et la détection d'intrusion.

ELK/Wazuh offre plusieurs avantages :

- **Centralisation des logs :** ELK permet de centraliser les logs de différents systèmes et applications, ce qui facilite l'analyse et la corrélation des événements.
- **Détection d'intrusion :** Wazuh permet de détecter les menaces et les anomalies en temps réel en analysant les logs et les événements système. Wazuh utilise des règles préconfigurées pour détecter les activités suspectes.
- **Réponse aux incidents :** Wazuh fournit des outils pour la réponse aux incidents, ce qui permet de prendre des mesures rapidement pour réduire l'impact d'une intrusion.
- **Conformité réglementaire :** Wazuh peut être configuré pour répondre aux exigences réglementaires, telles que PCI DSS, HIPAA et GDPR.
- **Visualisation et analyse :** Kibana permet de visualiser et d'analyser les logs de manière efficace, ce qui facilite l'identification des tendances et des schémas.

ELK/Wazuh permet de centraliser les logs, de détecter les menaces en temps réel, de répondre aux incidents rapidement, de se conformer aux exigences réglementaires et de visualiser et d'analyser les logs efficacement.

Le serveur et l'indexeur (ELK stack) sont généralement installés sur un seul serveur autonome. L'architecture de Wazuh est donc divisée en deux parties : les agents d'extrémité et les composants centraux.

3. Fonctionnement de Wazuh :

WAZUH solution est basé sur l'agent Wazuh, qui est déployé sur les monitored endpoints, et sur trois composants centraux : le serveur Wazuh, le Wazuh Indexer et le Wazuh Dashboard.

Le Wazuh Agent est un logiciel de surveillance de la sécurité open source qui permet de surveiller les journaux, les fichiers et le trafic. Il aide à la détection des menaces, à la conformité et à la réponse aux incidents. Le Wazuh Agent permet de collecter et d'analyser les données provenant des terminaux de votre réseau.

Le Wazuh serveur analyse les données reçues des agents. Il les traite par le biais de décodeurs et de règles, en utilisant les renseignements sur les menaces pour rechercher les well-known indicateurs de compromission (IOC).

Le Wazuh Indexer est un composant de la plate-forme Wazuh qui est responsable du stockage et de l'indexation des journaux. Le moteur d'indexation stocke les données dans un index Elasticsearch pour une analyse ultérieure. En utilisant le moteur d'indexation, vous pouvez rechercher et analyser les données provenant d'une ou de plusieurs sources.

Le Wazuh Dashboard est une interface web qui vous permet de surveiller et d'analyser les incidents de sécurité en temps réel. Il fournit une vue graphique des données collectées par la plateforme Wazuh. Le Wazuh Dashboard offre une vision complète de l'état de sécurité de votre environnement, détecte les incidents de sécurité et vous permet d'analyser et de répondre rapidement aux menaces .

4. Architecture de Déploiement de Wazuh :

Le schéma ci-dessous représente une architecture de déploiement de Wazuh. Il montre les composants de la solution et comment le serveur Wazuh et Wazuh indexer nodes peuvent être configurés en clusters, fournissant un load balancing et high Availability.

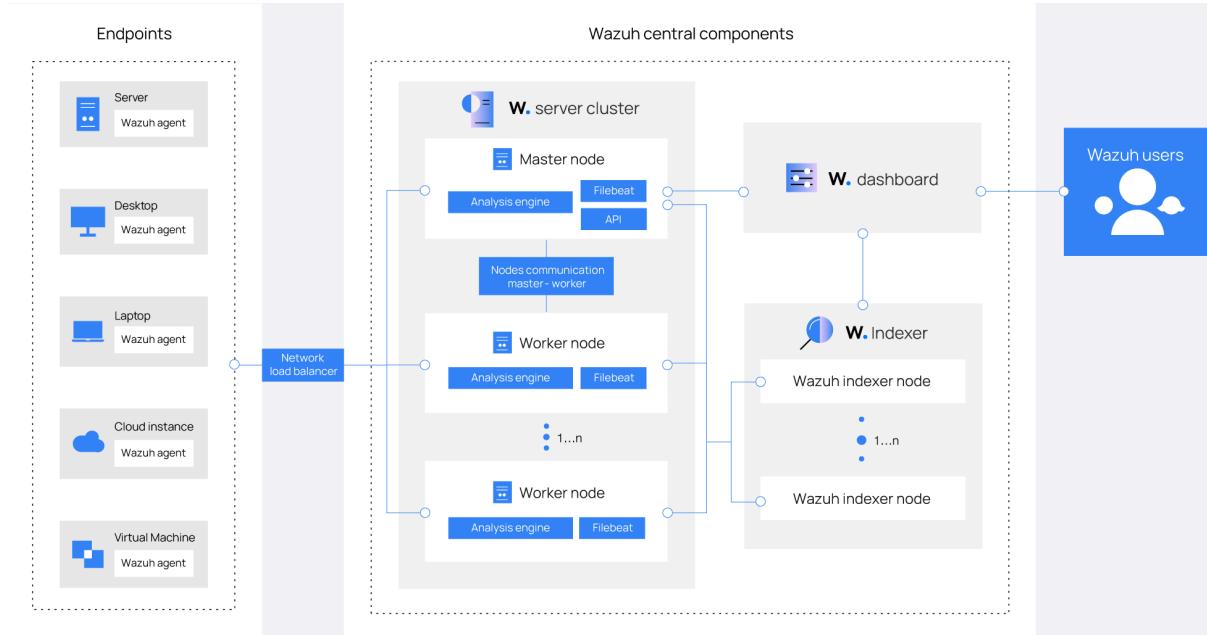


Figure 12 : architecture de Déploiement de Wazuh

Filebeat : Il est utilisé pour envoyer des événements et des alertes à l'indexeur Wazuh. Il lit la sortie du moteur d'analyse de Wazuh et envoie les événements en temps réel. Il assure également la répartition de charge lorsqu'il est connecté à un cluster d'indexeurs Wazuh multi-nœuds.

Partie 2: SOAR

I. Introduction

SOAR est une approche stratégique qui combine l'orchestration des processus de sécurité, l'automatisation des tâches et la réponse aux incidents, afin d'améliorer la gestion des alertes de sécurité. Au cours de ce chapitre, nous allons explorer en détail le fonctionnement de SOAR et examiner comment cette technologie peut nous aider à optimiser notre processus d'analyse des alertes de sécurité. Nous discuterons des avantages de SOAR, une analyse comparative des différentes solutions de SOAR, ainsi que la partie d'installation et de configuration de notre solution qu'on va choisir.

II. Introduction

1. Définition de Security Orchestration, Automation and Response :

La Security Orchestration, Automation and Response (SOAR) est une approche intégrée pour la gestion des incidents de sécurité et des opérations de sécurité. Elle combine les capacités d'orchestration, d'automatisation et de réponse pour aider les organisations à améliorer leur posture de sécurité, à réduire les temps de réponse aux incidents et à optimiser l'efficacité de leurs équipes de sécurité. Voici une définition détaillée de chaque composant de la SOAR:

- **Orchestration** : L'orchestration dans le contexte de la sécurité fait référence à la coordination et à la gestion des processus et des tâches de sécurité au sein de l'environnement informatique. Elle permet d'automatiser et de synchroniser les actions entre différentes solutions de sécurité, systèmes et équipes de sécurité. L'orchestration aide à rationaliser et à simplifier les workflows de sécurité, permettant une meilleure collaboration entre les équipes et une gestion plus efficace des incidents.
- **Automation** : L'automatisation est le processus d'exécution de tâches de sécurité de manière autonome, sans intervention humaine directe. Cela peut inclure des actions telles que la collecte d'informations, l'analyse de données, la vérification d'indicateurs de compromission, la suppression de menaces, la mise à jour des règles de sécurité, etc. L'automatisation permet d'accélérer les processus de sécurité, de réduire les erreurs humaines et de libérer les analystes de sécurité de tâches répétitives et de faible valeur ajoutée.
- **Response** : Il fait référence aux mesures prises pour gérer et résoudre les incidents de sécurité. Cela comprend l'identification, la classification, l'investigation, la réponse initiale et la remédiation des incidents. La SOAR facilite la gestion des incidents en fournissant des outils et des workflows préconfigurés, en intégrant des sources de renseignements sur les menaces, en automatisant les tâches de réponse et en fournissant une visibilité et des rapports sur les activités de réponse.



Figure 13 : SOAR overview

2. Les avantages de SOAR :

2.1. Amélioration de l'efficacité opérationnelle:

SOAR permet d'automatiser les tâches répétitives et manuelles, ce qui permet aux équipes de sécurité de gagner du temps et de se concentrer sur des activités à plus forte valeur ajoutée. L'automatisation réduit également les risques d'erreurs humaines et garantit une exécution cohérente des processus de sécurité.

2.2. Accélération de la détection et de la réponse aux incidents :

Grâce à l'orchestration et à l'automatisation, SOAR permet de détecter et de répondre plus rapidement aux incidents de sécurité. Les alertes sont gérées de manière plus efficace, les analyses sont automatisées, les décisions sont prises plus rapidement et les mesures correctives sont appliquées en temps réel.

2.3. Intégration des outils de sécurité :

SOAR permet d'intégrer et de centraliser les différents outils de sécurité utilisés au sein d'une organisation, tels que les systèmes SIEM (Security Information and Event Management), les solutions de gestion des vulnérabilités, les plates-formes de Threat Intelligence, etc. Cela permet une meilleure collaboration entre les équipes, une visibilité accrue et une meilleure corrélation des informations de sécurité.

2.4. Renforcement de la traçabilité et de la conformité :

SOAR offre une traçabilité complète des activités de sécurité, y compris des actions effectuées, des décisions prises et des mesures prises pour résoudre les incidents. Cela facilite l'analyse post-incident, l'audit de conformité et la génération de rapports.

2.5. Optimisation des ressources humaines :

SOAR permet de faire plus avec moins en optimisant l'utilisation des ressources humaines. Les tâches manuelles sont automatisées, les processus sont rationalisés et les équipes peuvent traiter un plus grand volume d'incidents avec une efficacité accrue.

2.6. Amélioration de la collaboration et de la communication :

SOAR facilite la collaboration entre les équipes du SOC et les autres parties prenantes, en fournissant une plateforme centralisée pour partager des informations, des connaissances et des actions. Cela favorise une meilleure communication et une meilleure coordination entre les équipes, ce qui est essentiel pour une réponse efficace aux incidents.

3. Analyse comparative de SOAR:

3.1. TheHive Project:

TheHive est une plateforme SOAR open source largement utilisée. Elle permet aux équipes de sécurité de centraliser et de gérer les alertes de sécurité provenant de différentes sources. TheHive facilite la collaboration entre les analystes, automatise les tâches répétitives et permet de suivre les investigations.



Figure 14 : TheHive Logo

3.2. Demisto:

Demisto, récemment acquis par Palo Alto Networks et renommé Cortex XSOAR, est une plateforme SOAR qui permet de centraliser, orchestrer et automatiser la réponse aux

incidents de sécurité. Elle intègre des fonctions de gestion des incidents, de collecte d'informations, d'automatisation des réponses et de collaboration entre équipes.



Figure 15 : Demisto Logo

3.3. **Swimlane:**

Swimlane est une autre solution SOAR populaire qui offre des fonctionnalités de gestion des incidents, d'automatisation des tâches de sécurité et de collaboration. Elle permet aux équipes de sécurité de créer des workflows personnalisés, d'automatiser les tâches répétitives et de suivre les progrès de manière centralisée.



Figure 16 : Swimlane Logo

4. Choix de solution

Après une analyse comparative approfondie des différentes solutions SOAR disponibles, nous avons choisi TheHive Project comme plateforme principale pour renforcer notre gestion de la sécurité. TheHive est une solution SOAR open source largement adoptée qui répond à nos besoins spécifiques. Elle offre une fonctionnalité puissante pour centraliser et gérer les alertes de sécurité provenant de diverses sources, ce qui nous permet d'avoir une vue d'ensemble de notre environnement de sécurité. La plateforme facilite la collaboration entre nos analystes en offrant des fonctionnalités de partage d'informations et de suivi des enquêtes. De plus, TheHive automatise les tâches répétitives, ce qui permet à notre équipe de se concentrer sur des activités à plus forte valeur ajoutée. Avec TheHive Project, nous sommes convaincus de pouvoir améliorer notre efficacité opérationnelle, accélérer la détection et la réponse aux incidents, et renforcer globalement notre posture de sécurité.

III. The Hive

1. Définition:

The Hive est une plateforme qui facilite la gestion et la résolution des incidents de sécurité. Il facilite la collecte, l'analyse et la réponse aux alertes de sécurité provenant de différentes sources. TheHive fournit des fonctionnalités pour la hiérarchisation des alertes, la collaboration des membres lors d'incidents, la création de cas d'incidents, le suivi des enquêtes et le signalement des incidents. Il facilite également l'intégration avec d'autres outils de sécurité pour automatiser les tâches et les réponses. Parmi ces fonctionnalités :

2. Les fonctionnalités de TheHive:

2.1. Gestion des incidents:

- **Création de cas d'incident** : TheHive vous permet de créer et de gérer des cas d'incident pour regrouper les alertes de sécurité liées à un même incident.
- **Affectation et suivi** : les cas d'incident peuvent être affectés aux membres de l'équipe pour faciliter le suivi et la responsabilisation.
- **Classification et étiquetage** : les événements peuvent être classés et étiquetés pour une meilleure organisation et une recherche plus facile.

2.2. Triage des alertes:

- **Consolidation des alertes** : TheHive centralise les alertes provenant de différentes sources de sécurité telles que les systèmes de détection d'intrusion, les outils de surveillance du réseau, etc.
- **Filtrage et hiérarchisation** : les alertes peuvent être filtrées et triées en fonction de leur gravité et de leur pertinence, ce qui permet aux équipes de se concentrer d'abord sur les problèmes les plus critiques.

2.3. Collaboration et communication

- **Collaboration d'équipe** : les membres de l'équipe de sécurité peuvent travailler ensemble sur des cas d'incident, partager des informations, des notes et des commentaires, favorisant ainsi la collaboration et la cohésion.
- **Journal d'activité** : TheHive enregistre toutes les actions et modifications dans un cas d'événement, permettant de suivre l'historique et de suivre l'activité passée.

2.4. Automatisation et orchestration

- **Intégration avec des outils externes** : TheHive peut être intégré à d'autres outils de sécurité pour automatiser les tâches et les réponses. Par exemple, l'intégration avec Cortex permet une automatisation plus poussée.
- **Flux de travail personnalisés** : TheHive facilite la coordination des réponses en permettant de définir des flux de travail personnalisés pour coordonner les actions prises en réponse aux alertes de sécurité.

2.5. Enrichissement des données:

- **Intégration d'outils riches** : TheHive peut se connecter à des outils riches en données tels que des scanners de fichiers malveillants, des services de réputation de domaine ou des bases de données d'adresses IP suspectes.
- **Collecte d'informations supplémentaires** : des informations supplémentaires provenant d'outils riches sont automatiquement ajoutées aux alertes, offrant une meilleure visibilité et une analyse approfondie.

2.6. Génération de rapports :

- **Tableaux de bord et visualisations** : TheHive fournit des fonctionnalités permettant de créer des tableaux de bord personnalisés et des visualisations graphiques afin de présenter les données de sécurité de manière claire et concise.
- **Rapport d'incident** : TheHive offre la possibilité de générer des rapports de cas d'incident détaillés, y compris les mesures prises, les conclusions et les recommandations de réponse.

3. Architecture de TheHive:

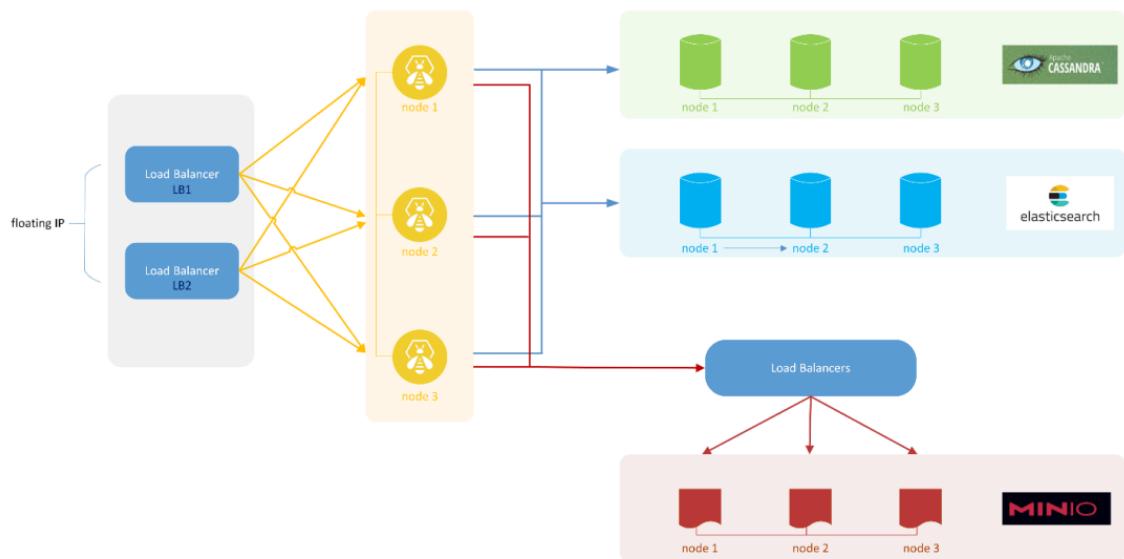


Figure 17 : TheHive architecture

IV. Cortex :

1. Définition:

Cortex est un logiciel gratuit qui facilite la réponse automatisée et collaborative aux incidents. Il fonctionne comme une plateforme pour les activités liées à la sécurité. Cortex collabore avec plusieurs outils de sécurité, pour permettre l'enrichissement et l'analyse automatisés des données de sécurité. Il permet aux utilisateurs de créer et d'exécuter une série de tâches analytiques, telles que l'exécution d'analyses antivirus sur les données de sécurité reçues du MISP ou d'une autre source, ou l'examen de la réputation du domaine sur les données de sécurité. Les résultats de ces enquêtes peuvent être partagés et comparés entre plusieurs disciplines, ce qui augmente la capacité globale de l'organisation en matière de collecte de renseignements.

2. Les fonctionnalités de Cortex:

2.1. Orchestration des analyses de sécurité :

Cortex coordonne et automatise l'exécution des analyses de sécurité sur les alertes ou les indicateurs de compromission (IOC). Il dispose d'une interface conviviale qui facilite la création de processus personnalisés qui spécifient les étapes et les actions nécessaires à l'analyse d'une alerte.

2.2. Intégration avec des outils d'analyse :

Cortex peut être combiné avec des outils d'analyse de sécurité tels que des analyseurs de fichiers malveillants, des outils de réputation de domaine ou d'adresse IP, des outils de détection d'intrusion, des outils de déchiffrement de protocole réseau, etc. Cette combinaison automatise et étend l'analyse des alertes de sécurité.

2.3. Analyses et enquêtes automatisées:

À l'aide de Cortex, vous pouvez définir des analyses et des enquêtes automatisées pour les alertes de sécurité. Cela signifie que certaines tâches peuvent être effectuées automatiquement sans intervention humaine, ce qui contribue à accélérer le processus de réponse aux incidents.

2.4. Enrichissement des alertes:

Cortex peut facilement enrichir les alertes en récupérant des informations supplémentaires à partir de sources externes. Par exemple, il peut interroger une base de données de réputation pour obtenir des informations sur un nom de domaine ou une adresse IP, ou un service de géolocalisation pour obtenir des données sur l'emplacement géographique d'une adresse IP.

2.5. Gestion des résultats et actions :

Une fois l'analyse effectuée, Cortex fournit des résultats et des informations détaillées sur les alertes. Il permet également de définir des actions à entreprendre en réponse à une alerte, telles que le blocage d'une adresse IP, la mise en quarantaine d'un fichier suspect, l'envoi d'une alerte ou la génération d'un rapport.

2.6. Extensibilité:

Cortex est extensible et permet l'ajout de nouvelles fonctionnalités et l'incorporation de composants personnalisés. Vous pouvez créer des analyseurs personnalisés prenant en charge des outils spécifiques ou créer des actions personnalisées adaptées aux exigences spécifiques de votre environnement de sécurité.

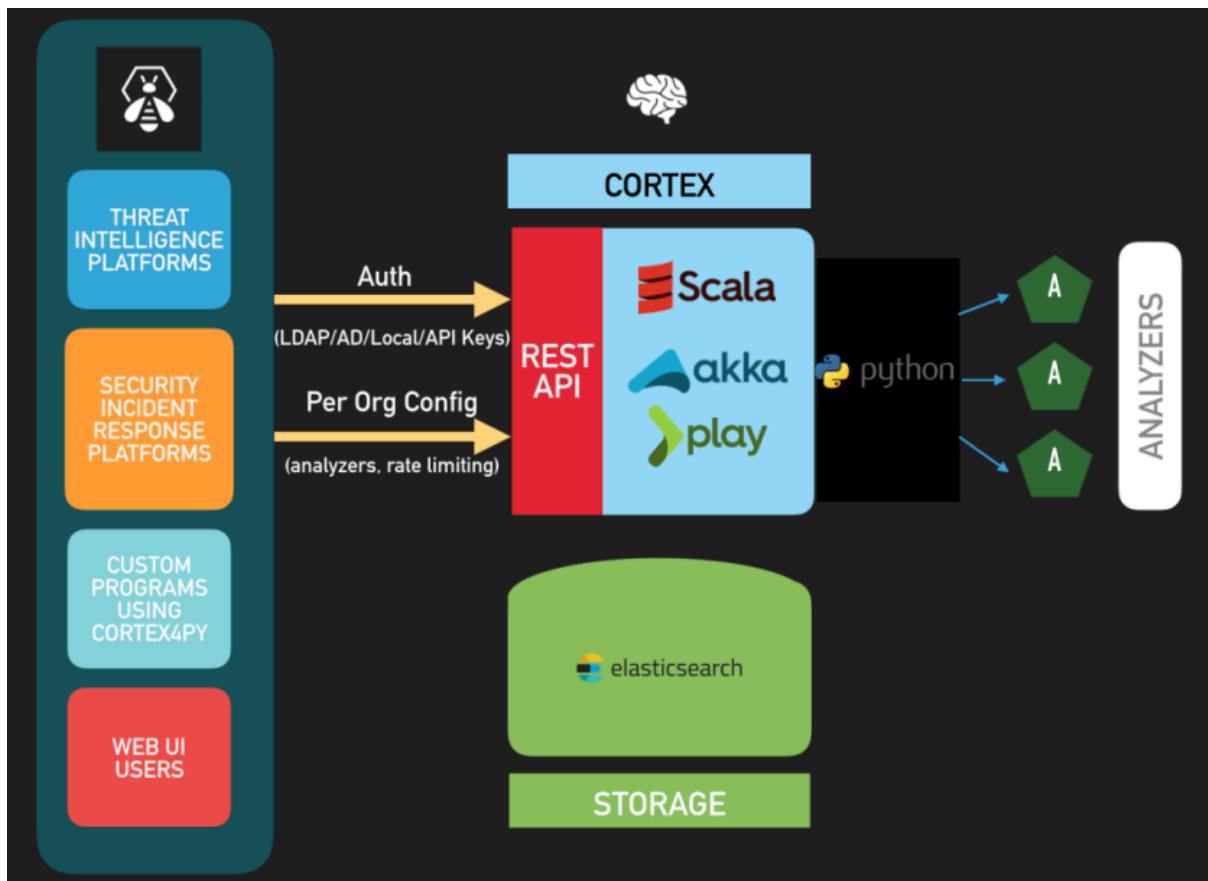


Figure 18 : Architecture de Cortex

V. MISP :

1. Définition de MISP:

MISP (Malware Information Sharing Platform) est une plateforme qui facilite la collaboration et l'échange d'informations sur les menaces liées aux logiciels malveillants entre les organisations et les équipes de sécurité. Il facilite la collecte, l'agrégation, l'analyse et le partage sécurisé des menaces, ce qui prend en charge la détection précoce des attaques, l'identification des individus malveillants et la réponse rapide aux incidents de sécurité. MISP dispose de fonctionnalités avancées telles que la classification, la corrélation, l'ingénierie inverse et l'intégration avec d'autres outils de sécurité. Le secret des informations partagées est considéré, par conséquent, les utilisateurs ont la possibilité de réglementer l'accès aux informations personnelles sensibles. En combinant l'expertise de la communauté de la sécurité, MISP augmente la sécurité globale de l'écosystème et prévient les cyberattaques.

2. Fonctionnalités de MISP:

2.1. Partage d'informations sur les menaces :

MISP est une plateforme conçue spécifiquement pour le partage d'informations sur les menaces entre les organisations et les équipes de sécurité. Il permet aux utilisateurs de partager des indicateurs de compromission (IOC) tels que des adresses IP malveillantes, des noms de domaine suspects, des signatures de logiciels malveillants, des schémas de comportement, etc.

2.2. Collecte et agrégation des données :

MISP permet de collecter et d'agréger des données provenant de différentes sources, telles que des rapports de sécurité, des listes de réputation, des analyses de logiciels malveillants, des journaux d'événements, etc. Cela permet aux utilisateurs d'avoir une vue d'ensemble des menaces et de bénéficier de sources multiples pour enrichir les informations sur les indicateurs de compromission.

2.3. Classification:

MISP offre une classification flexible pour organiser et catégoriser les indicateurs de compromission. Il utilise des taxonomies standard telles que ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) pour faciliter l'analyse et la recherche des informations sur les menaces.

2.4. Analyse et corrélation :

MISP propose des fonctionnalités d'analyse et de corrélation pour identifier les liens entre différents indicateurs de compromission et les attribuer à des campagnes de menaces spécifiques. Cela permet de détecter les schémas d'attaque, d'identifier les acteurs malveillants et de mieux comprendre les tactiques et les techniques utilisées.

2.5. Recherche et recherche inversée:

MISP facilite la recherche d'informations sur les menaces en offrant des fonctionnalités de recherche avancée, y compris la recherche inversée. Les utilisateurs peuvent rechercher des indicateurs de compromission spécifiques, des campagnes de menaces, des acteurs malveillants, des rapports de sécurité, etc.

2.6. Notifications et abonnements:

MISP permet aux utilisateurs de définir des abonnements pour recevoir des notifications lorsqu'il y a des mises à jour ou des nouveaux indicateurs de compromission pertinents. Cela garantit que les utilisateurs restent informés des dernières menaces et des développements dans leur domaine d'intérêt.

2.7. Intégration avec d'autres outils de sécurité:

MISP offre des fonctionnalités d'intégration avec d'autres outils et services de sécurité, tels que des outils d'analyse de logiciels malveillants, des passerelles de messagerie, des systèmes de détection d'intrusion, etc. Cela permet d'enrichir les informations sur les menaces et de faciliter la corrélation des données.

2.8. Confidentialité et contrôles d'accès:

MISP prend en compte les préoccupations liées à la confidentialité et permet aux organisations de contrôler l'accès aux informations partagées. Les utilisateurs peuvent définir des niveaux de confidentialité pour les événements et les indicateurs de compromission, ce qui garantit que seules les parties autorisées ont accès aux informations sensibles.



Figure 19 : Architecture de Misp

VI. TheHive, Cortex et MISP:

TheHive, Cortex et MISP sont trois produits open source et gratuits qui peuvent grandement vous aider à lutter contre les menaces et vous permet d'enquêter rapidement sur les incidents de sécurité de manière collaborative. Plusieurs analystes peuvent travailler simultanément sur des tâches et des cas. Alors que les cas peuvent être créés à partir de zéro, TheHive peut recevoir des alertes de différentes sources grâce à des flux d'alertes qui consomment les événements de sécurité générés par plusieurs sources et les alimentent dans la Ruche à l'aide de la bibliothèque Python Hive4py. La ruche peut également se synchroniser avec une ou plusieurs instances MISP pour recevoir des événements nouveaux et mis à jour qui apparaîtront dans le volet d'alerte avec toutes les autres alertes générées par d'autres sources. Les analystes peuvent ensuite prévisualiser les nouvelles alertes pour

décider si elles doivent être suivies d'effet. Si c'est le cas, ils peuvent les transformer en cas d'enquête à l'aide de modèles.

Pour analyser les observables collectés au cours d'une enquête et/ou importés à partir d'un événement MISP, TheHive peut s'appuyer sur un ou plusieurs moteurs d'analyse Cortex.

Cortex est un autre produit autonome que nous avons développé dont le seul but est de vous permettre d'analyser les observables à grande échelle grâce à son grand nombre d'analyseurs, de modules d'extension MISP et de tout analyseur que vous auriez pu développer sur le côté. Cortex dispose d'une API REST qui peut être utilisée pour habiliter d'autres produits de sécurité tels que des logiciels d'analyse, des SIRP alternatifs ou des MISP.

Partie 3: Autres outils utilisés (IDS, Sandbox)

I. Graylog :

Graylog is a centralized Log Management System (LMS) that allows you to aggregate, organize, and make sense of data from various sources such as devices, applications, and operating systems. It is designed specifically for log management, with an architecture that efficiently processes, indexes, and provides access to log data. Graylog's core features include streams for categorizing and routing messages, a search interface for querying logs, dashboards for visualizing data, alerts for monitoring conditions, and content packs for streamlining setup. It uses Elasticsearch or OpenSearch as the data node for indexing and searching log data, leveraging their full-text search capabilities to conduct in-depth analysis of petabytes of log events. MongoDB is used to store metadata like user information, stream configurations, and other settings, providing a scalable and flexible database solution.

Graylog introduces the Graylog Extended Log Format (GELF) which improves upon limitations of standard syslog formats. The Graylog Server acts as the central management interface, building an abstraction layer on top of the data node and MongoDB to simplify data access and configuration. With a strong community of over 8,000 members and a marketplace for plugins, extensions, and content packs contributed by developers, Graylog provides a powerful and flexible solution for managing and deriving insights from large volumes of log data across an organization.

Il'est aussi utilisé pour visualiser les logs comme kibana et wazuh Dashboard



Figure 20 : graylog logo

II. Suricata:

Suricata est un moteur de détection open source qui peut agir comme un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS). Il a été développé par l'Open Information Security Foundation (OSIF) et est un outil gratuit utilisé par les entreprises, petites et grandes. Le système utilise un ensemble de règles et un langage de signature pour détecter et prévenir les menaces. Le Suricata est compatible avec Windows, Mac, Unix et Linux.



Figure 21 : Suricata Logo

1. Avantages de Suricata :

- **Archivage:** Suricata permet l'archivage complet des logs de réseau et des événements de sécurité. Cette fonctionnalité est cruciale pour l'audit, l'analyse post-incident et la conformité aux régulations.

- **Gestion commerciale:** Suricata peut être utilisé dans des environnements commerciaux pour améliorer la sécurité réseau, surveiller les activités malveillantes et protéger les données sensibles des entreprises.
- **Accessibilité 24-7:** Suricata offre une surveillance continue et en temps réel du réseau, assurant une détection et une réponse immédiates aux menaces potentielles, 24 heures sur 24 et 7 jours sur 7.
- **Import – Export des données:** Suricata facilite l'importation et l'exportation de données, permettant une intégration fluide avec d'autres outils de sécurité et plateformes d'analyse, tels que Wazuh et TheHive.
- **Historique:** Suricata maintient un historique détaillé des événements de sécurité, aidant à identifier des tendances, des modèles et des attaques récurrentes pour renforcer les défenses de sécurité à long terme.
- **Extranet:** La capacité de Suricata à surveiller les activités sur les réseaux extranet permet de sécuriser les communications et les transactions inter-entreprises, protégeant ainsi les échanges de données sensibles avec les partenaires externes.

2. Les principales fonctionnalités

- **IDS/IPS (Intrusion Detection System/Intrusion Prevention System):** Suricata fonctionne à la fois comme un IDS et un IPS, fournissant des capacités robustes de détection et de prévention des intrusions pour sécuriser les réseaux contre les menaces.
- **Performances Élevées:** Grâce au multi-threading et à l'utilisation des GPU, Suricata offre des performances élevées, permettant une analyse rapide et efficace des données réseau.
- **Détection Automatique de Protocole:** Suricata supporte une détection automatique des protocoles tels que IPv4/6, TCP, UDP, ICMP, HTTP, TLS, FTP,

SMB, et DNS, ce qui permet une analyse approfondie et précise du trafic réseau.

- **Network Security Monitoring (NSM):** Suricata fournit des fonctionnalités NSM, telles que la journalisation DNS, le module de journalisation HTTP, l'enregistrement des certificats et l'extraction de fichiers, ainsi que la vérification de la somme de contrôle MD5.
- **Librairie HTP Indépendante:** La librairie HTP indépendante de Suricata permet une analyse HTTP avancée et flexible, essentielle pour la détection des menaces basées sur le web.
- **Formats de Sortie Variés:** Suricata supporte de nombreux formats de sortie, y compris Unified2, JSON, et Prelude, facilitant l'intégration avec divers systèmes de gestion et d'analyse de la sécurité.

3. Fonctionnement :

L'outil analyse le trafic sur une ou plusieurs interfaces réseaux en fonction de règles activées. Il génère, par défaut, un fichier JSON qui peut être utilisé par les solutions de type Extract Transform-load comme logstash (utilisé avec Elasticsearch).

III. Cloudblab:

CloudLab est une plateforme avancée de cloud computing dédiée à la recherche, offrant aux scientifiques un contrôle et une visibilité sans précédent jusqu'au niveau du matériel physique. Elle permet de provisionner rapidement des environnements cloud complets en quelques minutes, avec une isolation stricte entre les différentes tranches d'utilisateurs pour des expérimentations sans artefacts avec de nouvelles architectures cloud. Les chercheurs peuvent exécuter des stacks cloud standard comme OpenStack et Kubernetes, ou créer des solutions personnalisées de A à Z sur les presque 1 000 machines physiques de CloudLab, réparties sur trois sites aux États-Unis et interconnectées via Internet2. Construite sur les technologies familières d'Emulab et de GENI, CloudLab offre une interface cohérente et se

fédère avec les bancs d'essai existants dans le monde entier, permettant aux chercheurs d'innover et d'expérimenter avec les architectures, technologies et applications de cloud computing à grande échelle avec un contrôle total de la stack.



Figure 22 : CloudLab Logo

IV. Docker:

Docker est une plateforme logicielle open-source qui permet de développer, tester, déployer et exécuter des applications de manière isolée grâce à la technologie des conteneurs. Les conteneurs sont des unités standardisées de logiciel qui emballent le code et toutes ses dépendances pour que l'application puisse s'exécuter de manière rapide et fiable d'un environnement informatique à un autre.

Principales Caractéristiques de Docker :

- **Isolation des Applications** :Chaque conteneur fonctionne en isolation, garantissant que les applications n'interfèrent pas les unes avec les autres, ce qui améliore la sécurité et la stabilité.
- **Portabilité** :Les conteneurs Docker peuvent être exécutés de manière cohérente sur n'importe quel système d'exploitation prenant en charge Docker, qu'il s'agisse d'un poste de développeur, d'un centre de données sur site ou d'un fournisseur de cloud public.
- **Léger et Rapide** :Contrairement aux machines virtuelles, les conteneurs partagent le noyau du système d'exploitation de l'hôte, ce qui les rend beaucoup plus légers et rapides à démarrer.

- **Gestion des Dépendances** :Docker assure que les applications sont emballées avec toutes leurs dépendances, réduisant les problèmes de compatibilité et les conflits entre les environnements de développement, de test et de production.
- **Déploiement Simplifié** :Grâce à des fichiers de configuration appelés Dockerfiles, les développeurs peuvent définir les étapes nécessaires pour assembler une image Docker, simplifiant le processus de déploiement et de mise à jour des applications.
- **Ecosystème et Outils** :Docker Hub, un registre public de Docker, permet de partager et de distribuer des images Docker. D'autres outils comme Docker Compose et Docker Swarm facilitent la gestion des applications multi conteneurs et le déploiement de clusters de conteneurs.

Avantages de l'Utilisation de Docker :

- **Efficacité Ressources** :Utilise moins de ressources système comparé aux machines virtuelles, ce qui permet une meilleure utilisation de l'infrastructure matérielle.
- **Rapidité de Déploiement** :Les applications conteneurisées peuvent être déployées rapidement et efficacement, ce qui accélère le cycle de développement et de livraison.
- **Consistance des Environnements** :Assure que l'application fonctionne de manière cohérente dans les environnements de développement, de test et de production.
- **Scalabilité** :Facilement scalable horizontalement en ajoutant plus de conteneurs selon les besoins de l'application.



Figure 23 : Docker Logo

Conception de l'architecture du projet

Après avoir identifié le choix de nos outils, cette partie sera principalement dédiée pour présenter l'architecture fonctionnelle de la solution proposée, en montrant les différentes interactions entre les outils et technologies, ainsi que les actions effectuées entre eux.

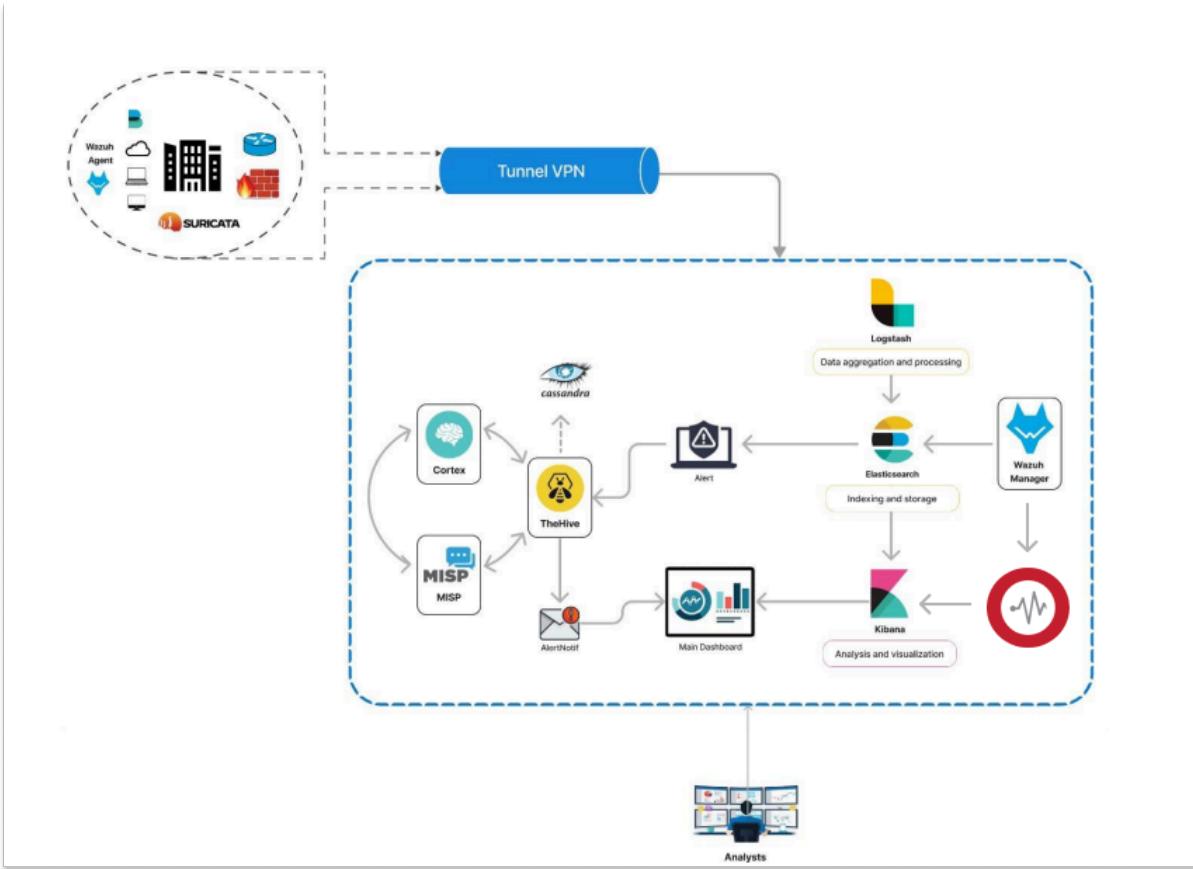


Figure 24 : Architecture

Chapitre 4 : IMPLEMENTATION DE LA SOLUTION ET PREUVE DE CONCEPT (POC)

I. Introduction :

Dans cette dernière section, nous détaillerons la mise en œuvre de notre solution pour résoudre le problème identifié. Nous présenterons les configurations et intégrations des outils mentionnés précédemment. De plus, nous partagerons les résultats des différentes études de cas menées pour tester l'efficacité de notre approche. Enfin, nous discuterons des prochaines étapes à suivre pour améliorer et affiner davantage notre solution, en tenant compte des enseignements tirés de notre proof of concept (POC).

II. Description de l'environnement de travail :

Notre environnement de travail est constitué de 3 machines sur le cloud dans la plateforme "[cloudlab.us](#)" voici leurs caractéristiques

IP	RÔLE	OS	CPU	MEMORY
	Wazuh server - indexer - dashboard	Ubuntu 22.04		
	Wazuh Agent	Ubuntu 22.04		
	theHive-Cortex	Ubuntu 22.04		

Tableau 3. Description de l'environnement

III. Déploiement All-in-one :

Le serveur Wazuh et Elastic Stack sont installés sur le même hôte. Ce type de déploiement est approprié pour les tests et les petits environnements de travail.

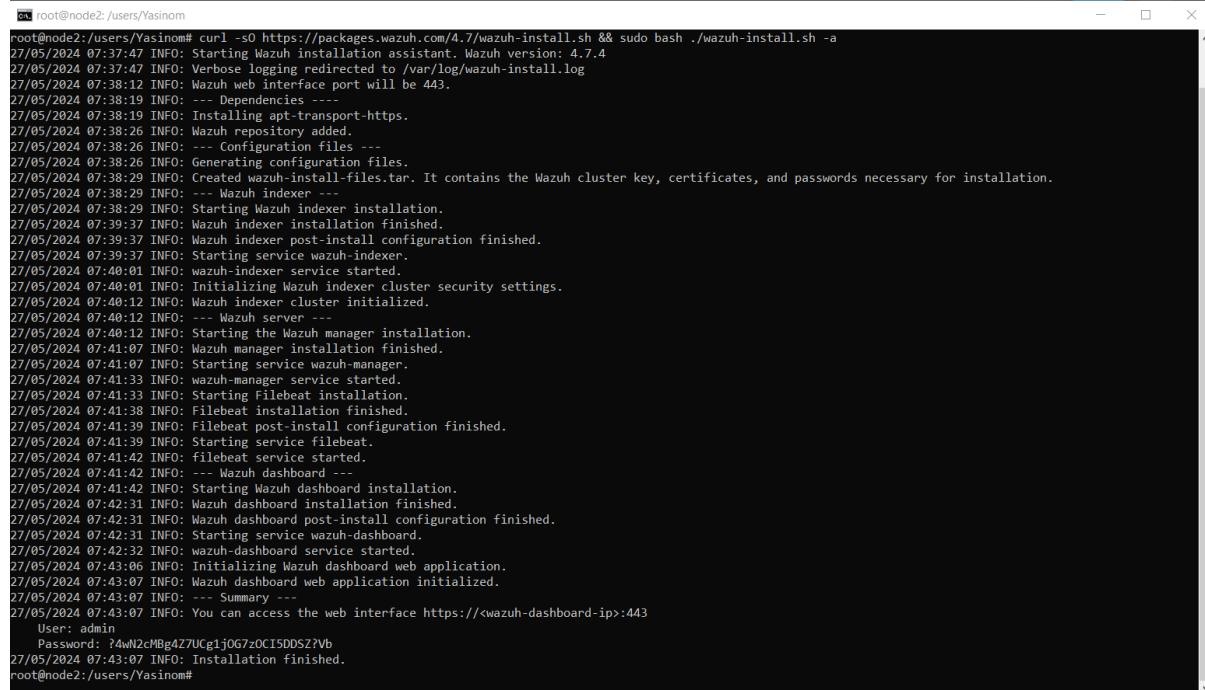
Les composants suivants seront installés :

- Le serveur **Wazuh**, y compris le gestionnaire **Wazuh** en tant que cluster à nœud unique, et Filebeat.
- Elastic Stack, y compris Elasticsearch en tant que cluster à nœud unique, et Kibana, y compris le plugin Wazuh Kibana.

Une fois l'installation faite on peut accéder à l' interface Wazuh via **https://** et en entrant nos données d' authentifications.

On utilise la commande suivante pour **installer** le tout:

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash  
.wazuh-install.sh -a
```



The terminal window shows the command being run and the resulting log output. The log details the installation process from version 4.7.4, through configuration file generation, indexer and manager installations, and finally the dashboard web application. It ends with a password prompt and a confirmation of successful installation.

```
ca root@node2:/users/Yasinom# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a  
27/05/2024 07:37:47 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.4  
27/05/2024 07:37:47 INFO: Verbose logging redirected to /var/log/wazuh-install.log  
27/05/2024 07:38:12 INFO: Wazuh web interface port will be 443.  
27/05/2024 07:38:19 INFO: --- Dependencies ---  
27/05/2024 07:38:19 INFO: Installing apt-transport-https.  
27/05/2024 07:38:26 INFO: Wazuh repository added.  
27/05/2024 07:38:26 INFO: --- Configuration files ---  
27/05/2024 07:38:26 INFO: Generating configuration files.  
27/05/2024 07:38:29 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.  
27/05/2024 07:38:29 INFO: --- Wazuh indexer ---  
27/05/2024 07:38:29 INFO: Starting Wazuh indexer installation.  
27/05/2024 07:39:37 INFO: Wazuh indexer installation finished.  
27/05/2024 07:39:37 INFO: Wazuh indexer post-install configuration finished.  
27/05/2024 07:39:37 INFO: Starting service wazuh-indexer.  
27/05/2024 07:40:01 INFO: wazuh-indexer service started.  
27/05/2024 07:40:01 INFO: Initializing Wazuh indexer cluster security settings.  
27/05/2024 07:40:12 INFO: Wazuh indexer cluster initialized.  
27/05/2024 07:40:12 INFO: --- Wazuh server ---  
27/05/2024 07:40:12 INFO: Starting the Wazuh manager installation.  
27/05/2024 07:41:07 INFO: Wazuh manager installation finished.  
27/05/2024 07:41:07 INFO: Starting service wazuh-manager.  
27/05/2024 07:41:33 INFO: wazuh-manager service started.  
27/05/2024 07:41:33 INFO: Starting Filebeat installation.  
27/05/2024 07:41:38 INFO: Filebeat installation finished.  
27/05/2024 07:41:38 INFO: Filebeat post-install configuration finished.  
27/05/2024 07:41:38 INFO: Starting service filebeat.  
27/05/2024 07:41:42 INFO: filebeat service started.  
27/05/2024 07:41:42 INFO: --- Wazuh dashboard ---  
27/05/2024 07:41:42 INFO: Starting Wazuh dashboard installation.  
27/05/2024 07:42:31 INFO: Wazuh dashboard installation finished.  
27/05/2024 07:42:31 INFO: Wazuh dashboard post-install configuration finished.  
27/05/2024 07:42:31 INFO: Starting service wazuh-dashboard.  
27/05/2024 07:42:32 INFO: wazuh-dashboard service started.  
27/05/2024 07:43:06 INFO: Initializing Wazuh dashboard web application.  
27/05/2024 07:43:07 INFO: Wazuh dashboard web application initialized.  
27/05/2024 07:43:07 INFO: --- Summary ---  
27/05/2024 07:43:07 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443  
User: admin  
Password: ?4wN2cMBg4Z7UCg1j0G7zOC15DD5Z?Vb  
27/05/2024 07:43:07 INFO: Installation finished.  
root@node2:/users/Yasinom#
```

Figure 25 : Déploiement All-in-one

À la fin de l'installation, on aura les coordonnées d'authentification sur l'interface web.

Ensuite on ajoute notre hostname sur **/etc/hosts**:

```
nano /etc/hosts  
hostname
```

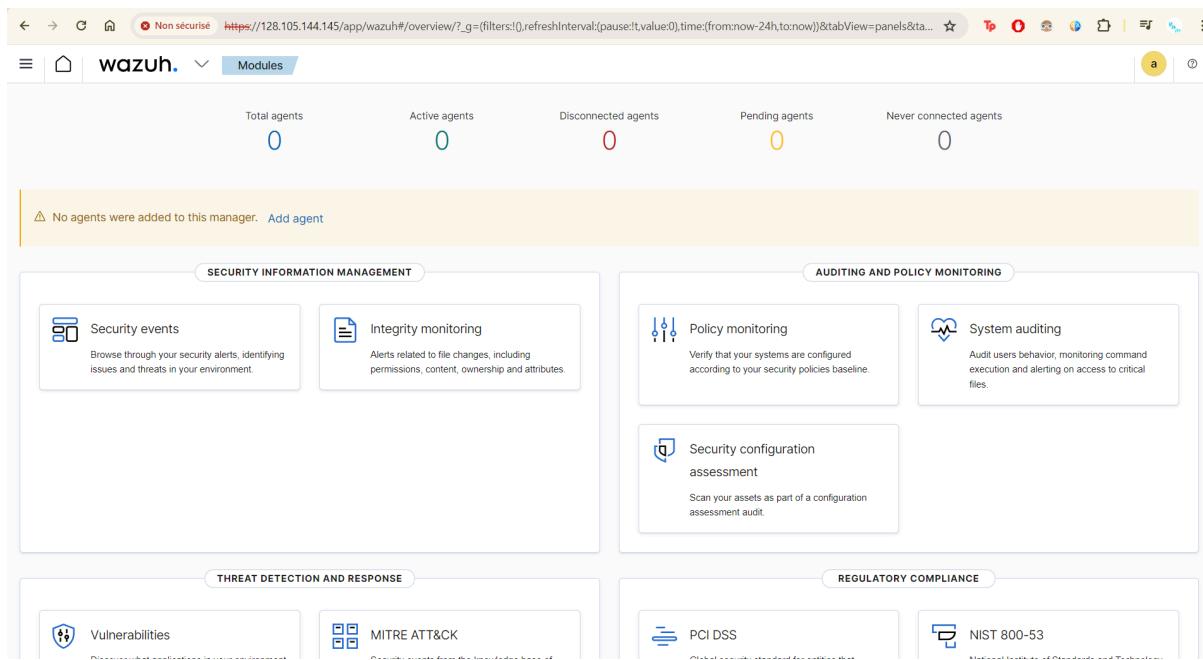


Figure 26 : Aperçu de l'interface WEB

IV. Wazuh agent :

Le **Manager** et l'**Agent** cryptent leur communication entre eux. Pour ce faire, le Manager et l'Agent doivent partager une **clé** client. Cette clé symétrique chiffre les journaux que l'agent transfère au Manager.

Pour cela on crée à l'avance sur Wazuh, deux groupes : **Windows et Linux** :
(leurs étapes de config seront spécifiées dans la partie graylog)

a. Pour les machines Linux:

Sur l'interface WEB, et sous le volet **AGENTS** :

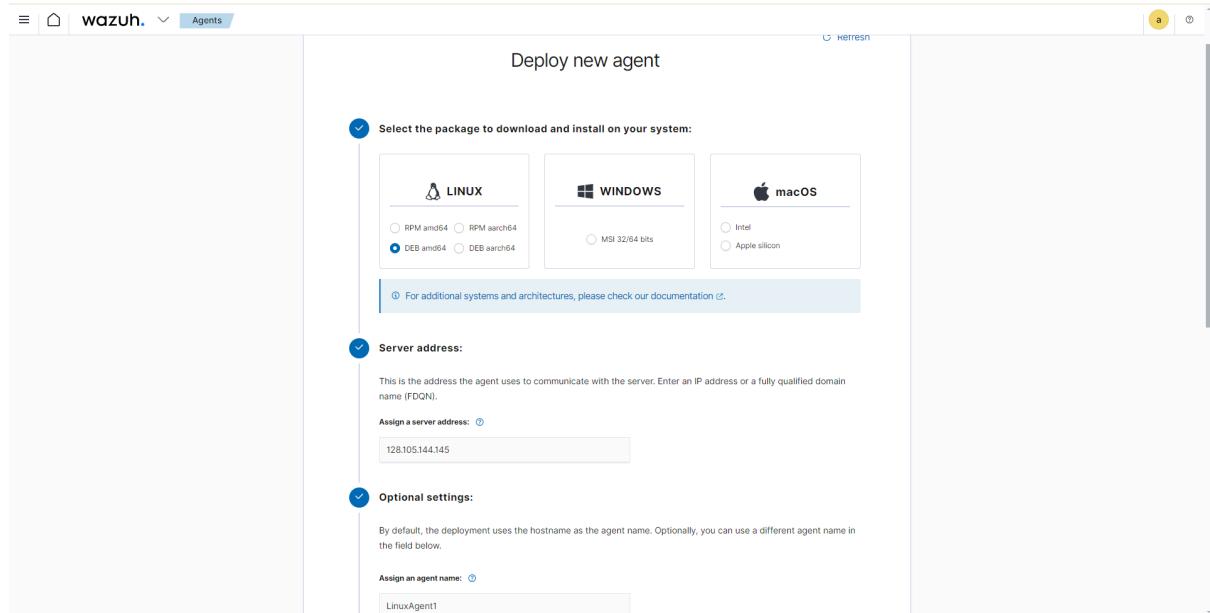


Figure 27 : Ajout de AgentLinux1

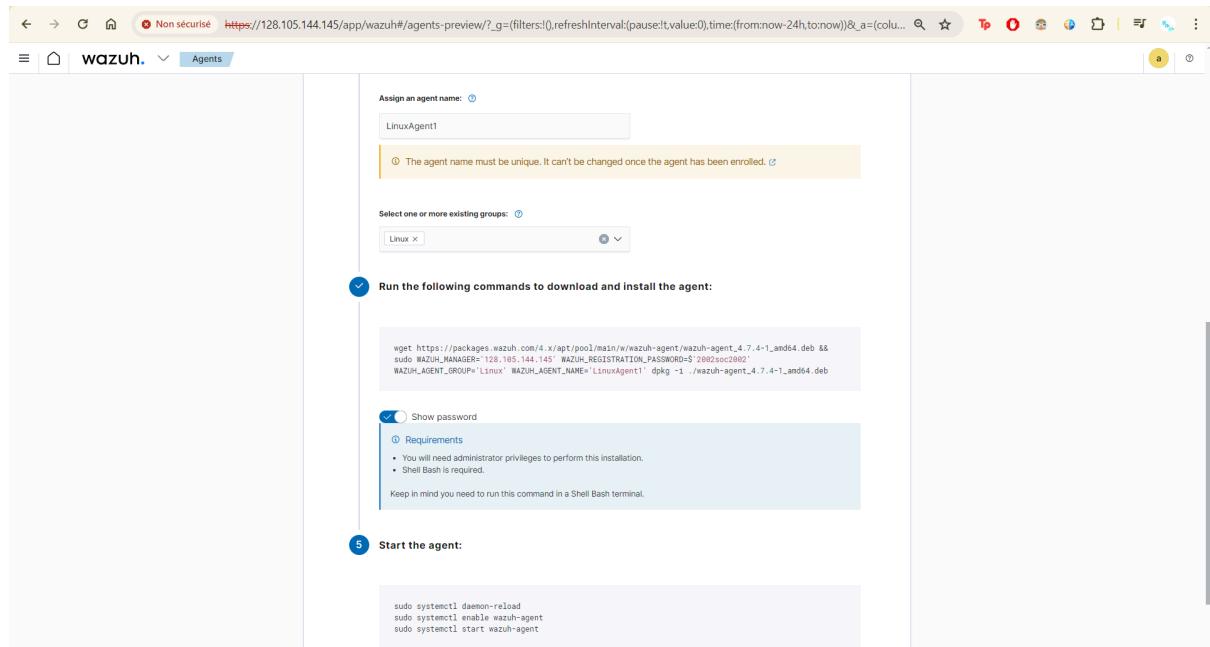


Figure 28 : Ajout de AgentLinux1

Sur la machine **LinuxAgent1**, on lance la commande spécifiée, et on ajoute :

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

```

Yasinom@node0:~$ Yasinom@node0:~$ uname -m
x86_64
Yasinom@node0:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb && sudo WAZUH_MANAGER='128.105.144.145' WAZUH_REGISTRATION_PASSWORD='2002soc2002' WAZUH_AGENT_GROUP='Linux' WAZUH_AGENT_NAME='LinuxAgent1' dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb
--2024-05-29 18:26:12-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 54.230.202.40, 54.230.202.2, 54.230.202.39, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|54.230.202.40|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9372734 (8.9M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.7.4-1_amd64.deb'

wazuh-agent_4.7.4-1_amd64.deb      100%[=====] 8.94M --.-KB/s   in 0.1s

2024-05-29 18:26:12 (66.3 MB/s) - 'wazuh-agent_4.7.4-1_amd64.deb' saved [9372734/9372734]

Selecting previously unselected package wazuh-agent.
(Reading database ... 95473 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.4-1_amd64.deb ...
Unpacking wazuh-agent (4.7.4-1) ...
Setting up wazuh-agent (4.7.4-1) ...
Yasinom@node0:~$ sudo systemctl daemon-reload
ctrl enable wazuh-agent
sudo systemctl start wazuh-agentsudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agentYasinom@node0:~$
```

Figure 29 : Commande lancée sur LinuxAgent1

Ainsi on remarque l'ajout du **LinuxAgent1** sur l'interface Web :

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	LinuxAgent1	128.105.144.165	Linux	Ubuntu 22.04.2 LTS	node01	v4.7.4	active	Deploy new agent Refresh Export formatted WQL Refresh

Figure 30 : LinuxAgent1 Ajoutée

Nous allons maintenant installer et configurer **PacketBeat**, un outil de surveillance de réseau en temps réel. PacketBeat capture le trafic réseau, analyse les paquets et envoie les données collectées à **Wazuh**. Cela permet de visualiser et de surveiller les performances et la sécurité des applications et des services réseau en temps réel.

On copie le script située sur :

et on l'exécute :

```

https://gist.githubusercontent.com/taylorwalton/a23f7e99c49e42bc524d61551d2045ba/raw/29f4424975ef0fd55267eba071be048a5e1a759b/install.sh

chmod +x script.sh
./script.sh

```

```

root@node0:/users/Yasinom# name please_subscribe.sh
root@node0:/users/Yasinom# chmod +x please_subscribe.sh
root@node0:/users/Yasinom# ./please_subscribe.sh
05/29/2024 18:47:00 INFO: Installing Packetbeat
% Total    % Received % Xferd  Average Speed   Time     Time  Current
          Dload  Upload Total Spent   Left  Speed
100 28.8M  100 28.8M  0     0  8665K  0:00:03  0:00:03  --- 8665K
Selecting previously unselected package packetbeat.
(Reading database ... 95853 files and directories currently installed.)
Preparing to unpack packetbeat-7.16.3-amd64.deb ...
Unpacking packetbeat (7.16.3) ...
Setting up packetbeat (7.16.3) ...
--2024-05-29 18:47:05-- https://raw.githubusercontent.com/socfortress/Wazuh-Rules/main/Packetbeat/packetbeat.yml
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10708 (10K) [text/plain]
Saving to: '/etc/packetbeat/packetbeat.yml'

/etc/packetbeat/packetbeat.yml      100%[=====] 10.46K --.-KB/s   in 0s

2024-05-29 18:47:05 (25.9 MB/s) - '/etc/packetbeat/packetbeat.yml' saved [10708/10708]

05/29/2024 18:47:05 INFO: Need assistance? Shoot us an email at info@socfortress.co!
root@node0:/users/Yasinom#

```

Figure 31 : Installation de PacketBeat

Ensuite sur le group Linux on ajoute la localisation du fichier dans lequel packetbeat enregistre les logs du réseau pour la machine Linux:

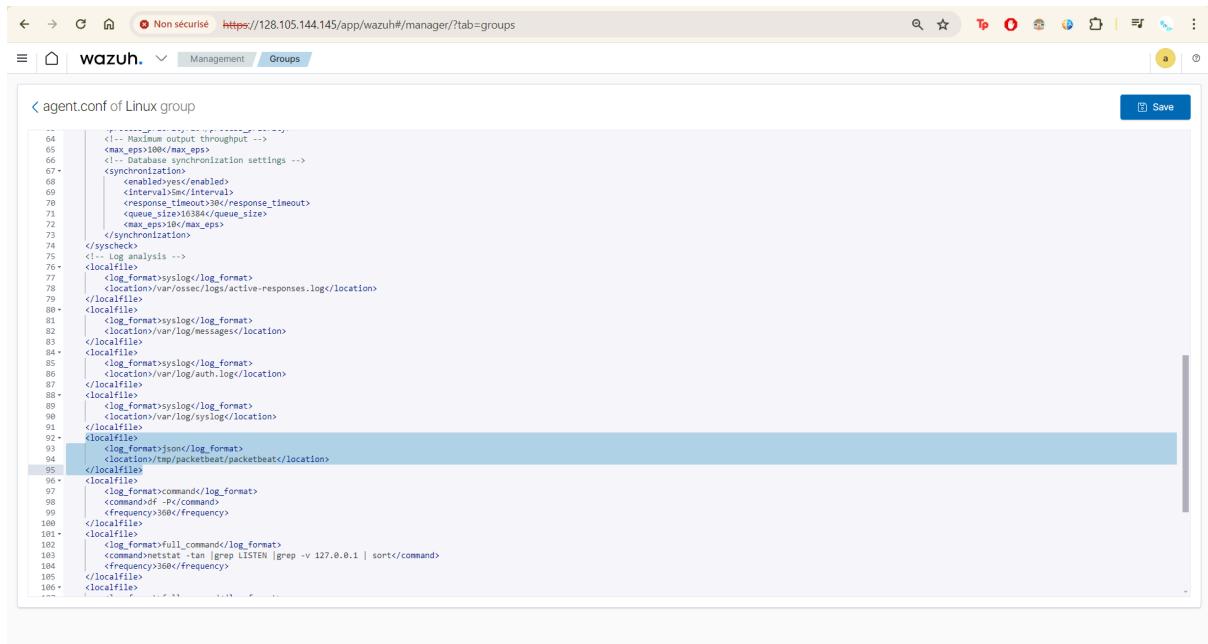


Figure 32 : Ajout de Localisation du fichier de logs de PacketBeat

b. Pour les machines Windows:

De même, on suit les même étapes :

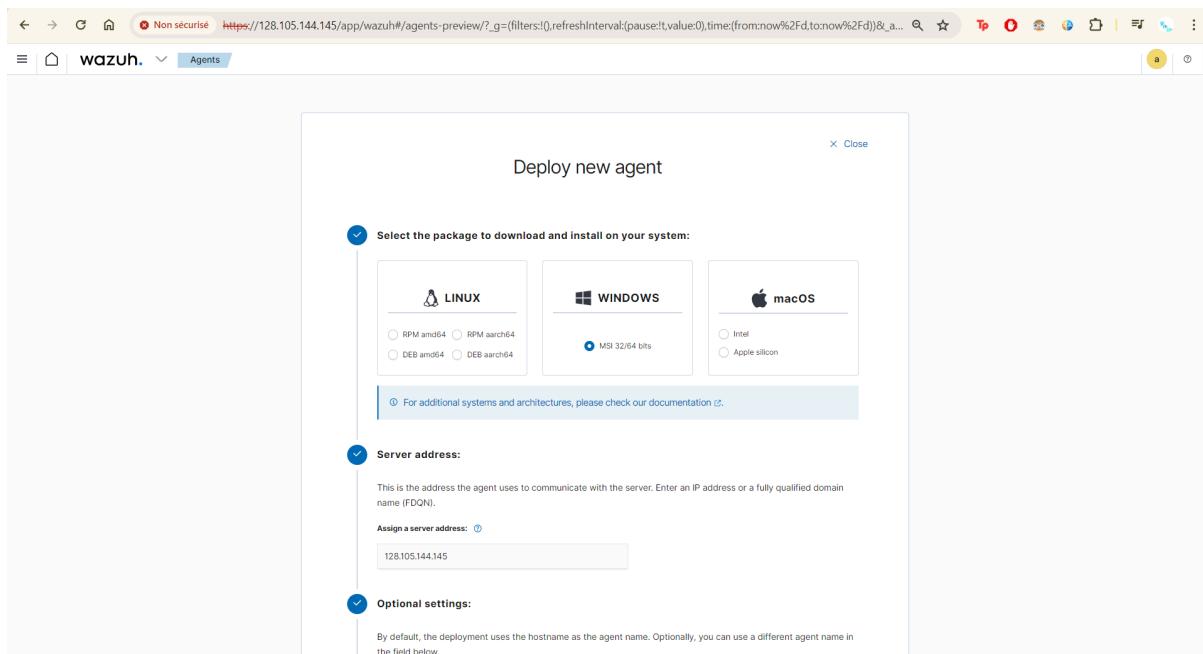


Figure 33 : Ajout de WindowsAgent

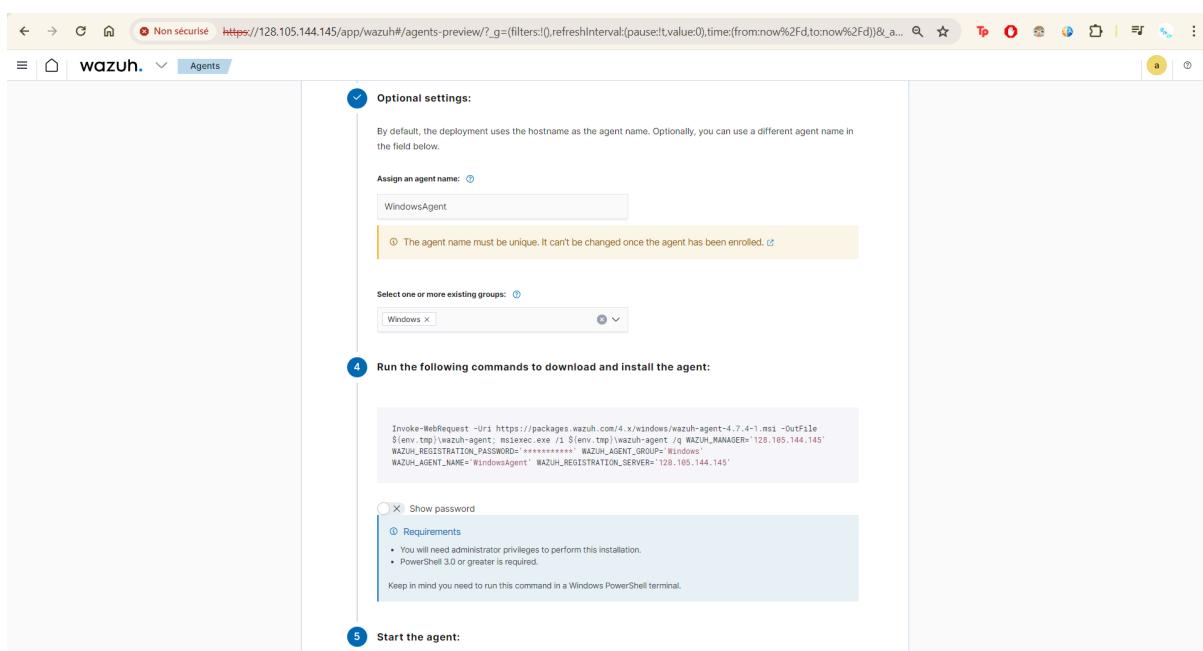


Figure 34 : Ajout de WindowsAgent

Ensuite sur le **WindowsAgent**, on exécute la commande qu'on nous a donné **Wazuh** :

```

Administrator : Windows PowerShell
PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Téléchargez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

C:\Windows\system32>
C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile ${env:tmp}\wazuh-agent; msieexec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='128.105.144.145' WAZUH_REGISTRATION_PASSWORD='2002soc2002' WAZUH_AGENT_GROUP='Windows' WAZUH_AGENT_NAME='WindowsAgent'
WAZUH_REGISTRATION_SERVER='128.105.144.145'
C:\Windows\system32> NET START WazuhSvc
service Wazuh démarre.
service Wazuh a démarré.

C:\Windows\system32>

```

Figure 34 : Commande lancée sur WindowsAgent

Installons **Sysmon** sur nos terminaux **Windows**. Sysmon est une version améliorée des journaux Windows et est fortement recommandé pour tous les terminaux Windows. Vous pouvez fournir votre propre fichier de configuration Sysmon, mais dans cette démonstration, on utilisera le Git Repository de **olafhartong : Sysmon Modular**.

Située dans :

```

https://gist.github.com/taylorwalton/22b3ef3f624edd494ebf6
40aba56120c/raw/cee2383e91aea2b850bd87c118f20fc010955cf8/sysmon_insta
ll.ps1

Administrator : Windows PowerShell ISE
Fichier Modifier Afficher Outils Déboguer Composants additionnels Aide
Sans titre1.ps1* X
1 $sysinternals_repo = 'download.sysinternals.com'
2 $sysinternals_downloadlink = 'https://download.sysinternals.com/files/SysinternalsSuite.zip'
3 $sysinternals_folder = 'C:\Program Files\Sysinternals'
4 $sysinternals_zip = 'SysinternalsSuite.zip'
5 $sysmonconfig_downloadlink = 'https://raw.githubusercontent.com/olafhartong/sysmon-r/master/config/sysmonconfig-export.xml'
6 $sysmonconfig_file = 'sysmonconfig-export.xml'
7
8 [Net.ServicePointManager]:SecurityProtocol = [Net.SecurityProtocolType]::Tls12
9
10 if (Test-Path -Path $sysinternals_folder) {
11     write-host ('$sysinternals folder already exists')
12 } else {
13     $outputPath = $env:TMP
14     $outputItem = $sysinternals_zip
15     New-Item -Path "C:\Program Files" -Name "sysinternals" -ItemType "directory"
16     $x = 0
17     do {
18         write-output "Waiting for network"
19         Start-Sleep -s 5
20     } until((($connectresult = Test-NetConnection $sysinternals_repo -Port 443) | ? { $_.Connected -eq $true }))
21
22     if ($connectresult.TcpTestSucceeded -eq $true) {
23         Try
24             write-host ('Downloading and copying Sysinternals Tools to C:\Program Files\sysinternals')
25             Invoke-WebRequest -Uri $sysinternals_downloadlink -OutFile $outputPath\$outputItem
26             Expand-Archive -path $outputPath\$outputItem -destinationpath $sysinternals_folder
27             Start-Sleep -s 10
28             Invoke-WebRequest -Uri $sysmonconfig_downloadlink -OutFile $outputPath\$sysmonconfig_file
29             $serviceName = 'Sysmon64'
30             If (Get-Service $serviceName -ErrorAction SilentlyContinue) {
31                 write-host ('$sysmon Is Already Installed')
32             } else {
33                 If (Get-Service $serviceName -ErrorAction SilentlyContinue) {
34                     write-host ('$sysmon Is Already Installed')
35                 } else {
36                     Invoke-Command [reg.exe ADD HKCU\Software\Sysinternals /v EulaAccepted /t REG_DWORD /d 1]
37                     Invoke-Command [reg.exe ADD HKU\DEFAULT\Software\Sysinternals /v EulaAccepted /t REG_DWORD /d 1]
38                     Start-Process -filepath $sysinternals_folder\Sysmon64.exe -ArgumentList @("-i", "$outputPath\$sysmonconfig_file")
39                 }
40             }
41             Catch
42             {
43                 $errorMessage = $_.Exception.Message
44                 $failedItem = $_.Exception.ItemName
45                 Write-Error -Message "$errorMessage $failedItem"
46                 exit 1
47             }
    }

Répertoire : C:\Program Files
Mode LastWriteTime Length Name
---- -- - - -
d---- 09/06/2024 06:17 sysinternals
Waiting for network
Downloading and copying Sysinternals Tools to C:\Program Files\sysinternals...
L'opération a réussi.

PS C:\Windows\system32>

```

Figure 36 : Script d'Installation Sysmon lancée sur WindowsAgent

On remarquera ensuite dans l' Observateur d'événements que les logs **sysmon** sont capturés et stockés sous forme : **Microsoft Windows Sysmon/Operational**

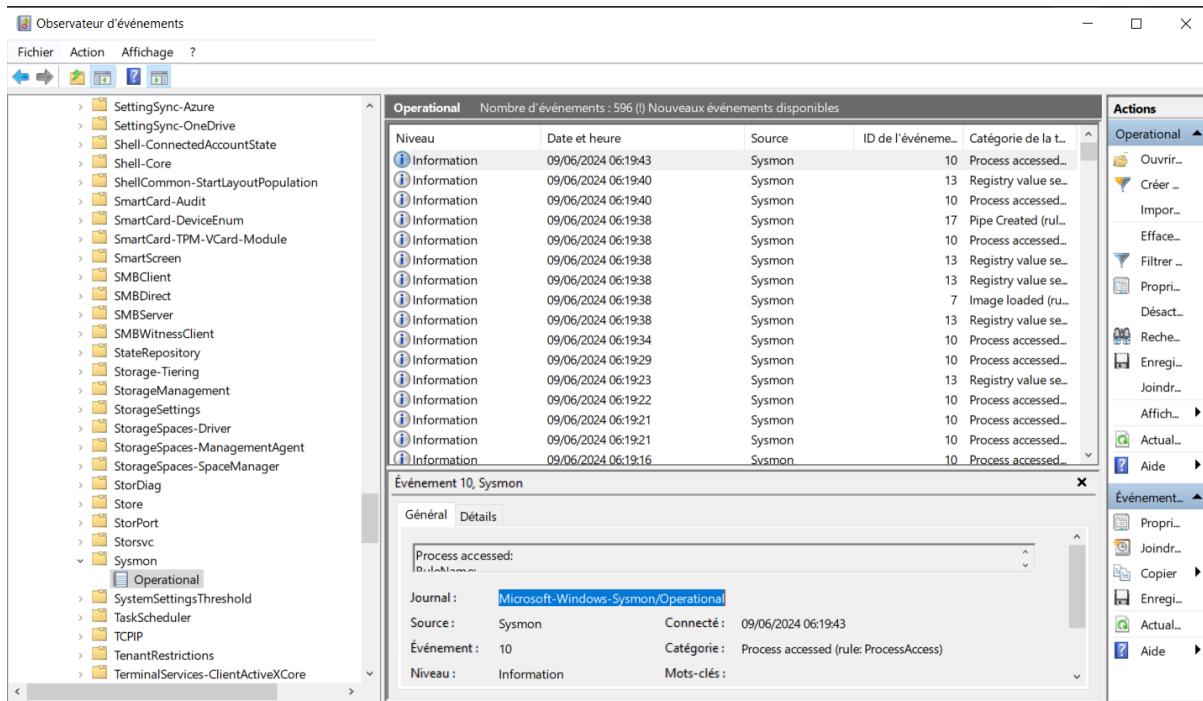


Figure 37 : Logs Sysmon Capturées

et sur la config du group ‘windows’ sur Wazuh, on ajoute la localisation des logs Sysmon pour qu’ils soient capturées :

```

< agent.conf Windows group >
114     <java_path>\server\jre\bin\java.exe</java_path>
115     <iscat_path>C:\cls\cat\iscat_.path
116
117     <!-- Osquery Integration -->
118     <wodle>osquery</wodle>
119     <!-- wodle disabled -->
120     <run_daemon>yes</run_daemon>
121     <bin_path>C:\Program Files\osquery\osqueryd\bin.path
122     <log_path>C:\Program Files\osquery\log\osquery.log</log_path>
123     <config_path>C:\Program Files\osquery\osquery.conf</config_path>
124     <add_labels>yes</add_labels>
125
126     </wodle>
127     <!-- active response -->
128     <active-response>
129         <disabled>no</disabled>
130         <ca_verification>root.pem</ca_verification>
131         <ca_verification>yes</ca_verification>
132     </active-response>
133
134     <!-- log analysis -->
135     <location>Microsoft-Windows-Sysmon/Operational</location>
136     <log_format>eventchannel</log_format>
137     <localfile>
138         <location>Windows PowerShell</location>
139         <log_format>eventchannel</log_format>
140     </localfile>
141     <localfile>
142         <location>Microsoft-Windows-CodeIntegrity/Operational</location>
143         <log_format>eventchannel</log_format>
144     </localfile>
145     <localfile>
146         <location>Microsoft-Windows-TaskScheduler/Operational</location>
147         <log_format>eventchannel</log_format>
148     </localfile>
149     <localfile>
150         <location>Microsoft-Windows-PowerShell/Operational</location>
151         <log_format>eventchannel</log_format>
152     </localfile>
153
154     <location>Microsoft-Windows-Windows Firewall With Advanced Security/Firewall</location>
155     <log_format>eventchannel</log_format>
156
157

```

Figure 38 : Ajout de la localisation des logs Sysmon

V. Installation de Graylog — Ingestion de Journaux :

a. Installation de Graylog :

Nous commençons par installer **MongoDB 7**, qui est la dernière version disponible. MongoDB est une base de données NoSQL populaire, connue pour sa flexibilité et sa capacité à gérer de grandes quantités de données de manière efficace.

on commence par exécuter les commandes :

```
root@node2:/users/Yasinom# curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | sudo gpg -o /usr/share/keyrings/mongodb-server-7.0.gpg --dearmor
File '/usr/share/keyrings/mongodb-server-7.0.gpg' Overwritten. Overwrite? (y/N) y
root@node2:/users/Yasinom# echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ] https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-7.0.list
deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ] https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 multiverse
root@node2:/users/Yasinom# apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:3 https://packages.wazuh.com/4.x/apt stable InRelease
Ign:4 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:6 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 Release [2,090 B]
Get:7 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:8 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 Release.gpg [866 B]
Hit:9 http://repos.emulab.net/emulab/ubuntu jammy InRelease
Hit:10 http://repos.emulab.net/grub-backports/ubuntu jammy InRelease
Get:11 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0/multiverse amd64 Packages [40.9 kB]
Get:12 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0/multiverse arm64 Packages [39.8 kB]
Fetched 313 kB in 2s (165 kB/s)
Reading package lists... Done
root@node2:/users/Yasinom#
```

Figure 39 : Installation de MongoDB

```
root@node2:/users/Yasinom# sudo apt-get install -y mongodb-org
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mongodb-org is already the newest version (7.0.11).
0 upgraded, 0 newly installed, 0 to remove and 163 not upgraded.
root@node2:/users/Yasinom# systemctl daemon-reload
root@node2:/users/Yasinom# systemctl start mongod
root@node2:/users/Yasinom# systemctl status mongod
● mongod.service - MongoDB Database Server
   Loaded: loaded (/lib/systemd/system/mongod.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-05-27 12:46:22 CDT; 6s ago
     Docs: https://docs.mongodb.org/manual
 Main PID: 61938 (mongod)
    Memory: 380.2M
      CPU: 1.536s
       CGroup: /system.slice/mongod.service
           └─61938 /usr/bin/mongod --config /etc/mongod.conf

May 27 12:46:22 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us systemd[1]: Started MongoDB Database Server.
May 27 12:46:22 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us mongod[61938]: {"t":{"$date":"2024-05-27T12:46:22.558Z"}, "s": "I", "c": "CONTROL", "id": 748456}
lines 1-12/12 (END)
```

Figure 40 : Installation de MongoDB

Ensuite on importe les packages **Graylog**, et on l'installe :

```
root@node2:/users/Yasinom# wget https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
--2024-05-27 12:59:31-- https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
Resolving packages.graylog2.org (packages.graylog2.org)... 104.21.88.209, 172.67.153.95, 2606:4700:3035::ac43:995f, ...
Connecting to packages.graylog2.org (packages.graylog2.org)|104.21.88.209|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-5.2-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20240527T179912X-Amz-SignedHeaders=hostX-Amz-Expires=0000X-Amz-Credential=AKIAJ1S1GMCSPIXFVDPIAV2F20240527%2Feu-west-1%2Fs%3Faws4_request&X-Amz-Signature=54f20356eb6fc70ade6969
fdfc58e82668a0fd721ee07cefe17fdb53f93b19 [following]
--2024-05-27 12:59:31-- https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-5.2-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20240527T179912X-Amz-SignedHeaders=hostX-Amz-Expires=0000X-Amz-Credential=AKIAJ1S1GMCSPIXFVDPIAV2F20240527%2Feu-west-1%2Fs%3Faws4_request&X-Amz-Signature=54f20356eb6fc70ade6969
6eb6fc70ade6969fdcc58e82668a0fd721ee07cefe17fdb53f93b19
Resolving graylog-package-repository.s3.eu-west-1.amazonaws.com (graylog-package-repository.s3.eu-west-1.amazonaws.com)|52.218.89.112, 52.218.98.4, 52.218.117.122, ...
...
Connecting to graylog-package-repository.s3.eu-west-1.amazonaws.com (graylog-package-repository.s3.eu-west-1.amazonaws.com)|52.218.89.112|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2092 (2.0K) [application/x-debian-package]
Saving to: 'graylog-5.2-repository_latest.deb.1'

graylog-5.2-repository_latest.deb.1          100%[=====] 2.04K --.-KB/s   in 0s

2024-05-27 12:59:32 (47.9 MB/s) - 'graylog-5.2-repository_latest.deb.1' saved [2092/2092]

root@node2:/users/Yasinom# sudo dpkg -i graylog-5.2-repository_latest.deb
Selecting previously unselected package graylog-5.2-repository.
(Reading database ... 215993 files and directories currently installed.)
Preparing to unpack graylog-5.2-repository_latest.deb ...
Unpacking graylog-5.2-repository (1-2) ...
Setting up graylog-5.2-repository (1-2) ...
root@node2:/users/Yasinom#
```

Figure 41 : Installation de Graylog

```

root@node2:/users/Yasinom# sudo apt-get update && sudo apt-get install graylog-server
Hit:1 https://packages.wazuh.com/4.x/apt stable InRelease
Ign:2 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 InRelease
Hit:3 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 Release
Hit:5 http://repos.emulab.net/emulab/ubuntu jammy InRelease
Hit:6 http://repos.emulab.net/grub-backports/ubuntu jammy InRelease
Get:4 https://packages.graylog2.org/repo/debian stable InRelease [68.8 kB]
Get:8 https://packages.graylog2.org/repo/debian stable/5.2 amd64 Packages [8,793 B]
Hit:9 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Hit:10 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:11 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:12 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease
Fetched 77.6 kB in 5s (15.3 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  graylog-server
0 upgraded, 1 newly installed, 0 to remove and 163 not upgraded.
Need to get 271 MB of archives.
After this operation, 390 MB of additional disk space will be used.
Get:1 https://packages.graylog2.org/repo/debian stable/5.2 amd64 graylog-server amd64 5.2.7-1 [271 MB]
Fetched 271 MB in 11s (24.3 MB/s)
Selecting previously unselected package graylog-server.
(Reading database ... 215997 files and directories currently installed.)
Preparing to unpack .../graylog-server_5.2.7-1_amd64.deb ...
Unpacking graylog-server (5.2.7-1) ...
Setting up graylog-server (5.2.7-1) ...
#####
Graylog does NOT start automatically!

Please run the following commands if you want to start Graylog automatically on system boot:
  sudo systemctl enable graylog-server.service
  sudo systemctl start graylog-server.service
#####
root@node2:/users/Yasinom#

```

Figure 42 : Installation de Graylog

Ensuite sur Wazuh Web Interface, on ajoute un user gralog avec role ‘admin’:

The security plugin includes an internal user database. Use this database in place of, or in addition to, an external authentication system such as LDAP or Active Directory. Learn more [↗](#)

Credentials

Username
Specify a descriptive and unique user name. You cannot edit the name once the user is created.
graylog

The user name must contain from 2 to 50 characters. Valid characters are A-Z, a-z, 0-9, (.) underscore, (-) hyphen and unicode characters.

Password
 Password should be at least 8 characters long and contain at least one uppercase letter, one lowercase letter, one digit, and one special character.

Re-enter password
 The password must be identical to what you entered above.

Figure 43 : Ajout du user graylog

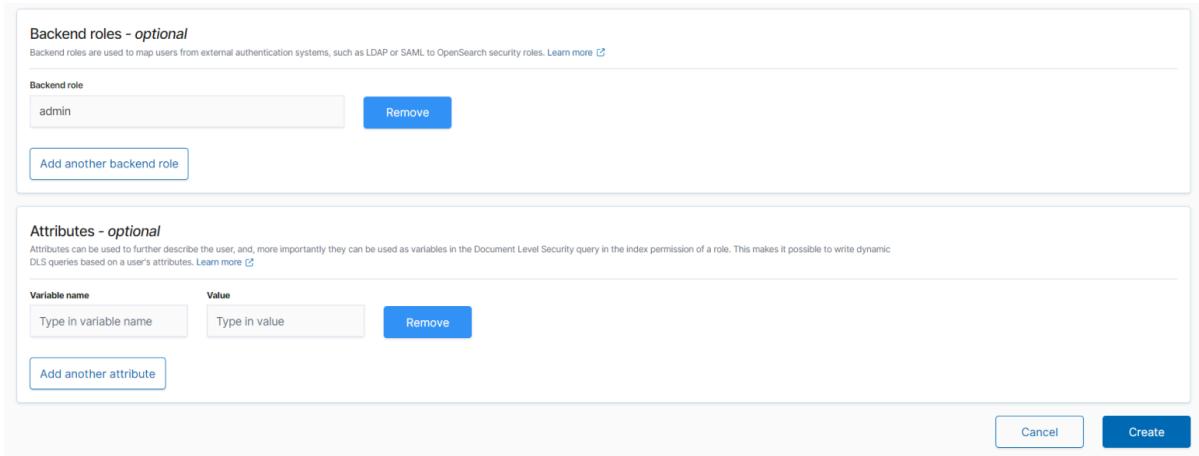


Figure 44 : Ajout du user graylog

On envisage maintenant la configuration de notre **serveur graylog**, en utilisant les commandes :

```
- password_secret : pwgen -N 1 -s 96
- root_password_sha2 : echo -n "Enter Password: " && head
-1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
- nano /etc/graylog/server/server.conf
```

```
Sélection root@node2: /users/Yasinom
GNU nano 6.2
/etc/graylog/server/server.conf *
# Default: false
#http_enable_tls = true

# The X.509 certificate chain file in PEM format to use for securing the HTTP interface.
#http_tls_cert_file = /path/to/graylog.crt

# The PKCS#8 private key file in PEM format to use for securing the HTTP interface.
#http_tls_key_file = /path/to/graylog.key

# The password to unlock the private key used for securing the HTTP interface.
#http_tls_key_password = secret

# If set to "true", Graylog will periodically investigate indices to figure out which fields are used in which streams.
# It will make field list in Graylog interface show only fields used in selected streams, but can decrease system performance,
# especially on systems with great number of streams and fields.
stream_aware_field_types=false

# Comma separated list of trusted proxies that are allowed to set the client address with X-Forwarded-For
# header. May be subnets, or hosts.
#trusted_proxies = 127.0.0.1/32, 0:0:0:0:0:1/128

# List of Elasticsearch hosts Graylog should connect to.
# Need to be specified as a comma-separated list of valid URIs for the http ports of your elasticsearch nodes.
# If one or more of your elasticsearch hosts require authentication, include the credentials in each node URI that
# requires authentication.
#
# Default: http://127.0.0.1:9200
#elasticsearch_hosts = http://node1:9200,http://user:password@node2:19200

elasticsearch_hosts = https://graylog:2002soc2002@node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us:9200

# Maximum number of attempts to connect to elasticsearch on boot for the version probe.
#
# Default: 0, retry indefinitely with the given delay until a connection could be established
#elasticsearch_version_probe_attempts = 5

# Waiting time in between connection attempts for elasticsearch_version_probe_attempts
#
```

Figure 45 : Configuration de graylog

```

root@node2: /users/yasinom
GNU nano 6.2                                     /etc/graylog/server/server.conf

#
# If you are running more than one instances of Graylog server you have to select one of these
# instances as leader. The leader will perform some periodical tasks that non-leaders won't perform.
is_leader = true

# The auto-generated node ID will be stored in this file and read after restarts. It is a good idea
# to use an absolute file path here if you are starting Graylog server from init scripts or similar.
node_id_file = /etc/graylog/server/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (e.g. encrypted access tokens)
password_secret = DM7X4Z0aLQ13UJnZsDSDG0ZnmQ1tpmNF3DXx1jsymSSYwmI8J9sOYJUEebLgizh86DB10kORcYi5M09BF0lvedm0JdvxfsbK

# The default root user is named 'admin'
root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = 0038d54565ef7fae32f4842c87da0d3220914b4de27618efddb6947aba0248af

# The email address of the root user.
# Default is empty
root_email = ""

# The time zone setting of the root user. See http://www.joda.org/joda-time/timezones.html for a list of valid time zones.
# Default is UTC
root_timezone = UTC

# Set the bin directory here (relative or absolute)
# This directory contains binaries that are used by the Graylog server.
# Default: bin_

```

Figure 46 : Configuration de graylog

on se redémarre le service :

```
systemctl restart graylog-server
```

et on se rend sur [http:<ip_wazuh>:9000](http://<ip_wazuh>:9000)

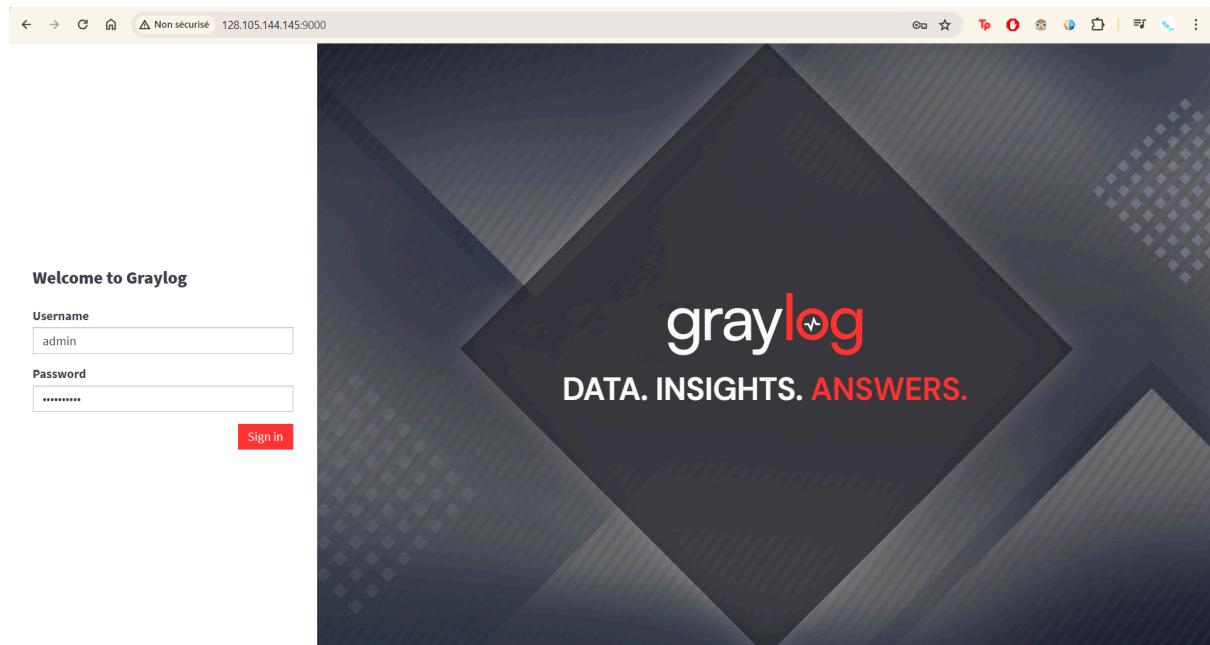


Figure 47 : Interface Web de graylog

On trouve bien, que notre node **Wazuh** est ajoutée et référencée sur ‘nodes’:

The screenshot shows the Graylog web interface at the URL <https://128.105.144.145/system/nodes>. The page title is "Nodes". It indicates there is 1 active node. The node listed is "df116280 / node2-link-1". Below the node list, it says "The journal contains 0 unprocessed messages in 1 segment. 0 messages appended, 0 messages read in the last second." and "Current lifecycle state: Running, Message processing: Enabled, Load balancer indication: ALIVE". A progress bar shows the JVM is using 705.1MiB of 4.0GiB heap space.

Figure 47 : Node Wazuh sur graylog

Voici nos indices :

Index	Health	Managed by p...	Status	Total size	Size of primaries	Total documents	Deleted docu...	Primaries	Replicas
wazuh-statistics-2024.22w	Green	No	Open	366kb	366kb	347	0	1	0
wazuh-monitoring-2024.22w	Green	No	Open	208b	208b	0	0	1	0
wazuh-alerts-4.x-2024.05.27	Green	No	Open	884kb	884kb	234	0	3	0
investigation_message_index_0	Green	No	Open	208b	208b	0	0	1	0
investigation_event_index_0	Green	No	Open	208b	208b	0	0	1	0
graylog_0	Green	No	Open	208b	208b	0	0	1	0
gl-system-events_0	Green	No	Open	28.4kb	28.4kb	1	44	1	0
gl-failures_0	Green	No	Open	208b	208b	0	0	1	0
gl-events_0	Green	No	Open	208b	208b	0	0	1	0
opensearch-observability	Green	No	Open	208b	208b	0	0	1	0
opendistro_security	Green	No	Open	46.4kb	46.4kb	10	1	1	0
kibana_1	Green	No	Open	25.8kb	25.8kb	4	1	1	0

Figure 48 : Indices Wazuh

b. liaison de graylog avec Wazuh manager :

On par exécuter le suivant :

```
systemctl enable wazuh-manager  
systemctl start wazuh-manager  
systemctl status wazuh-manager
```

Sur l’interface Web de graylog, on ajoute un Input pour wazuh :

The screenshot shows the Graylog web interface at the URL 128.105.144.145:9000/welcome. The top navigation bar includes links for Search, Streams, Alerts, Dashboards, Enterprise, Security, System (with a red notification badge), and a user icon. The main content area displays a 'Welcome to Graylog!' message and sections for 'Last Opened' and 'Recent Activity'. On the right, a sidebar menu under 'System' has 'Inputs' selected, which is highlighted in blue. Other menu items include Overview, Configurations, Nodes, Logging, and Pipelines. Below the sidebar, there are sections for 'Saved Items' and 'Releases'.

Figure 49 : Ajout du Input FluentBit pour Wazuh

The screenshot shows the 'Inputs' configuration page in the Graylog web interface at the URL 128.105.144.145:9000/system/inputs. The top navigation bar is identical to Figure 49. The main content area shows a list of available inputs: Raw/Plaintext TCP, Random HTTP message generator, Raw/Plaintext AMQP, Raw/Plaintext Kafka, Raw/Plaintext TCP (selected and highlighted in blue), Raw/Plaintext UDP, Salesforce, Syslog AMQP, Syslog Kafka, and Syslog TCP. A 'Launch new input' button is visible at the top of the list.

Figure 50 : Ajout du Input FluentBit pour Wazuh

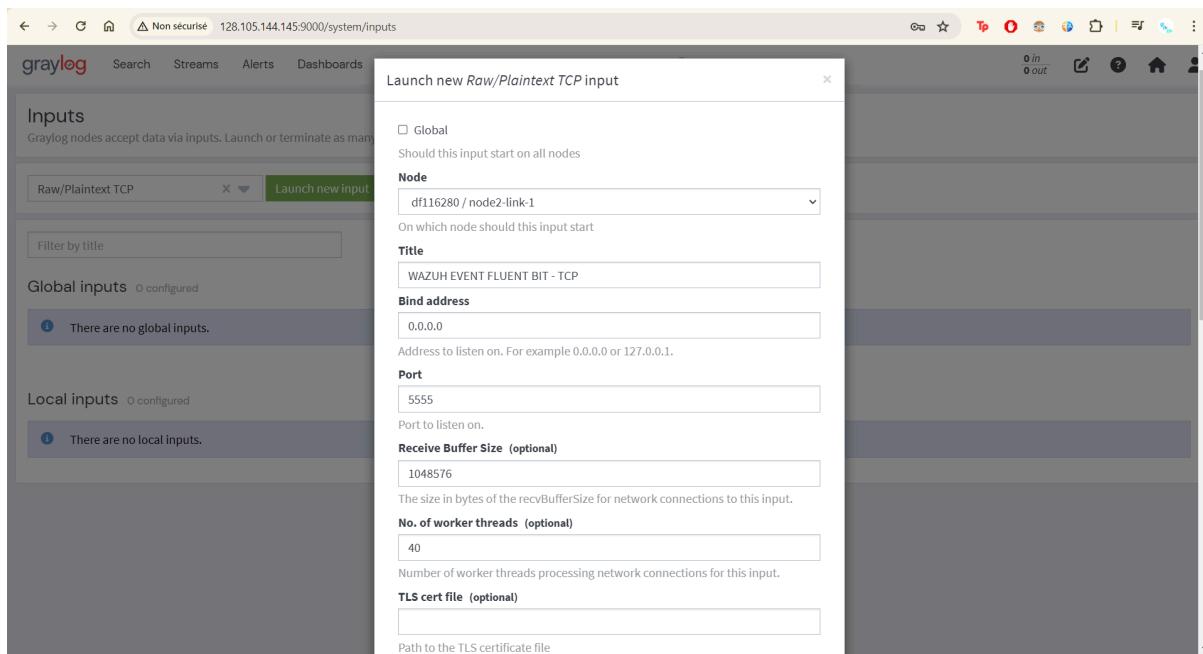


Figure 51 : Ajout du Input FluentBit pour Wazuh

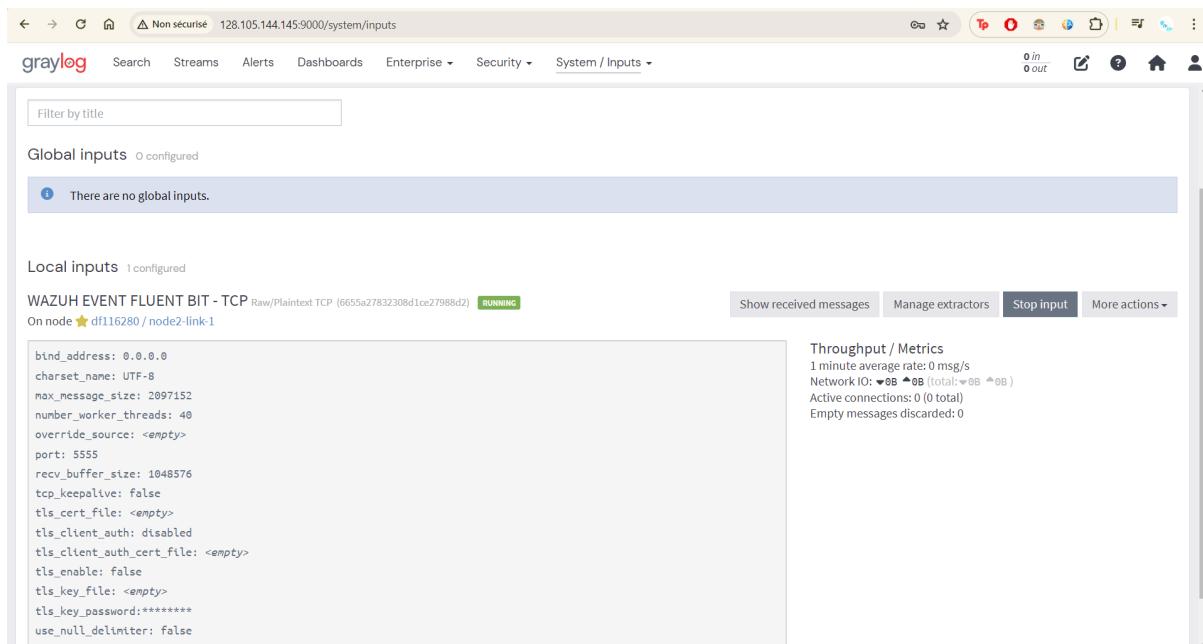


Figure 52 : Ajout du Input FluentBit pour Wazuh

Ensuite, on remarque que Graylog active le **port 5555 en mode écoute** :

```

root@node2:/etc/wazuh-indexer# netstat -ltpnd
Active Internet connections (only servers)
Proto Recv-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0 128.105.144.145:443   0.0.0.0:*
tcp        0      0 0.0.0.0:16505     0.0.0.0:*
tcp        0      0 0.0.0.0:111       0.0.0.0:*
tcp        0      0 0.0.0.0:22        0.0.0.0:*
tcp        0      0 0.0.0.0:1515     0.0.0.0:*
tcp        0      0 0.0.0.0:1514     0.0.0.0:*
tcp        0      0 127.0.0.53:53      0.0.0.0:*
tcp        0      0 0.0.0.0:55000     0.0.0.0:*
tcp        0      0 127.0.0.1:27017    0.0.0.0:*
tcp6       0      0 128.105.144.145:9000  :::*
tcp6       0      0 :::5555          :::*
tcp6       0      0 ::::111         :::*
tcp6       0      0 ::::22          :::*
tcp6       0      0 10.10.1.3:9300    :::*
tcp6       0      0 10.10.1.3:9200    :::*

```

Figure 53 : Ports ouverts

On installe ensuite FluentBit :

- Fluent Bit récupère les **données capturées par le gestionnaire Wazuh** et les envoie à Graylog.
- Fluent Bit prend le fichier : **/var/ossec/logs/alerts/alerts.json** et l'envoie à Graylog.
-

on installe **FluentBit** avec :

```

curl https://raw.githubusercontent.com/fluent/fluent-bit/master/install.sh | sh

```

Ensuite on le configure :

```

root@node2:/etc/fluent-bit
GNU nano 6.2                                     fluent-bit.conf

[SERVICE]
flush      5
daemon    Off
log_level  info
parsers_file parsers.conf
plugins_file plugins.conf
http_server Off
http_listen 0.0.0.0
http_port   2020
storage.metrics on
storage.path /var/log/flb-storage/
storage.sync normal
storage.checksum off
storage.backlog.mem_limit 5M
log_file /var/log/td-agent-bit.log

[INPUT]
name tail
path  /var/ossec/logs/alerts/alerts.json
tag wazuh
parser json
Buffer_Max_Size 5MB
Buffer_Chunk_Size 400k
storage.type filesystem
Mem_Buf_Limit 512MB

[OUTPUT]
Name tcp
Host node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us
Port 5555
net.keepalive off
Match wazuh
Format json_lines
json_date_key true

```

Figure 54 : Configuration de FluentBit

```

root@node2:/etc/fluent-bit# systemctl enable fluent-bit
Created symlink /etc/systemd/system/multi-user.target.wants/fluent-bit.service → /lib/systemd/system/fluent-bit.service.
root@node2:/etc/fluent-bit# systemctl start fluent-bit
root@node2:/etc/fluent-bit# systemctl status fluent-bit
● fluent-bit.service - Fluent Bit
   Loaded: loaded (/lib/systemd/system/fluent-bit.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-05-28 05:20:08 CDT; 4s ago
       Docs: https://docs.fluentbit.io/manual/
   Main PID: 81515 (fluent-bit)
      Tasks: 5 (limit: 230387)
        Memory: 3.2M
         CPU: 29ms
        CGroup: /system.slice/fluent-bit.service
           └─81515 /opt/fluent-bit/bin/fluent-bit -c //etc/fluent-bit/fluent-bit.conf

May 28 05:20:08 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us fluent-bit[81515]: Fluent Bit v3.0.6
May 28 05:20:08 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us fluent-bit[81515]: * Copyright (C) 2015-2024 The Fluent Bit Authors
May 28 05:20:08 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us fluent-bit[81515]: * Fluent Bit is a CNCF sub-project under the umbrella of Fluentd
May 28 05:20:08 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us fluent-bit[81515]: * https://fluentbit.io
May 28 05:20:08 node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us fluent-bit[81515]: 
lines 1-21/21 (END)

```

Figure 55 : Configuration de FluentBit

Bonus : Pour éviter toute éventuelle erreur, commentez la ligne suivante dans '`/etc/wazuh-indexer/opensearch.yml`'

```

root@node2:/users/Yasinom
GNU nano 2.2                               /etc/wazuh-indexer/opensearch.yml

node.max_local_storage_nodes: "1"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

bootstrap.memory_lock: true

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us-key.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.resolve_hostname: false
plugins.security.ssl.http.enabled.ciphers:
  - "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
  - "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384"
plugins.security.ssl.http.enabled_protocols:
  - "Tlsv1.2"
plugins.security.authz.admin_dn:
  - "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
  - "CN=node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
  - "all_access"
  - "security_rest_api_access"

plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".opendistro-alerting-config", ".opendistro-alerting-alert*", ".opendistro-anomaly-results*", ".opendistro-anomaly-detector*"]

## Option to allow Filebeat-oss 7.10.2 to work ##
#compatibility.override_main_response_version: true

```

Figure 56 : Modification sur `opensearch.yml`

On remarque que nous recevons les journaux depuis **10.10.1.3 (WAZUH)** :

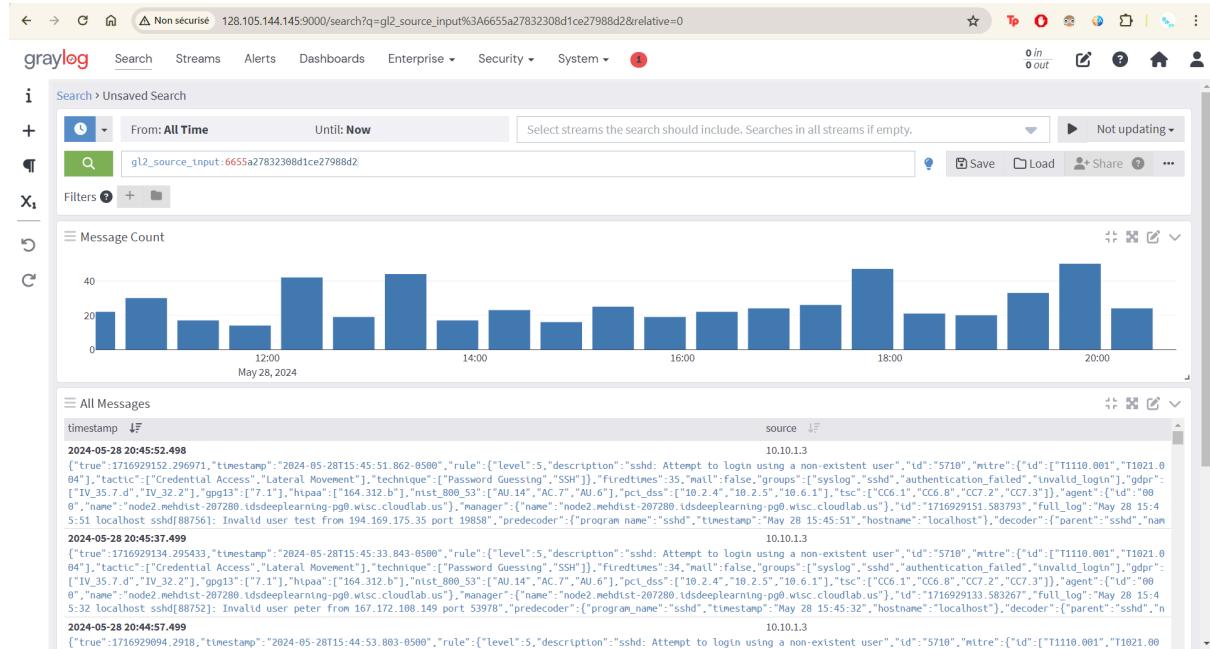


Figure 57 : Reçoi des Logs

On configure maintenant Wazuh Manager :

The screenshot shows a terminal window with the command "nano /var/ossec/etc/ossec.conf" running. The file contains XML configuration for the Wazuh system. Key sections include "rule_test" (with "max_sessions" and "session_timeout" settings), "auth" (with "use_source_ip" and "use_password" options), and "cluster" (specifying a node name and IP). The terminal also shows standard nano key bindings at the bottom.

```

<rule_test>
  <enabled>yes</enabled>
  <threads></threads>
  <max_sessions>64</max_sessions>
  <session_timeout>15m</session_timeout>
</rule_test>

<!-- Configuration for wazuh-authd -->
<auth>
  <disabled>no</disabled>
  <port>1515</port>
  <use_source_ip>no</use_source_ip>
  <purge>yes</purge>
  <use_password>yes</use_password>
  <ciphers>HIGH:!ADH:!EXP:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>
  <!-- <ssl_agent_ca><ssl_agent_ca> -->
  <ssl_verify_host>no</ssl_verify_host>
  <ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
  <ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
  <ssl_auto_negotiate>no</ssl_auto_negotiate>
</auth>

<cluster>
  <name>wazuh</name>
  <node_name>node01</node_name>
  <node_type>master</node_type>
  <key></key>
  <port>1516</port>
  <bind_addr>0.0.0.0</bind_addr>
  <nodes>
    <node>NODE_IP</node>
  </nodes>
  <hidden>no</hidden>
  <disabled>yes</disabled>
</cluster>

</ossec_config>

```

Figure 58 : Configuration de ossec.conf

```

root@node2:/users/Yasinom
root@node2:/users/Yasinom# echo "2002soc2002" > /var/ossec/etc/authd.pass
root@node2:/users/Yasinom# cat /var/ossec/etc/authd.pass
2002soc2002
root@node2:/users/Yasinom# chmod 640 /var/ossec/etc/authd.pass
root@node2:/users/Yasinom# chown root:wazuh /var/ossec/etc/authd.pass
root@node2:/users/Yasinom#

```

Figure 59 : Configuration de ossec.conf

Et on Active la détection de vulnérabilités :

```

root@node2:/users/Yasinom
GNU nano 6.2                               /var/ossec/etc/ossec.conf *

<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>
    <os>bullseye</os>
    <os>bookworm</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- RedHat OS vulnerabilities -->
  <provider name="redhat">
    <enabled>yes</enabled>
    <os>5</os>
    <os>6</os>
    <os>7</os>
    <os>8</os>
    <os>9</os>
    <update_interval>1h</update_interval>
  </provider>

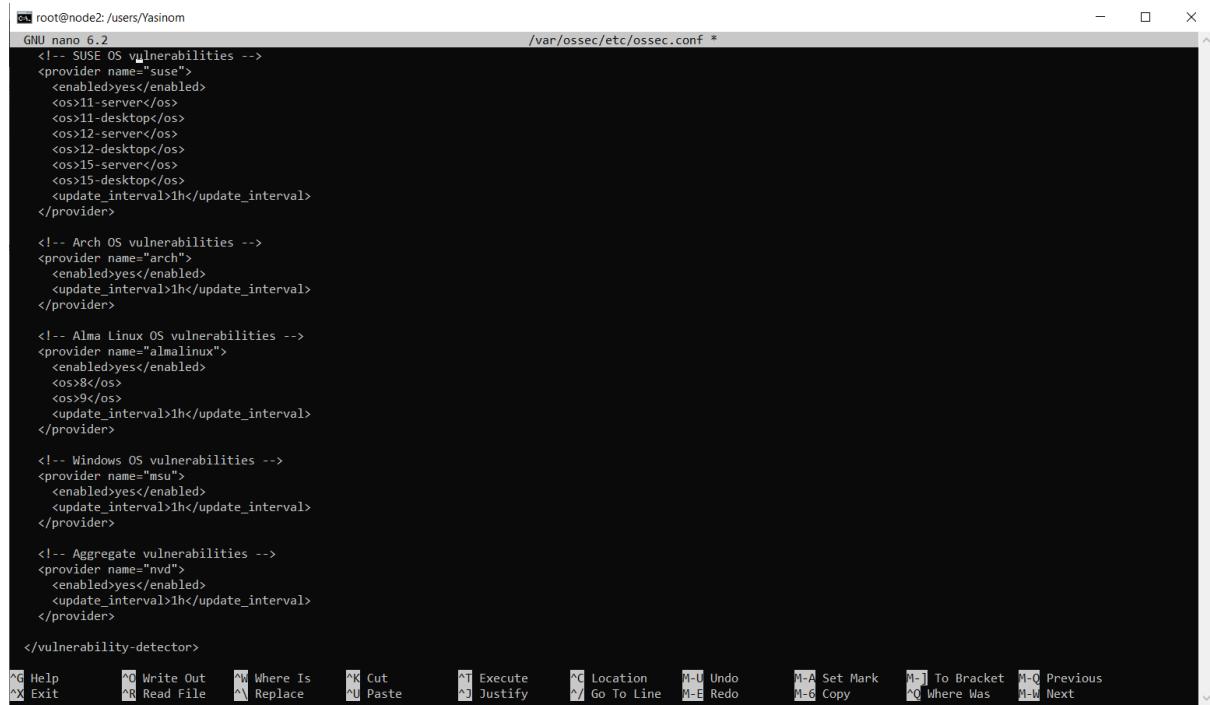
  <!-- Amazon Linux OS vulnerabilities -->

```

Keyboard shortcuts at the bottom:

- Help: ⌘H
- Exit: ⌘X
- Write Out: ⌘W
- Read File: ⌘R
- Where Is: ⌘F
- Replace: ⌘R
- Cut: ⌘K
- Paste: ⌘V
- Execute: ⌘E
- Justify: ⌘J
- Location: ⌘L
- Go To Line: ⌘G
- Undo: M-U
- Redo: M-E
- Copy: M-A
- Set Mark: M-B
- To Bracket: M-J
- Where Was: M-Q
- Previous: M-W
- Next: M-H

Figure 60 : Activation de la détection de vulnérabilités



```
GNU nano 6.2                               /var/ossec/etc/ossec.conf *
```

```
<!-- SUSE OS vulnerabilities -->
<provider name="suse">
  <enabled>yes</enabled>
  <os>11-server</os>
  <os>11-desktop</os>
  <os>12-server</os>
  <os>12-desktop</os>
  <os>15-server</os>
  <os>15-desktop</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Arch OS vulnerabilities -->
<provider name="arch">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
</provider>

<!-- Alma Linux OS vulnerabilities -->
<provider name="almalinux">
  <enabled>yes</enabled>
  <os>8c</os>
  <os>9c</os>
  <update_interval>1h</update_interval>
</provider>

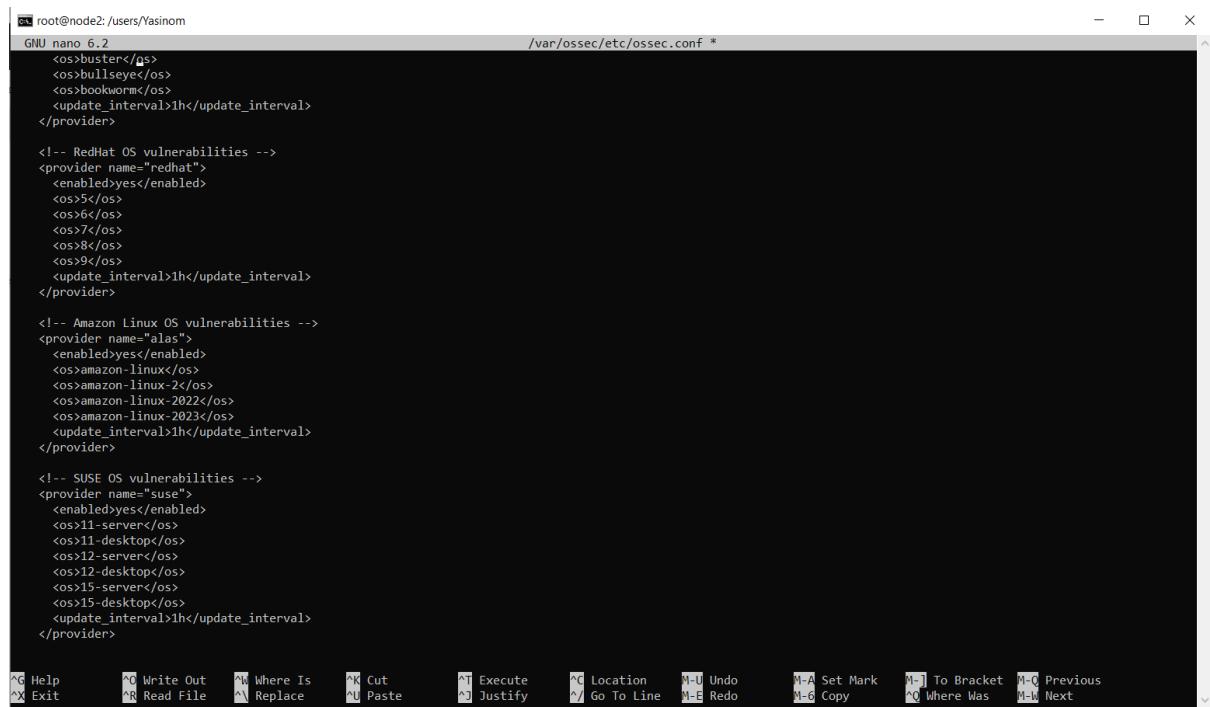
<!-- Windows OS vulnerabilities -->
<provider name="msu">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
</provider>

<!-- Aggregate vulnerabilities -->
<provider name="nvd">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
</provider>

</vulnerability-detector>
```

File menu: Help, Write Out, Where Is, Cut, Execute, Location, Undo, Set Mark, To Bracket, Previous, Next, Exit, Read File, Replace, Paste, Justify, Go To Line, Undo, Redo, Copy, Where Was, Next.

Figure 61 : Activation de la détection de vulnérabilités



```
GNU nano 6.2                               /var/ossec/etc/ossec.conf *
```

```
<!-- buster OS vulnerabilities -->
<provider name="buster">
  <os>bullseye</os>
  <os>bookworm</os>
  <update_interval>1h</update_interval>
</provider>

<!-- RedHat OS vulnerabilities -->
<provider name="redhat">
  <enabled>yes</enabled>
  <os>5c</os>
  <os>6c</os>
  <os>7c</os>
  <os>8c</os>
  <os>9c</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Amazon Linux OS vulnerabilities -->
<provider name="alas">
  <enabled>yes</enabled>
  <os>amazon-linux</os>
  <os>amazon-linux-2</os>
  <os>amazon-linux-2022</os>
  <os>amazon-linux-2023</os>
  <update_interval>1h</update_interval>
</provider>

<!-- SUSE OS vulnerabilities -->
<provider name="suse">
  <enabled>yes</enabled>
  <os>11-server</os>
  <os>11-desktop</os>
  <os>12-server</os>
  <os>12-desktop</os>
  <os>15-server</os>
  <os>15-desktop</os>
  <update_interval>1h</update_interval>
</provider>
```

File menu: Help, Write Out, Where Is, Cut, Execute, Location, Undo, Set Mark, To Bracket, Previous, Next, Exit, Read File, Replace, Paste, Justify, Go To Line, Undo, Redo, Copy, Where Was, Next.

Figure 62 : Activation de la détection de vulnérabilités

Maintenant on Configure les fichiers de groupe d'agents :

Figure 63 : Configuration des fichiers de groupe d'agents

Figure 64 : Configuration des fichiers de groupe d'agents

```

<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>
<localfile>
  <log_format>full_command</log_format>
  <command>netsat -tan | grep LISTEN | grep -v 127.0.0.1 | sort</command>
  <frequency>360</frequency>
</localfile>
<localfile>
  <log_format>full_command</log_format>
  <command>last -n 5</command>
  <frequency>360</frequency>
</localfile>
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>24h</interval>
  <scan_on_start>yes</scan_on_start>
  <packages>yes</packages>
  <osyes>os</os>
  <hotfixes>yes</hotfixes>
  <ports all="no">yes</ports>
  <processes>yes</processes>
</wodle>
</agent_config>

```

Figure 65 : Configuration des fichiers de groupe d'agents

Ce fichier peut être copié sur :

LINUX :

```
https://gist.github.com/taylorwalton/93868507d72b3d40ad2e1318d5983e77/raw/be4f6457c5f60dd04d098cac57754422beef88de/linux%20agent%20group
```

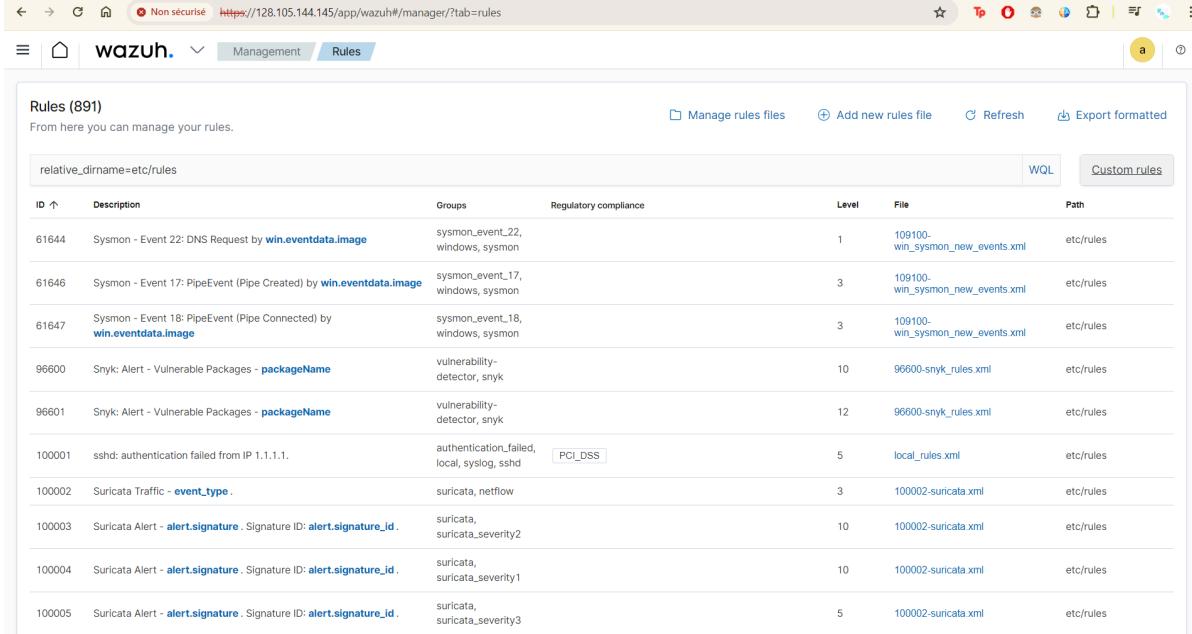
WINDOWS :

```
https://gist.github.com/taylorwalton/db7035a2bd248c7ce0960c6a4ea1510b/raw/8589f43fd66106f9a52530e62b37c751eb6fa  
c7c/windows%20agent%20group
```

```
systemctl restart wazuh-manager
```

Maintenant, on va ajouter des règles de détection avancées personnalisées par **SocFortress**, avec la commande :

```
curl -so ~/wazuh_socfortress_rules.sh  
https://raw.githubusercontent.com/socfortress/Wazuh-Rules/main/wazuh\_socfortress\_rules.sh && bash ~/wazuh_socfortress_rules.sh
```



The screenshot shows the Wazuh Rules management interface. At the top, there's a navigation bar with tabs for Management and Rules. Below the navigation, a header reads "Rules (891)" and "From here you can manage your rules." On the right side of the header are buttons for "Manage rules files", "Add new rules file", "Refresh", and "Export formatted". A search bar labeled "relative dirname=etc/rules" is positioned above a table. The table has columns: ID, Description, Groups, Regulatory compliance, Level, File, and Path. There are 10 rows of data listed:

ID	Description	Groups	Regulatory compliance	Level	File	Path
61644	Sysmon - Event 22: DNS Request by win.eventdata.image	sysmon_event_22, windows, sysmon		1	109100-win_sysmon_new_events.xml	etc/rules
61646	Sysmon - Event 17: PipeEvent (Pipe Created) by win.eventdata.image	sysmon_event_17, windows, sysmon		3	109100-win_sysmon_new_events.xml	etc/rules
61647	Sysmon - Event 18: PipeEvent (Pipe Connected) by win.eventdata.image	sysmon_event_18, windows, sysmon		3	109100-win_sysmon_new_events.xml	etc/rules
96600	Snyk: Alert - Vulnerable Packages - packageName	vulnerability-detector, snyk		10	96600-snyk_rules.xml	etc/rules
96601	Snyk: Alert - Vulnerable Packages - packageName	vulnerability-detector, snyk		12	96600-snyk_rules.xml	etc/rules
100001	sshd: authentication failed from IP 1.1.1.1.	authentication_failed, local, syslog, sshd	PCI_DSS	5	local_rules.xml	etc/rules
100002	Suricata Traffic - event_type .	suricata, netflow		3	100002-suricata.xml	etc/rules
100003	Suricata Alert - alert.signature . Signature ID: alert.signature_id .	suricata, suricata_severity2		10	100002-suricata.xml	etc/rules
100004	Suricata Alert - alert.signature . Signature ID: alert.signature_id .	suricata, suricata_severity1		10	100002-suricata.xml	etc/rules
100005	Suricata Alert - alert.signature . Signature ID: alert.signature_id .	suricata, suricata_severity3		5	100002-suricata.xml	etc/rules

Figure 66 : Règles de détection avancées personnalisées ajoutée

VI. Surveillance du système:

On commence par créer les extracteurs pour les JSON arrivés sur Graylog depuis Wazuh :

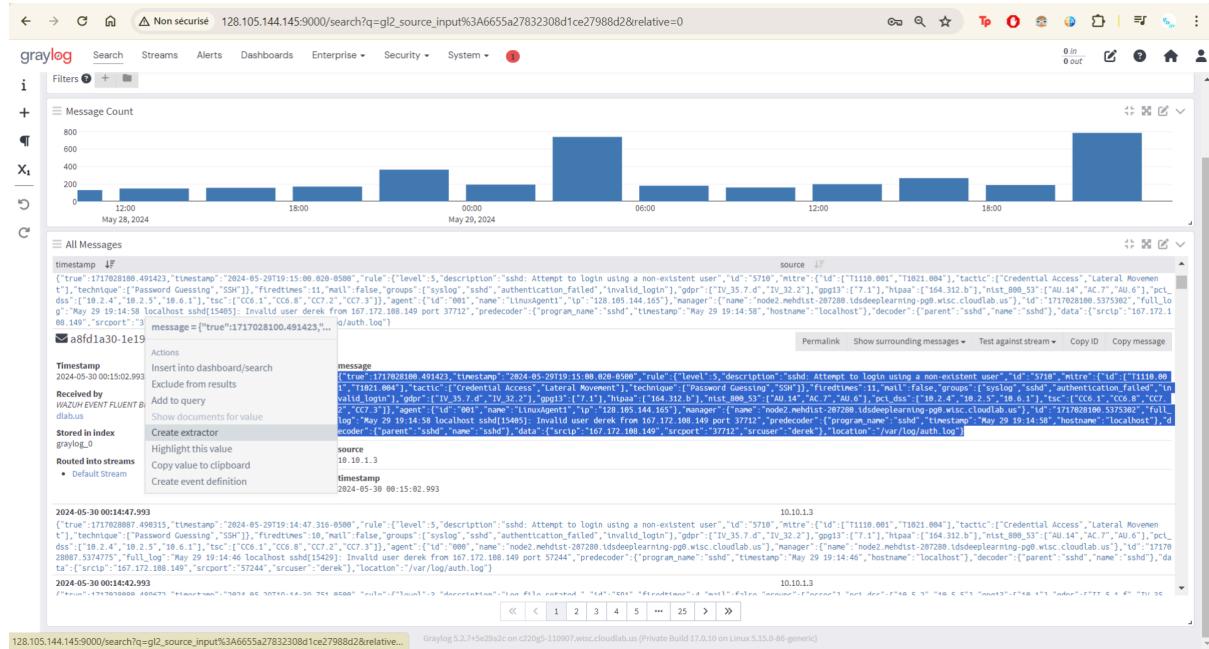


Figure 67 : Création des extracteurs des champs

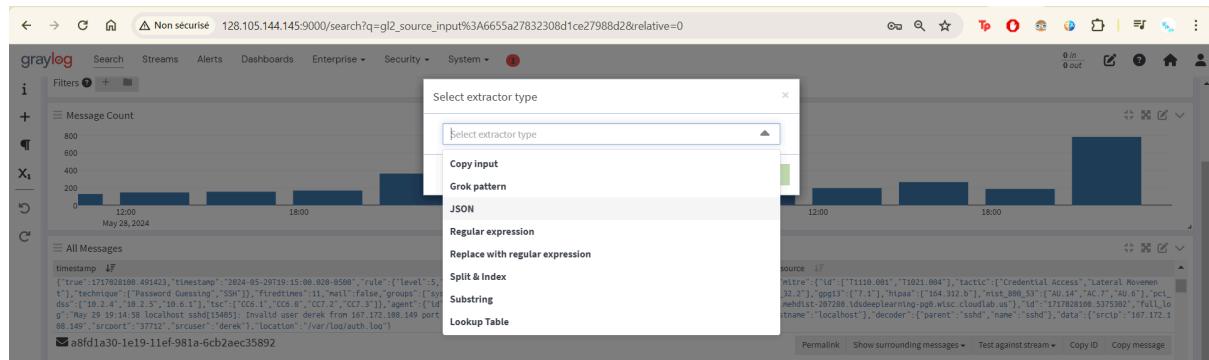


Figure 68 : Création des extracteurs des champs

New extractor for input **WAZUH EVENT FLUENT BIT - TCP**

Extractors are applied on every message that is received by an input. Use them to extract and transform any text data into fields that allow you easy filtering and analysis later on.

Example message

```
[{"true":1717028108.491423,"timestamp":"2024-05-29T19:15:00.020-0500","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":[{"id":["T1119.001","T1021.004"]}], "tactic":["Credential Access","Lateral Movement"],"technique":["Password Guessing","SSH"]}, "fireddtimes":11,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"], "gdrp":["IV_35.7.d","IV_32.2"], "gpg13":["7.1"], "htpaa": [{"id":164.312.b"}],"nist_800_53": ["AU_14","AC_7","AU_6"],"pcl_das": ["10.2.4","10.2.5","10.6.1"]}, "tsc": ["CC6.1","CC6.8","CC7.2","CC7.3"], "agent": {"id": "001", "name": "LinuxAgent1", "ip": "128.105.144.145"}, "manager": {"name": "node2.mehdist-207280.tdsdeeplearning-pg8.wtsc.cloudlab.us"}, "id": "1717028108.5375302"}, "full_log": "May 29 19:14:58 localhost sshd[15405]: Invalid user derek from 167.172.108.149 port 37712", "decoder": {"parent": "sshd", "name": "sshd"}, "data": {"srcip": "167.172.108.149", "srcport": "37712", "srcuser": "derek"}, "location": "/var/log/auth.log"}]
```

Wrong example? [Load another message](#)

Extractor configuration

Extractor type: JSON

Source field: message

Flatten structures
Whether to flatten JSON objects into a single message field or to expand into multiple fields.

List item separator: ,
What string to use to concatenate items of a JSON list.

Key separator: -
What string to use to concatenate different keys of a nested JSON object (only used if not flattened).

Key/value separator: :
What string to use when concatenating key/value pairs of a JSON object (only used if flattened).

Key prefix:
Text to prepend to each key extracted from the JSON object.

Replace whitespaces in keys
Field keys containing whitespaces will be discarded when storing the extracted message. Check this box to replace whitespaces in JSON keys with another character.

Key whitespace replacement: -
What character to use when replacing whitespaces in message keys. Please ensure the replacement character is valid in Lucene, e.g. '-' or '_'.
Try: agent_id, 001, agent_name, LinuxAgent1, decoder_parent, sshd, rule_tsc, CC6.1, CC6.8, CC7.2, CC7.3, rule_gdrp, IV_35.7.d, IV_32.2, rule_level, 5, rule_mitre_technique, Password Guessing, SSH, rule_fireddtimes, 11, full_log, May 29 19:14:58 localhost sshd[15405]: Invalid user derek from 167.172.108.149 port 37712, decoder_program_name, sshd, rule_mail, rule_pcl_das, 10.2.4, 10.2.5, 10.6.1, rule_nist_800_53, AU_14, AU_7, AU_6, decoder_timestamp, May 29 19:14:58, decoder_name, sshd, rule_description, sshd: Attempt to login using a non-existent user, id, 1717028108.5375302, timestamp, 2024-05-29T19:15:00.020-0500, rule_mitre_tactic, Credential Access, Lateral Movement, rule_mitre_id

Extractors documentation [?](#)

Figure 69 : Crédation des extracteurs des champs

Extractor preview

```
agent_id
001
agent_name
LinuxAgent1
decoder_parent
sshd
rule_tsc
CC6.1, CC6.8, CC7.2, CC7.3
rule_gdrp
IV_35.7.d, IV_32.2
rule_level
5
rule_mitre_technique
Password Guessing, SSH
rule_fireddtimes
11
full_log
May 29 19:14:58 localhost sshd[15405]: Invalid user derek from 167.172.108.149 port 37712
decoder_program_name
sshd
rule_mail
rule_pcl_das
10.2.4, 10.2.5, 10.6.1
rule_nist_800_53
AU_14, AU_7, AU_6
decoder_timestamp
May 29 19:14:58
decoder_name
sshd
rule_description
sshd: Attempt to login using a non-existent user
id
1717028108.5375302
timestamp
2024-05-29T19:15:00.020-0500
rule_mitre_tactic
Credential Access, Lateral Movement
rule_mitre_id
```

Figure 70 : Crédation des extracteurs des champs

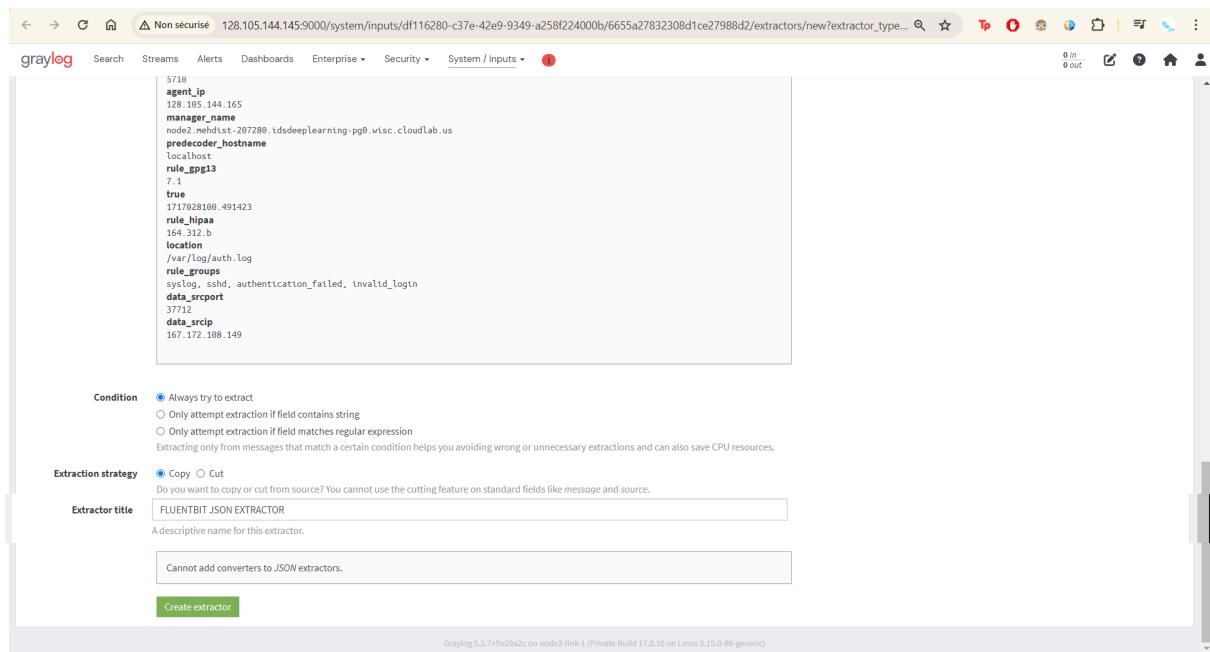


Figure 71 : Crédation des extracteurs des champs

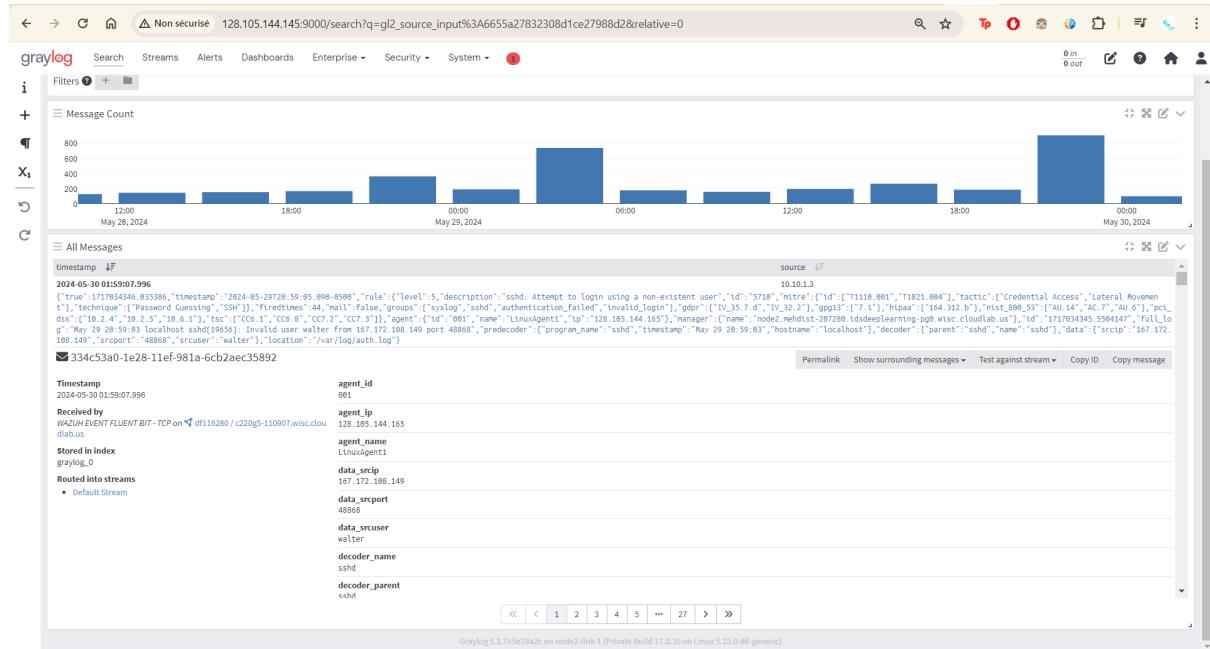


Figure 72 : Crédation des extracteurs des champs

Nous passons maintenant à la création de l'index :

The screenshot shows the 'Indices & Index Sets' section of the Graylog web interface. It lists several index sets:

- Graylog Events**: Stores Graylog events. Configuration: Index prefix: gl-events, Shards: 1, Replicas: 0, Field type refresh interval: 5 seconds. Index rotation strategy: Index Time Size Optimizing, Minimum lifetime: P30D (30 days), Maximum lifetime: P40D (40 days). Index retention strategy: Delete, Max number of indices: 20.
- Graylog Investigation Events**: Stores Graylog Investigation Events. Configuration: Index prefix: investigation_event_index, Shards: 1, Replicas: 0, Field type refresh interval: 5 seconds. Index rotation strategy: Index Time Size Optimizing, Minimum lifetime: P30D (30 days), Maximum lifetime: P40D (40 days). Index retention strategy: Delete, Max number of indices: 20.
- Graylog Investigation Messages**: Configuration: Index prefix: 128.105.144.145:9000/system/index_sets/create, Shards: 1, Replicas: 0, Field type refresh interval: 5 seconds. Index rotation strategy: Index Time Size Optimizing, Minimum lifetime: P30D (30 days), Maximum lifetime: P40D (40 days). Index retention strategy: Delete, Max number of indices: 20.

Figure 73 : Crédation des Indexes

The screenshot shows the 'Create Index Set' form. The fields are as follows:

- Title**: WAZUH ALERTS
- Description**: WAUH ALERTS
- Index prefix**: wazuh-alerts-gatosoc
- Analyzer**: standard
- Index shards**: 1
- Index replicas**: 0
- Max. number of segments**: 1
- Index optimization after rotation**: Disable index optimization after rotation
- Field type refresh interval**: 5 seconds

Below the form is a note about index rotation and a dropdown for selecting the rotation strategy.

Figure 74 : Crédation des Indexes

Index shards: 1
 Index replicas: 0
 Max. number of segments: 1
 Index optimization after rotation: Disable index optimization after rotation
 Field type refresh interval: 5 seconds

Index Rotation Configuration:
 Select rotation strategy: Index Size
 Max size per index (in bytes): 10737418240 (10.06GB)

Index Retention Configuration:
 Select retention strategy: Delete Index
 Max number of indices: 10

Figure 75 : Création des Indexes

Nous passons maintenant à la création du Stream.

Description	Index Set	Rules	Throughput	Status	Actions
Stream containing all events created by Graylog	Graylog Events	0	0 msg/s	Running	<input type="button" value="Share"/> <input type="button" value="More"/>
Stream containing all Graylog Investigation events	Graylog Investigation Events	0	0 msg/s	Running (II)	<input type="button" value="Share"/> <input type="button" value="More"/>
Stream containing all Graylog Investigation messages	Graylog Investigation Messages	0	0 msg/s	Running (II)	<input type="button" value="Share"/> <input type="button" value="More"/>
Stream containing all system events created by Graylog	Graylog System Events	0	0 msg/s	Running	<input type="button" value="Share"/> <input type="button" value="More"/>
Contains messages that are not explicitly routed to other streams	Default index set	0	0 msg/s	Running	<input type="button" value="Share"/> <input type="button" value="More"/>
Stream containing messages that failed to be processed or indexed	Graylog Message Failures	0	0 msg/s	Running	<input type="button" value="Share"/> <input type="button" value="More"/>

Figure 76 : Création du Stream

Create stream

Title: WAZUH ALERTS
 Description (Opt.): WAZUH ALERTS
 Index Set: WAZUH ALERTS
 Remove matches from 'Default Stream'

Cancel Create stream

Figure 77 : Création du Stream

Inputs

Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

Select input ▾ Launch new input Find more inputs

Filter by title

Global inputs 0 configured

There are no global inputs.

Local inputs 1 configured

WAZUH EVENT FLUENT BIT - TCP Raw/PlainText TCP (6655a27882308d1ce27988d2) WARNING

On node ★ d11c6280 / c2020gs-110907.wisc.cloudlab.us

```
bind_address: 0.0.0.0
charset_name: UTF-8
max_message_size: 2097152
number_worker_threads: 48
override_source: <empty>
port: 5555
recv_buffer_size: 1048576
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password: *****
use_null_delimiter: false
```

Show received messages Manage extractors Stop input More actions ▾

Throughput / Metrics

1 minute average rate: 0 msg/s
Network IO: ▼ 0B ▲ 0B (total: ▼ 1.8MB ▲ 0B)
Active connections: 0 (361 total)
Empty messages discarded: 1

Edit input Show metrics Add static field Delete input

Figure 78 : Création du Stream

Add static field

Define a static field that is added to every message that comes in via this input. The field is not overwritten if the message already has that key. Key must only contain alphanumeric characters or underscores and not be a reserved field.

Field name log_type

Field value wazuh

Cancel Add field

Figure 79 : Création du Stream

Streams

You can route incoming messages into streams by applying rules against them. Messages matching the rules of a stream are routed into it. A message can also be routed into multiple streams.

Streams documentation Create stream

Enter search query...	Filters +	Actions				
		Description ↗	Index Set ↗	Rules	Throughput	Status ↗
<input type="checkbox"/> Title ↑	All events	Stream containing all events created by Graylog	Graylog Events	0 msg/s	Running	Share More ▾
<input type="checkbox"/> All Investigation events	All Investigation events	Stream containing all Graylog Investigation events	Graylog Investigation Events	0 msg/s	Running ⓘ	Share More ▾
<input type="checkbox"/> All Investigation messages	All Investigation messages	Stream containing all Graylog Investigation messages	Graylog Investigation Messages	0 msg/s	Running ⓘ	Share More ▾
<input type="checkbox"/> All system events	All system events	Stream containing all system events created by Graylog	Graylog System Events	0 msg/s	Running	Share More ▾
<input type="checkbox"/> Default Stream Default	Contains messages that are not explicitly routed to other streams	Default index set	0 msg/s	Running	Share More ▾	
<input type="checkbox"/> Processing and Indexing failures	Processing and Indexing failures	Graylog Message Failures	0 msg/s	Running	Share More ▾	
<input type="checkbox"/> WAZUH ALERTS	WAZUH ALERTS	WAZUH ALERTS	0 msg/s	Paused ⓘ	Share More ▾	

Show 20 Rows ▾ Columns ▾

Start Stream Quick add rule Edit stream

Manage Rules Manage Outputs Manage Alerts

Set as startpage Clone this stream Delete this stream

Figure 80 : Création du Stream

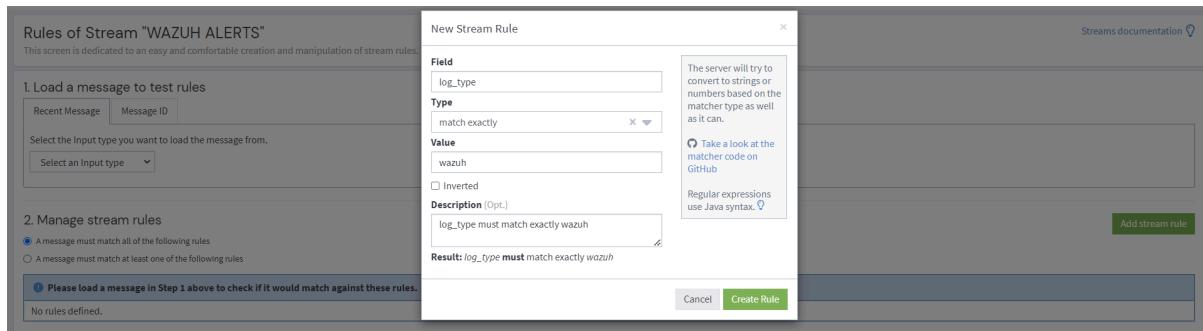


Figure 81 : Crédation du Stream

Cliquez sur le bouton de lecture pour démarrer le flux :

Title	Description	Index Set	Rules	Throughput	Status	Actions
All events	Stream containing all events created by Graylog	Graylog Events	0	0 msg/s	Running	Share More
All Investigation events	Stream containing all Graylog Investigation events	Graylog Investigation Events	0	0 msg/s	Running	Share More
All Investigation messages	Stream containing all Graylog Investigation messages	Graylog Investigation Messages	0	0 msg/s	Running	Share More
All system events	Stream containing all system events created by Graylog	Graylog System Events	0	0 msg/s	Running	Share More
Default Stream	Contains messages that are not explicitly routed to other streams	Default index set	0	0 msg/s	Running	Share More
Processing and Indexing Failures	Stream containing messages that failed to be processed or indexed	Graylog Message Failures	0	0 msg/s	Running	Share More
WAZUH ALERTS	WAZUH ALERTS	WAZUH ALERTS	1	0 msg/s	Paused	Share More

Figure 82 : Lancement du Stream

VII. Configuration de Grafana : Tableaux de bord SIEM open source

Grafana est l'outil de visualisation parfait pour visualiser nos événements de sécurité. Kibana (Wazuh-Dashboards) peut également être utilisé pour visualiser nos données, mais au fil des ans, je n'ai pas été impressionné par les visualisations de Kibana, sa difficulté à personnaliser, le manque de sources de données uniques et sa vitesse globale. À mon avis, Grafana est le meilleur outil de visualisation pour toutes les piles SIEM :

On commence par installer ces exigences :

```
- sudo apt-get install -y apt-transport-https
- sudo apt-get install -y software-properties-common wget
- sudo wget -q -O /usr/share/keyrings/grafana.key
https://apt.grafana.com/gpg.key
```

```

- echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://apt.grafana.com stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
- sudo apt-get update
- sudo apt-get install grafana

```

Et sur /etc/grafana/grafana.ini , Nous avons effectué les changements suivants :

- Passer de HTTP à HTTPS
- Changer le port HTTP en 3000
- Modifier le domaine en : grafana.gatosoc.co

```

root@node2:/users/Yasinom
GNU nano 6.2                               /etc/grafana/grafana.ini *
#####
## Server #####
[server]
# Protocol (http, https, h2, socket)
protocol = https

# This is the minimum TLS version allowed. By default, this value is empty. Accepted values are: TLS1.2, TLS1.3. If nothing is set TLS1.2 would be used.
;min_tls_version = ""

# The ip address to bind to, empty will bind to all interfaces
;http_addr =

# The http port to use
http_port = 3000

# The public facing domain name used to access grafana from a browser
domain = grafana.gatosoc.co

# Redirect to correct domain if host header does not match domain
# Prevents DNS rebinding attacks
;enforce_domain = false

# The full public facing url you use in browser, used for redirects and emails
# If you use reverse proxy and sub path specify full url (with sub path)
;root_url = %(protocol)s://%(domain)s:%(http_port)s/

# Serve Grafana from subpath specified in `root_url` setting. By default it is set to `false` for compatibility reasons.
;serve_from_sub_path = false

# Log web requests
;router_logging = false

# the path relative working path
;static_root_path = public

# enable gzip
;enable_gzip = false

# https certs & key file
;cert_file = /etc/ssl/certs/node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us.pem
;cert_key = /etc/ssl/private/node2.mehdist-207280.idsdeeplearning-pg0.wisc.cloudlab.us-key.pem

```

Figure 83 : Configuration de grafana.ini

Et enfin, on active le service :

```

- systemctl enable grafana-server
- systemctl start grafana-server

```

Et on se rend sur l'interface Web Grafana:

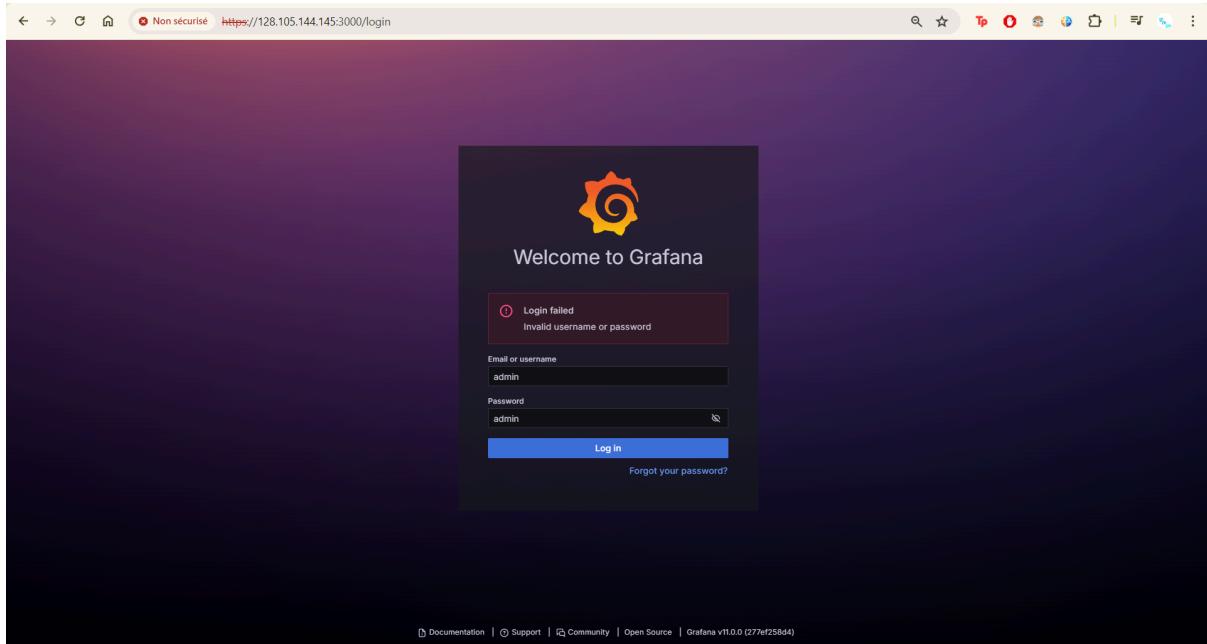


Figure 84 : Interface Web grafana

Et on change notre mdp :

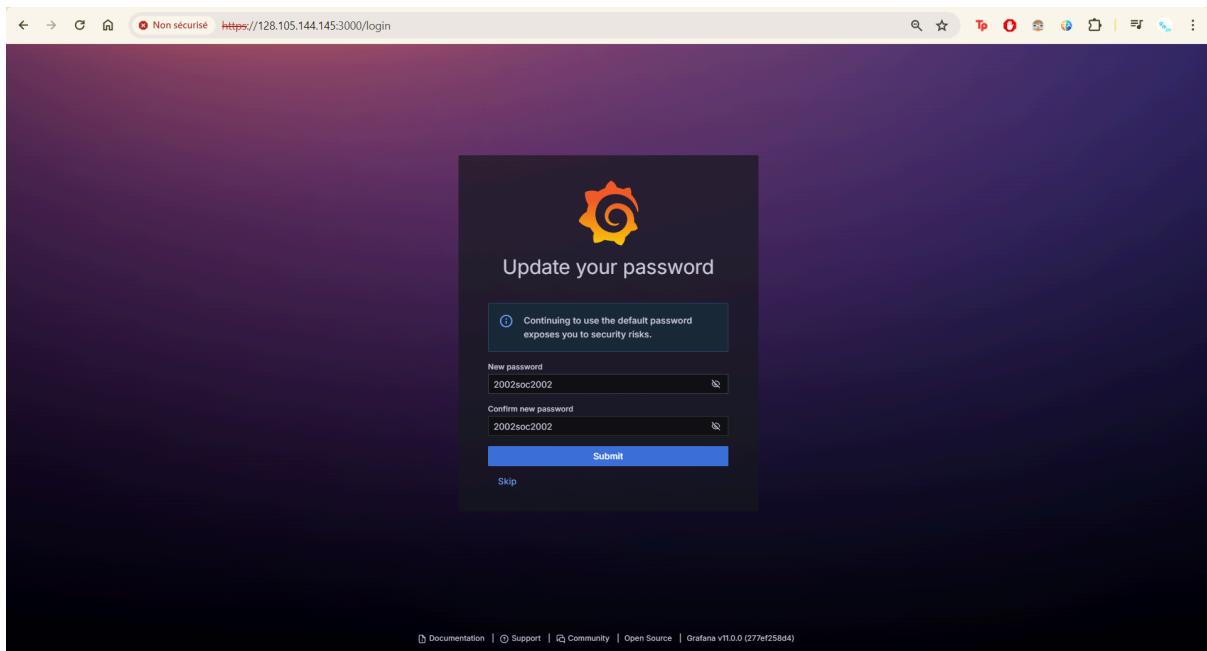


Figure 85 : Interface Web grafana

Ensuite on ajoute notre **Datasource Wazuh (Elasticsearch)** :

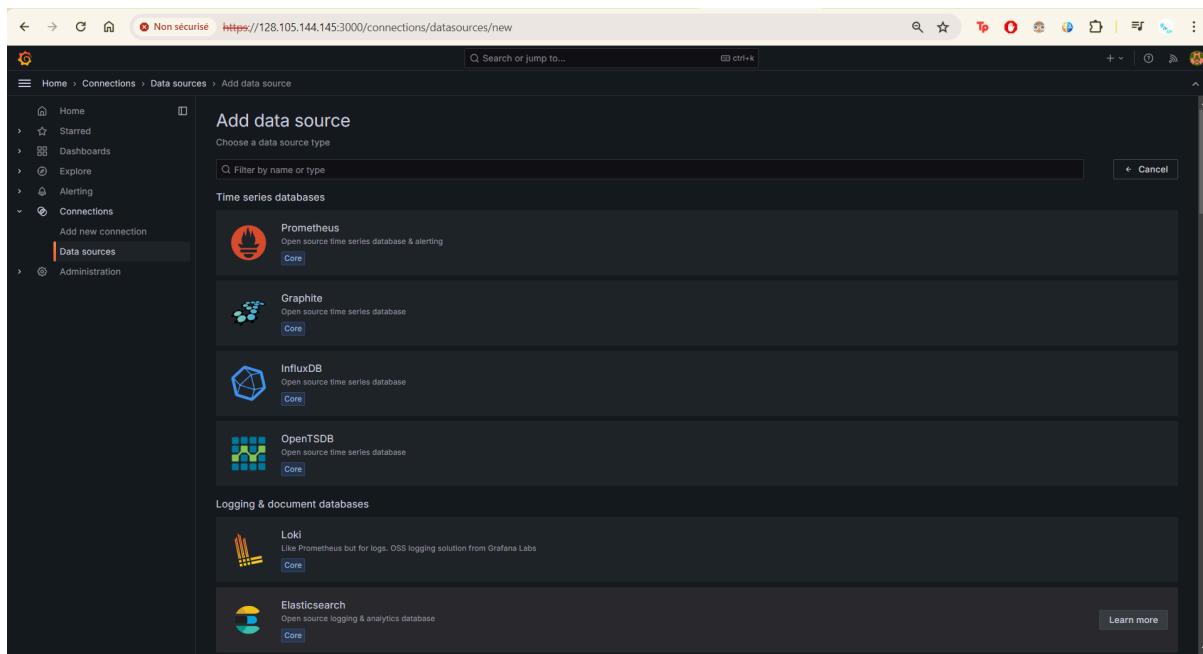


Figure 86 : Ajout de la Datasource

Simultanément, nous ajoutons un rôle sur le gestionnaire Wazuh pour Grafana.

Role	Cluster permissions	Index permissions	Internal users	Backend roles	Tenants	Customization
asynchronous_search_read_access	cluster:admin/opendistro/asynchronous_search/get	—	—	—	—	Reserved
readall_and_monitor	cluster_monitor cluster_composite_ops_no	*	—	—	—	Reserved
kibana_user	cluster_composite_ops	.kibana .kibana-6 .kibana_*	—	kibanauser	—	Reserved
own_index	cluster_composite_ops	\$user_name)	*	—	—	Reserved
kibana_read_only	—	—	—	—	—	Reserved
alerting_full_access	cluster_monitor cluster:admin/opendistro/alerting/*	*	—	—	—	Reserved

Figure 87 : Ajout du rôle grafana

Create Role

Roles are the core way of controlling access to your cluster. Roles contain any combination of cluster-wide permission, index-specific permissions, document- and field-level security, and tenants. Once you've created the role, you can map users to the roles so that users gain those permissions. [Learn more](#)

Name
Specify a descriptive and unique role name. You cannot edit the name once the role is created.

grafana_role

The role name must contain from 2 to 50 characters. Valid characters are A-Z, a-z, 0-9, _, underscore, (-) hyphen and unicode characters.

Cluster permissions
Specify how users in this role can access the cluster. By default, no cluster permission is granted. [Learn more](#)

Cluster Permissions
Specify permissions using either action groups or single permissions. An action group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.

indices_all x read x kibana_all_read x Create new permission group

Index permissions
Index permissions allow you to specify how users in this role can access the specific indices. By default, no index permission is granted. [Learn more](#)

✓ *

Index
Specify index pattern using *

Remove

Specify index pattern using *

Index permissions
You can specify permissions using both action groups or single permissions. A permission group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.

index x read x indices_all x Create new permission group

Document level security - optional
You can restrict a role to a subset of documents in an index. [Learn more](#)

{
 "bool": {
 "must": {
 "match": {
 "genres": "Comedy"
 }
 }
 }
}

Figure 88 : Ajout du rôle grafana

Specify index pattern using *

Index permissions
You can specify permissions using both action groups or single permissions. A permission group is a list of single permissions. You can often achieve your desired security posture using some combination of the default permission groups. You can also create your own reusable permission groups.

index x read x indices_all x Create new permission group

Document level security - optional
You can restrict a role to a subset of documents in an index. [Learn more](#)

{
 "bool": {
 "must": {
 "match": {
 "genres": "Comedy"
 }
 }
 }
}

Field level security - optional
You can restrict what document fields a user can see. If you use field-level security in conjunction with document-level security, make sure you don't restrict access to the field that document-level security uses.

Exclude Type in field name

Anonymization - optional
Masks any sensitive fields with a random value to protect your data security.

Type in field name

Add another index permission

Tenant permissions
Tenants are useful for safely sharing your work with other OpenSearch Dashboards users. You can control which roles have access to a tenant and whether those roles have read and/or write access. [Learn more](#)

Tenant

Search tenant name or add a tenant pattern Read and Write Remove

Add another tenant permission

Cancel Create

Figure 89 : Ajout du rôle grafana

Maintenant on crée un utilisateur interne :

Create internal user

The security plugin includes an internal user database. Use this database in place of, or in addition to, an external authentication system such as LDAP or Active Directory. [Learn more](#)

Credentials

Username
Specify a descriptive and unique user name. You cannot edit the name once the user is created.

Password

Password should be at least 8 characters long and contain at least one uppercase letter, one lowercase letter, one digit, and one special character.

Re-enter password

The password must be identical to what you entered above.

Backend roles - optional
Backend roles are used to map users from external authentication systems, such as LDAP or SAML, to OpenSearch security roles. [Learn more](#)

Backend role

[Add another backend role](#)

Attributes - optional
Attributes can be used to further describe the user, and, more importantly they can be used as variables in the Document Level Security query in the index permission of a role. This makes it possible to write dynamic DLS queries based on a user's attributes. [Learn more](#)

Variable name	Value
<input type="text" value="Type in variable name"/>	<input type="text" value="Type in value"/> <input type="button" value="Remove"/>

Figure 90 : Ajout du user grafana

Internal users (3)

The security plugin includes an internal user database. Use this database in place of, or in addition to, an external authentication system such as LDAP server or Active Directory. You can map an internal user to a role from Roles. First, click into the detail page of the role. Then, under "Mapped users", click "Manage mapping". [Learn more](#)

<input type="checkbox"/> Username	Backend roles	Attributes
<input type="checkbox"/> logstash	logstash	—
<input checked="" type="checkbox"/> grafana		—
<input type="checkbox"/> snapshotrestore	snapshotrestore	—
<input type="checkbox"/> graylog	admin	—
<input type="checkbox"/> admin [Current]	admin	—
<input type="checkbox"/> kibanaserver	—	—
<input type="checkbox"/> kibanaro	kibanouser	attribute1: "value1" attribute2: "value2" attribute3: "value3"
<input type="checkbox"/> readall	readall	—

Rows per page: 10 < 1 >

Figure 91 : Ajout du user grafana

Ensuite on Fait correspondre l'utilisateur au rôle:

The screenshot shows the 'Map user' configuration page in Grafana. At the top, there's a navigation bar with tabs: 'Security', 'Roles', 'grafana_role', and 'Map user'. Below the navigation is a section titled 'Map user' with the sub-instruction 'Map users to this role to inherit role permissions. Two types of users are supported: user, and backend role. Learn more'. There are two main sections: 'Users' and 'Backend roles'. In the 'Users' section, there's a search input with 'grafana' typed in, a 'Create new internal user' button, and a note about looking up by user name. In the 'Backend roles' section, there's a search input with 'Type in backend role', a 'Remove' button, and a 'Add another backend role' button. At the bottom right are 'Cancel' and 'Map' buttons.

Figure 92 : Ajout du user grafana

En retournant sur Grafana :

The screenshot shows the 'Connections / Data sources' configuration page for 'WAZUH'. The left sidebar has links for Home, Starred, Dashboards, Explore, Alerting, Connections (which is selected), Data sources (which is highlighted), and Administration. The main area shows a 'WAZUH' data source configuration. It includes fields for 'Name' (set to 'WAZUH'), 'Type' (set to 'Elasticsearch'), and 'URL' (set to 'https://10.10.1.3:9200'). Under 'Authentication', 'Basic authentication' is selected, with 'User' set to 'grafana' and 'Password' masked. Under 'TLS settings', the 'Skip TLS certificate validation' checkbox is checked. Other options like 'Add self-signed certificate' and 'TLS Client Authentication' are available but unchecked.

Figure 93 : Config de la Datasource

The screenshot shows the 'Indices' section of the OpenSearch Index Management interface. On the left, there are two main sections: 'Index Management' and 'Snapshot Management'. The 'Index Management' section contains links for State management policies, Policy managed indices, Data streams, Templates, Aliases, Rollup Jobs, Transform Jobs, and Notification settings. The 'Snapshot Management' section contains links for Snapshot Policies, Snapshots, and Repositories. The main area is titled 'Indices (17)' and displays a table with 17 rows. The columns are: Index, Health, Managed by policy, Status, Total size, Size of primaries, Total documents, Deleted documents, Primaries, and Replicas. Each row represents an index with its name, status (e.g., Green, Open), and various metrics like size and document count.

Index	Health	Managed by policy	Status	Total size	Size of primaries	Total documents	Deleted documents	Primaries	Replicas
wazuh-statistics-2024.23w	Green	No	Open	1.8mb	1.8mb	3032	0	1	0
wazuh-statistics-2024.22w	Green	No	Open	1.3mb	1.3mb	3680	0	1	0
wazuh-monitoring-2024.23w	Green	No	Open	654.9kb	654.9kb	502	0	1	0
wazuh-monitoring-2024.22w	Green	No	Open	469.1kb	469.1kb	399	0	1	0
wazuh-alerts-gatosoc_0	Green	No	Open	56.4mb	56.4mb	50898	0	1	0
wazuh-alerts-4.x-2024.05.27	Green	No	Open	884kb	884kb	234	0	3	0
investigation_message_index_0	Green	No	Open	208b	208b	0	0	1	0
investigation_event_index_0	Green	No	Open	208b	208b	0	0	1	0
graylog_1	Green	No	Open	208b	208b	0	0	1	0
graylog_0	Green	No	Open	3.1mb	3.1mb	3958	0	1	0
gl-system-events_1	Green	No	Open	208b	208b	0	0	1	0
gl-system-events_0	Green	No	Open	10kb	10kb	1	0	1	0
gl-failures_0	Green	No	Open	208b	208b	0	0	1	0
gl-events_0	Green	No	Open	208b	208b	0	0	1	0
opensearch-observability	Green	No	Open	208b	208b	0	0	1	0
opendistro_security	Green	No	Open	78.2kb	78.2kb	10	3	1	0
kibana_1	Green	No	Open	29.5kb	29.5kb	4	1	1	0

Figure 94 : Obtention de l'indice

The screenshot shows the 'Data sources' configuration page for a connection named 'WAZUH'. The left sidebar has a tree view with Home, Starred, Dashboards, Explore, Alerting, Connections (selected), Data sources (selected), and Administration. The main area has tabs for 'HTTP headers' (disabled) and 'Additional settings'. Under 'Additional settings', there are sections for 'Advanced HTTP settings' (Allowed cookies, Timeout) and 'Elasticsearch details' (Index name: wazuh-alerts-gatosoc*, Pattern: No pattern, Time field name: timestamp, Max concurrent Shard Requests: 5, Min time interval: 10s, Include Frozen Indices: checked). Below that is a 'Logs' section (Message field name: rule_description, Level field name: syslog_level) and a 'Data links' section (Field: data_vulnerability_cve\$).

Figure 95 : Config de la Datasource

Figure 96 : Config de la Datasource

On passe maintenant à la **Construction du dashboard** :

Figure 97 : Construction du Dashboard

On crée premièrement un extracteur pour les groupes de règles. Afin d'avoir les **events Sysmon de Windows**.

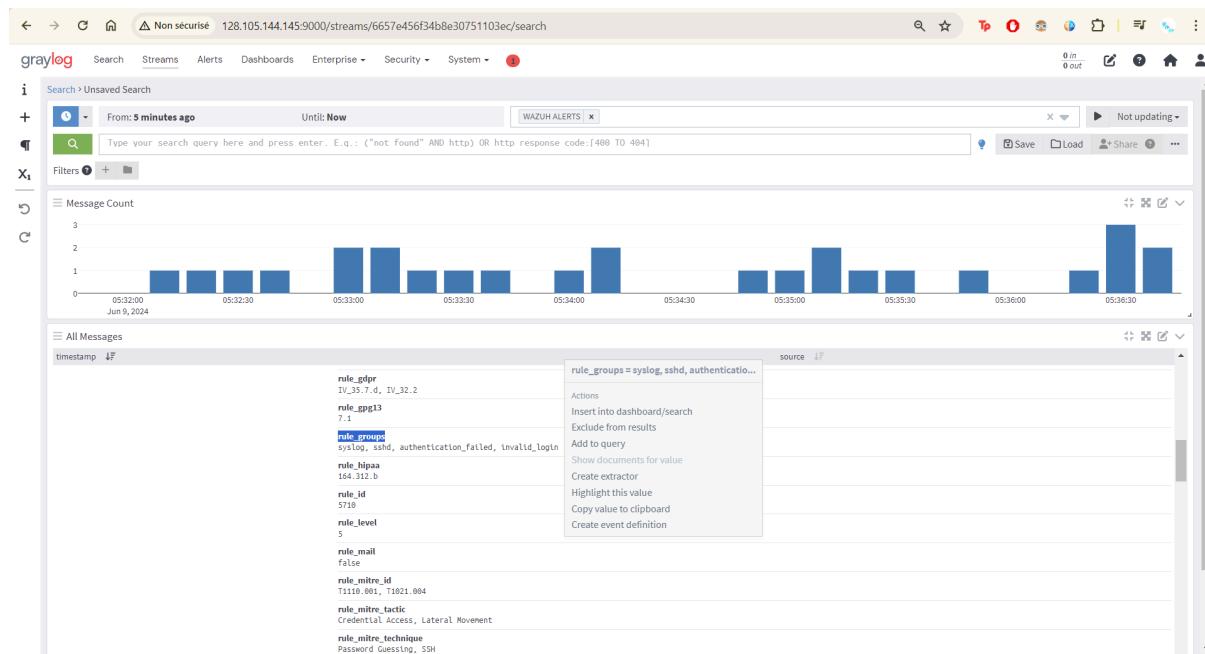


Figure 97 : Extracteur pour les groupes de règles

Pour les champ 1,2 et 3 :

The screenshot shows the configuration of a new extractor for input 'WAZUH EVENT FLUENT BIT - TCP'. The 'Extractor type' is set to 'Split & Index'. The 'Source field' is 'rule_groups'. The 'Split by' field contains a whitespace character. The 'Target index' is '1'. The 'Condition' is set to 'Always try to extract'. The 'Store as field' is 'rule_group1'. The 'Extraction strategy' is 'Copy'. The 'Extractor title' is 'Rule Group 1'. The 'Add converter' section is empty.

Figure 98 : Extracteur du champ 1

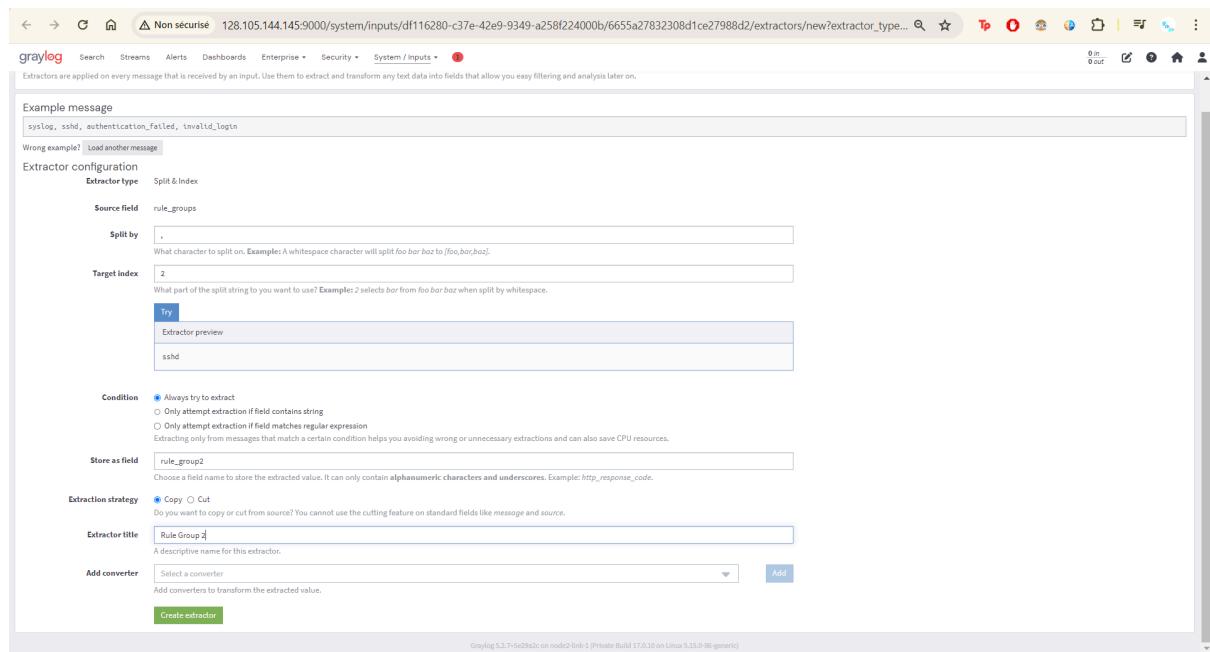


Figure 99 : Extracteur du champ 2

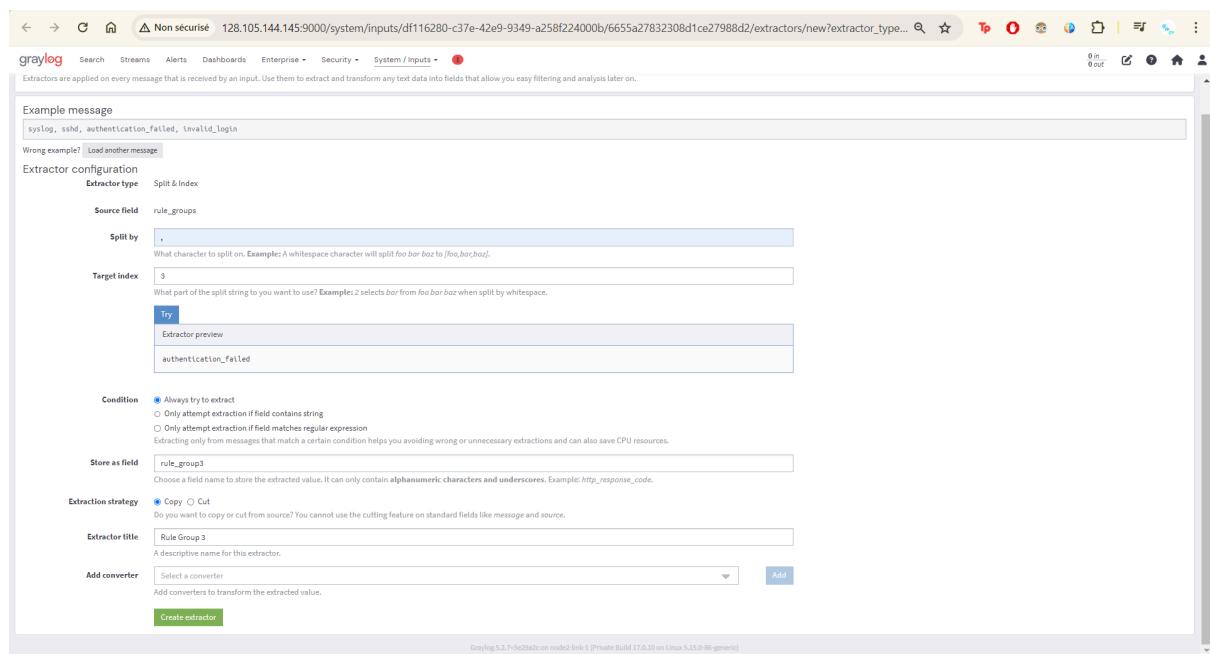


Figure 100 : Extracteur du champ 3

Et voilà nos extractors :

The screenshot shows the Wazuh Extractors interface at the URL <https://128.105.144.145:9000/system/inputs/df116280-c37e-42e9-9349-a258f224000b/6655a27832308d1ce27988d2/extractors>. The page title is "Extractors of WAZUH EVENT FLUENT BIT - TCP". It displays three configured extractors:

- Rule Group 2**: Trying to extract data from `rule_groups` into `rule_group2`, leaving the original intact.
- Rule Group 1**: Trying to extract data from `rule_groups` into `rule_group1`, leaving the original intact.
- Rule Group 3**: Trying to extract data from `rule_groups` into `rule_group3`, leaving the original intact.

Each rule group has "Details", "Edit", and "Delete" buttons.

Figure 100 : Extracteurs du champ 1,2 et 3

Voilà, dans ce cas, notre journal Sysmon est bien séparé et positionné sur le **champ 3**:

The screenshot shows the Wazuh search interface at the URL <https://128.105.144.145:9000/search?q=&rangetype=relative&relative=0>. The interface includes a bar chart titled "Message Count" showing daily message volumes and a detailed view of a selected event titled "All Messages". The event details include:

- rule_description**: Sysmon - Event 3: Network connection by C:\Users\21262\AppData\Local\Discord\app-1.0.9149\Discord.exe
- rule_firetimes**: 34
- rule_group1**: windows
- rule_group2**: sysmon
- rule_group3**: sysmon_event3
- rule_group4**: windows, sysmon
- rule_id**: 102138
- rule_level**: 3
- rule_mall**: false
- rule_mitre_id**: T1030
- rule_mitre_tactic**: Defense Evasion

A context menu is open for the `rule_group3` field, showing options like "Actions", "Insert into dashboard/search", "Exclude from results", "Add to query", "Show documents for value", "Create extractor", "Highlight this value", "Copy value to clipboard", and "Create event definition".

Figure 101 : sysmon_event3 bien conteneurisée

Ensuite on crée notre dashboard :

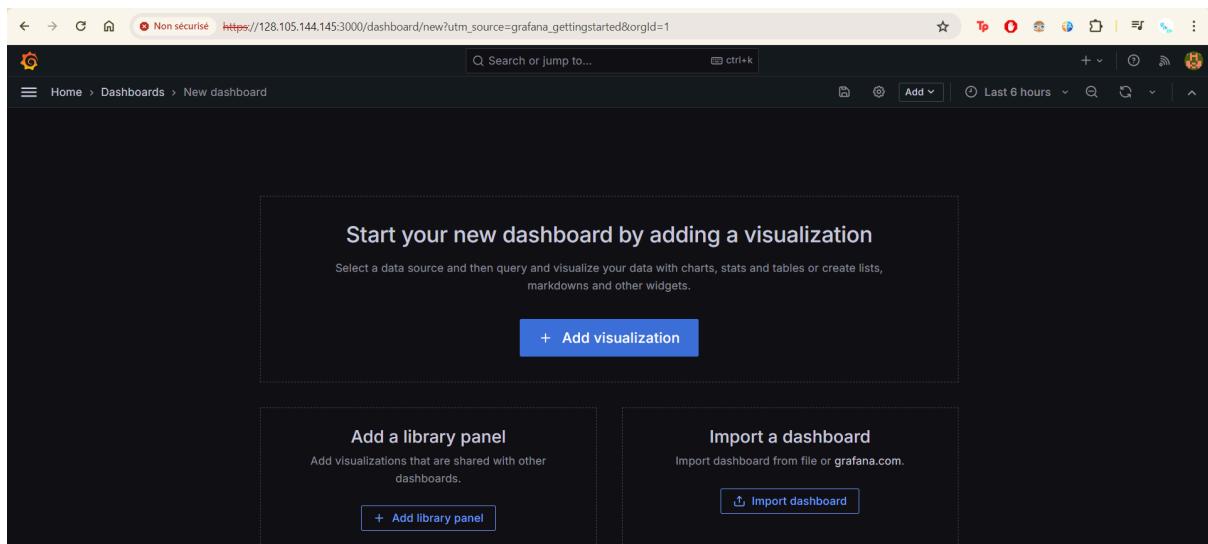


Figure 102 : Construction du Dashboard

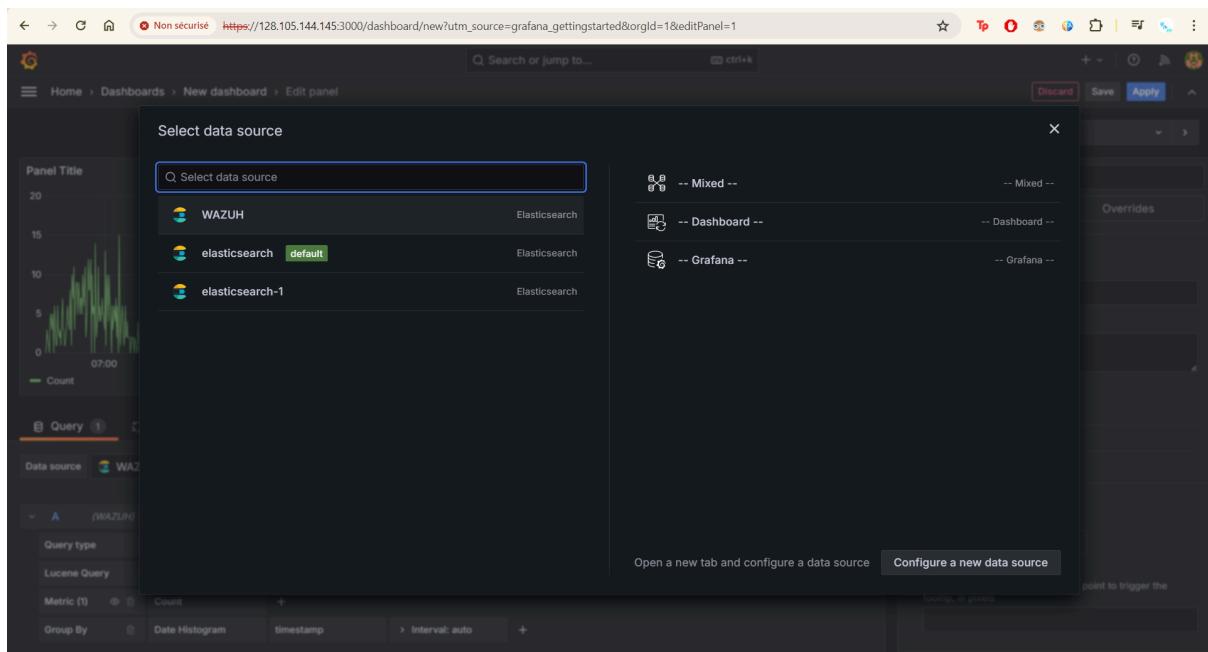


Figure 103 : Construction du Dashboard

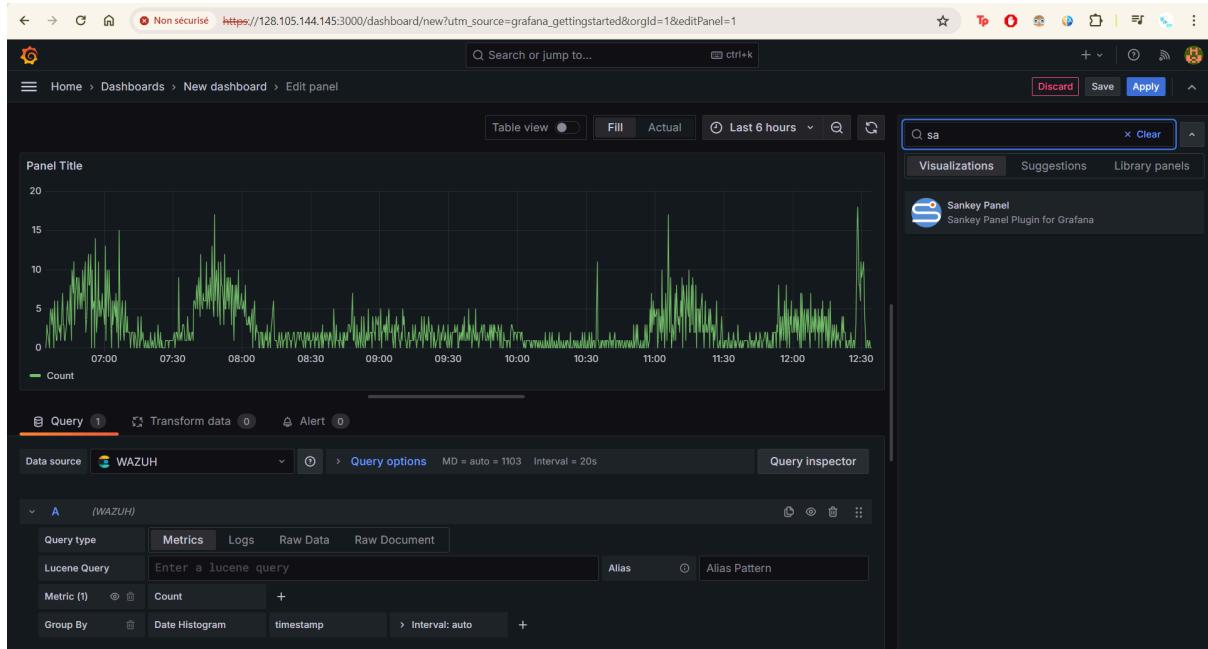


Figure 104 : Construction du Dashboard

On ajoute les champs :

- Adresse IP source
- Adresse IP de destination
- Port

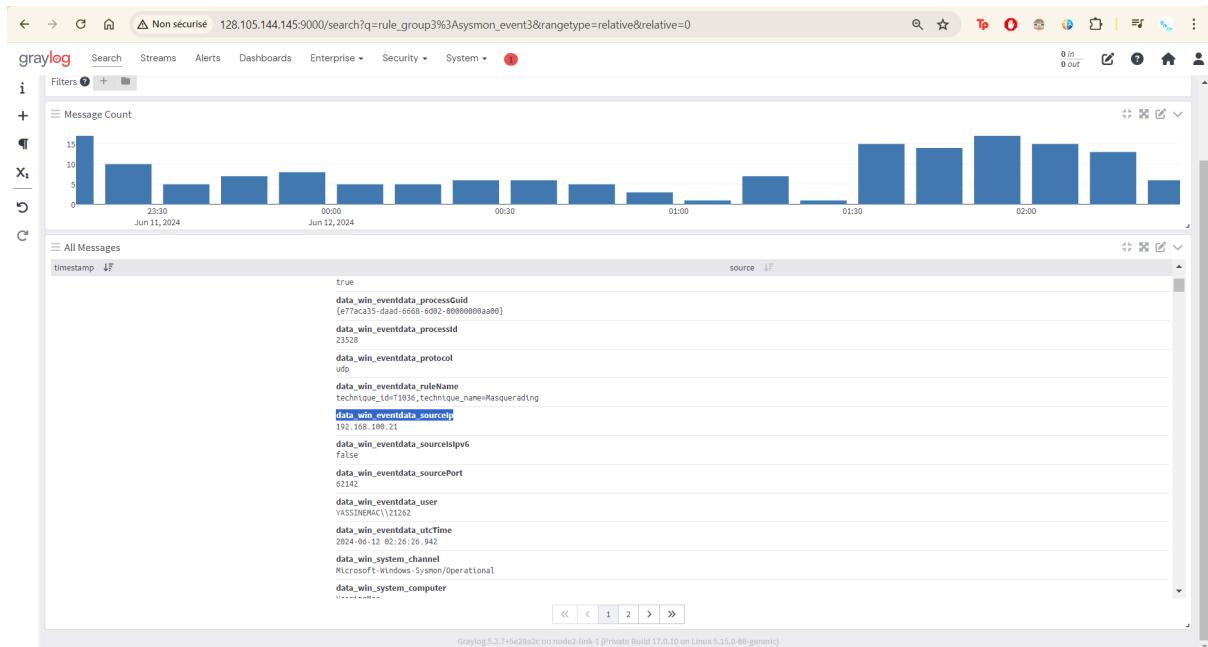


Figure 105 : Source Ip champ

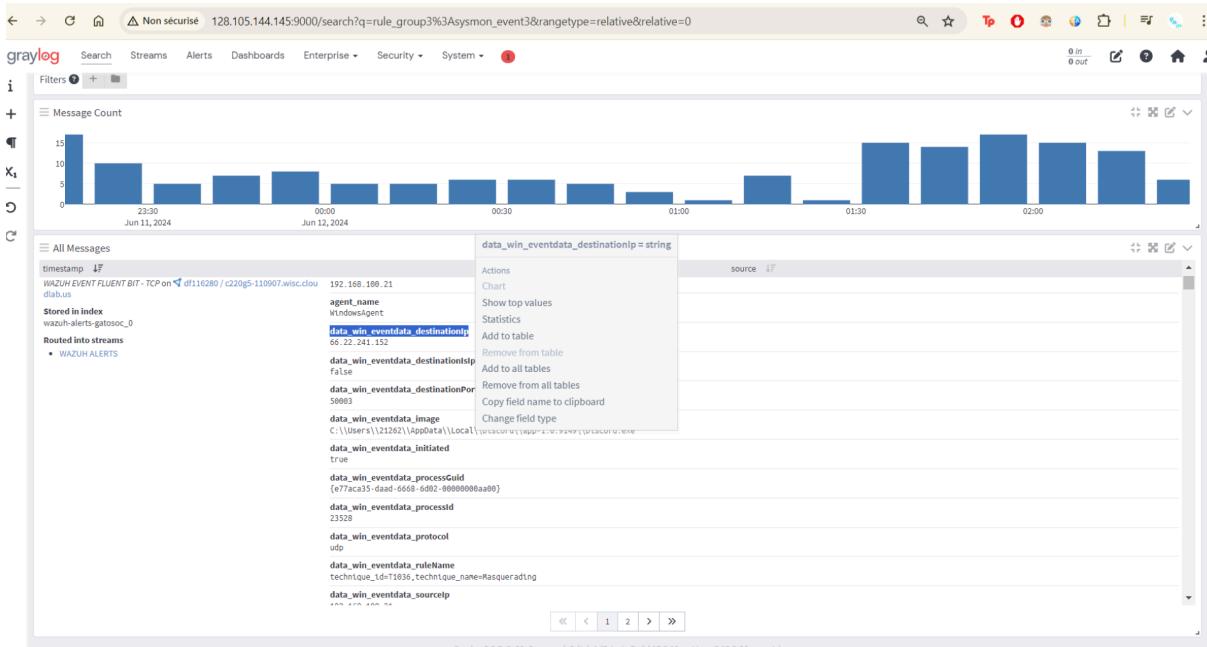


Figure 106 : Destination Ip champ

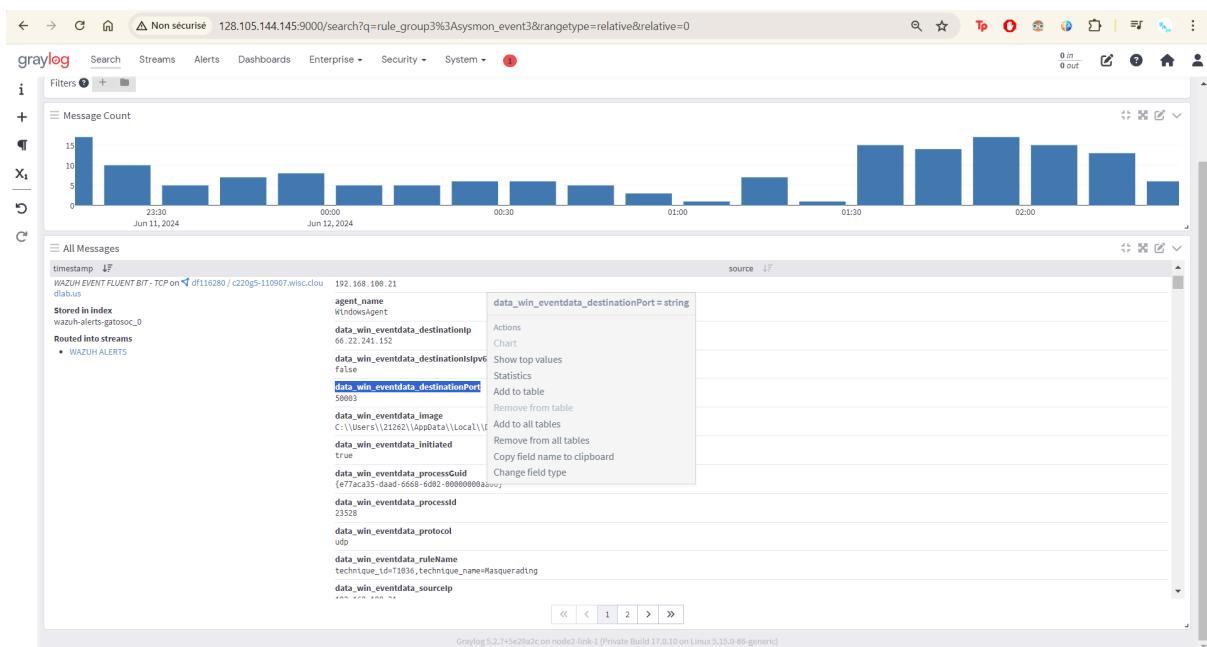


Figure 107 : Destination port champ

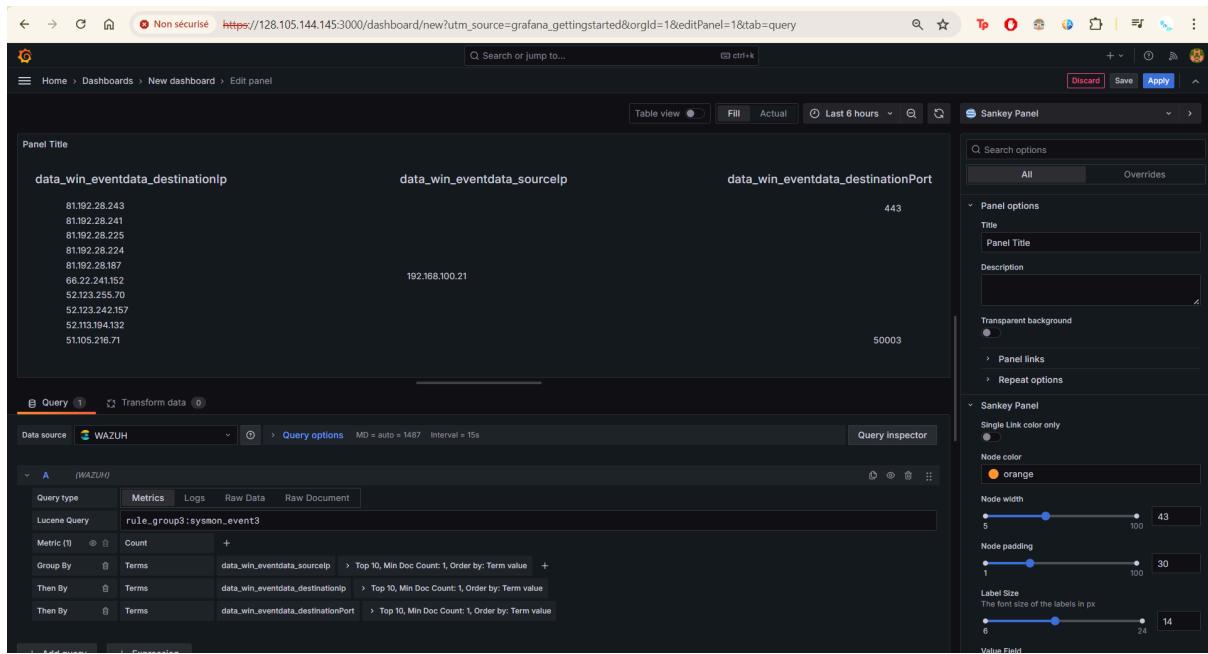


Figure 108 : Champs ajoutés

On renomme les champs :

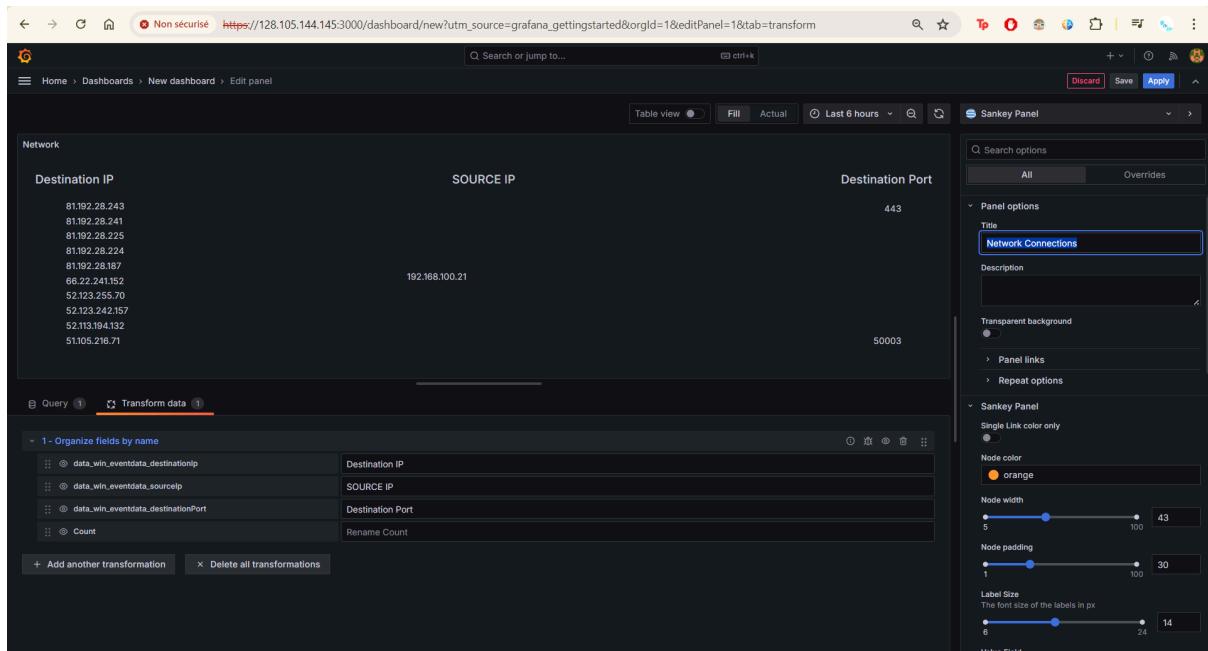


Figure 109 : Champs renommés

On remarque finalement la géolocalisation, et les **dest Ip**, **source IP** et **dest Port** :

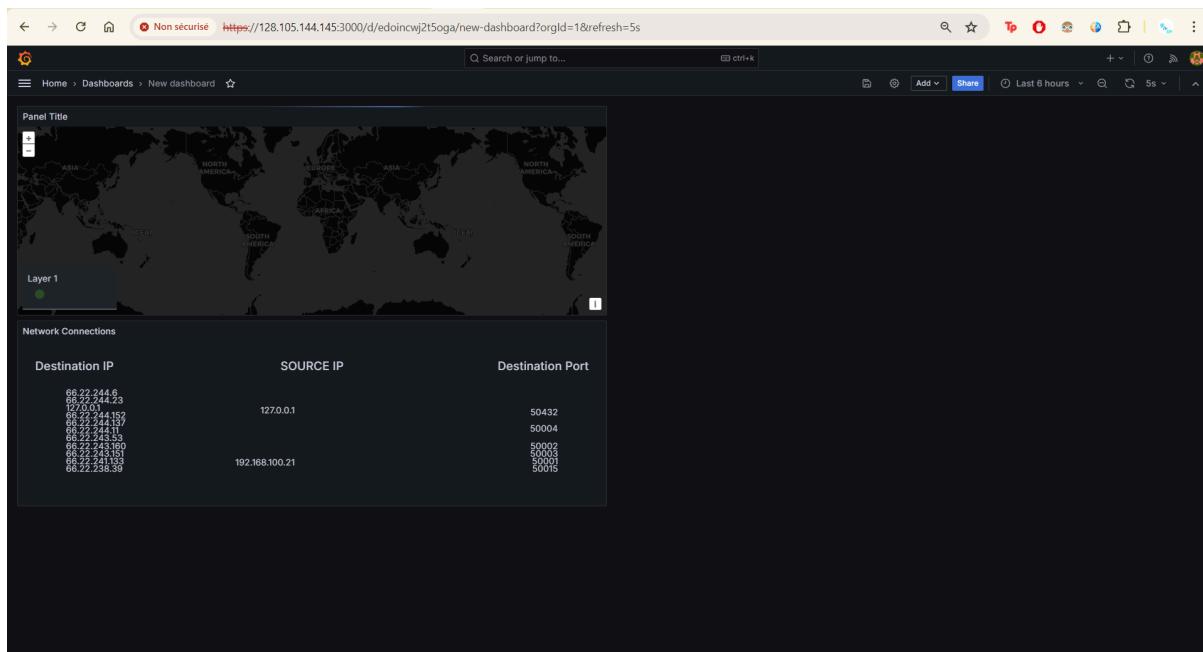


Figure 110 : Visualisation Finale

VIII. Surveillance du système:

Après avoir installé l'agent Wazuh et configuré la collecte des logs, vous pouvez commencer à surveiller votre système, obtenir une vue unifiée et en temps réel de vos données de journal, détecter les anomalies, suivre les performances et résoudre les problèmes potentiels.

Une fois que les logs sont apparus dans l'interface Wazuh, vous avez maintenant accès à une visualisation unifiée et en temps réel de vos données de journal.

La surveillance du système à l'aide de Wazuh vous permet de :

- **Recherche et exploration des logs :** Vous pouvez utiliser la puissance de la recherche d'Elasticsearch intégrée dans Wazuh pour interroger et explorer les logs. Utilisez la barre de recherche dans l'interface Wazuh pour effectuer des requêtes flexibles et filtrer les logs en fonction de différents critères tels que la date, l'heure, les niveaux de journalisation, les mots-clés, etc.
- **Visualisation des données :** Wazuh permet de créer des visualisations graphiques pour mieux comprendre vos données de journal. Utilisez l'outil de création de visualisations de Wazuh intégré à Kibana pour créer des graphiques, des tableaux de

bord et des métriques basées sur les logs collectés. Cela vous permet de détecter des tendances, des anomalies et de visualiser l'état de votre système.

- **Détection d'anomalies et d'incidents** : Vous pouvez configurer des alertes basées sur des critères spécifiques pour détecter les anomalies et les incidents. Par exemple, vous pouvez définir des alertes pour surveiller les erreurs critiques, les comportements suspects, les attaques potentielles, etc. Ces alertes peuvent être déclenchées en temps réel et vous pouvez les recevoir par e-mail, Slack ou tout autre canal de notification configuré.
- **Analyse des performances et dépannage** : La surveillance des logs avec Wazuh vous permet de comprendre les performances de votre système et d'identifier les problèmes potentiels. Vous pouvez suivre les métriques clés, telles que la charge CPU, l'utilisation de la mémoire, les temps de réponse, etc., à l'aide des données de journal collectées. Cela facilite le dépannage des problèmes et l'optimisation des performances de votre système.

IX. Détection d'un malware avec l'intégration de Yara

YARA est un outil open-source et multiplateforme très populaire qui fournit un mécanisme permettant d'exploiter les similitudes de code entre les échantillons de logiciels malveillants d'une même famille. Les fichiers de signature prennent en charge la documentation des séquences d'octets et des correspondances de chaînes qui se produisent dans les logiciels malveillants, ainsi que les opérateurs logiques qui prennent en charge des conditions très robustes et précises pour réduire l'incidence de la réception de faux positifs. Certaines plateformes de partage de renseignements sur les menaces, telles que MISP, prennent en charge YARA. Cela vous permet d'élaborer des règles basées sur vos propres informations collectées sur les menaces.



Figure 111 : Logo Yara

Wazuh intègre Yara pour améliorer ses capacités de détection et de réponse aux menaces.

- Les IOC sont des éléments de données qui peuvent être utilisés pour identifier des menaces de sécurité potentielles, telles que les adresses IP, les domaines, les hachages de fichiers et d'autres artefacts associés à une activité malveillante connue.

Résumé du fonctionnement de YARA avec Wazuh :

- Création de règles YARA : Les analystes créent des règles YARA pour détecter des familles de logiciels malveillants ou des comportements spécifiques.
- Intégration des règles YARA : Les règles YARA sont intégrées aux capacités de détection de Wazuh, soit en étant ajoutées à un ensemble de règles existant, soit en créant un nouvel ensemble de règles.
- Surveillance des journaux : Wazuh surveille les journaux provenant de diverses sources, telles que les journaux système et le trafic réseau, afin de détecter les indicateurs de compromission (IOC).
- Génération d'alertes : Lorsqu'une entrée de journal correspond à une règle YARA, Wazuh génère une alerte et notifie les équipes de sécurité, leur permettant ainsi d'enquêter et de répondre aux menaces potentielles.

Démonstration:

Le processus consiste à configurer un scanner Yara avec des règles personnalisées, à configurer Wazuh pour qu'il surveille les modifications d'un répertoire et déclenche le scanner Yara lorsqu'un nouveau fichier est ajouté ou modifié, et à tester la configuration en téléchargeant des échantillons de logiciels malveillants et en vérifiant les correspondances avec les règles de Yara.

1. Installer YARA:

```
sudo apt update

sudo apt install -y make gcc autoconf libtool libssl-dev
pkg-config jq

sudo curl -LO
https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz

sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f
v4.2.3.tar.gz

cd /usr/local/bin/yara-4.2.3/

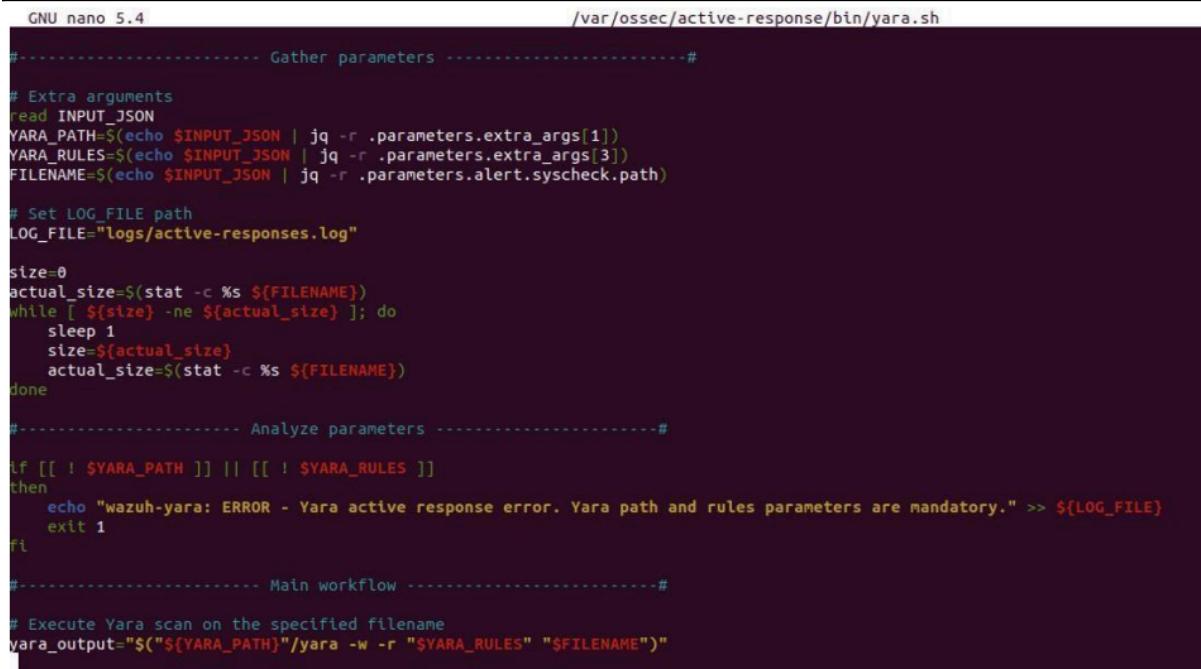
sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make
install && sudo make check
```

2. Télécharger YARA detection Rules :

```
cd /usr/local
git clone https://github.com/Neo23x0/signature-base.git
```

3. Créez un script yara.sh dans le répertoire /var/ossec/active-response/bin/.

```
nano /usr/share/yara/yara_update_rules.sh
```



```
GNU nano 5.4                               /var/ossec/active-response/bin/yara.sh

#----- Gather parameters -----
# Extra arguments
read INPUT_JSON
YARA_PATH=$(echo $INPUT_JSON | jq -r .parameters.extra_args[1])
YARA_RULES=$(echo $INPUT_JSON | jq -r .parameters.extra_args[3])
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.syscheck.path)

# Set LOG_FILE path
LOG_FILE="/logs/active-responses.log"

size=0
actual_size=$(stat -c %s ${FILENAME})
while [ ${size} -ne ${actual_size} ]; do
    sleep 1
    size=${actual_size}
    actual_size=$(stat -c %s ${FILENAME})
done

#----- Analyze parameters -----
if [[ ! $YARA_PATH ]] || [[ ! $YARA_RULES ]]
then
    echo "wazuh-yara: ERROR - Yara active response error. Yara path and rules parameters are mandatory." >> ${LOG_FILE}
    exit 1
fi

#----- Main workflow -----
# Execute Yara scan on the specified filename
yara_output=$( "${YARA_PATH}" /yara -w -r "$YARA_RULES" "$FILENAME" )
```

Figure 112 : Script yara.sh

Ce script Bash permet d'effectuer une analyse Yara sur un fichier donné en réponse active à une alerte Wazuh.

- Lit les paramètres d'entrée à partir d'une chaîne JSON transmise au script.
- Extrait le chemin d'accès Yara, les règles Yara et le nom du fichier à partir des paramètres d'entrée.
- Attends que le fichier soit entièrement écrit avant de l'analyser.
- Vérifie si le chemin d'accès et les règles de Yara sont présents.
- Exécute une analyse Yara sur le fichier spécifié en utilisant le chemin d'accès et les règles Yara
- Ajoute les résultats de l'analyse à un fichier journal.

4. Changez le propriétaire du fichier yara.sh en root:wazuh et les permissions du fichier.

```
#sudo chown root:wazuh /var/ossec/active-response/bin/yara.sh  
#sudo chmod 750 /var/ossec/active-response/bin/yara.sh
```

5. Pour surveiller le répertoire /tmp/yara/malware, modifiez le fichier de configuration de l'agent Wazuh /var/ossec/etc/ossec.conf :

6. Redémarrer l' agent wazuh

```
#sudo systemctl restart wazuh-agent
```

- **Wazuh Server :**

Configurer Wazuh pour qu'il signale les changements de fichiers dans le répertoire surveillé par le point d'accès.

Configurez un script de réponse active pour qu'il se déclenche chaque fois qu'un fichier suspect est détecté.

1. Ajouter des règles au fichier /var/ossec/etc/rules/local_rules.xml.

```
<group name="syscheck">  
  <rule id="100300" level="7">  
    <if_sid>550</if_sid>  
    <field name="file">/tmp/yara/malware/</field>  
    <description>File modified in /tmp/yara/malware/ directory.</description>  
  </rule>  
  <rule id="100301" level="7">  
    <if_sid>554</if_sid>  
    <field name="file">/tmp/yara/malware/</field>  
    <description>File added to /tmp/yara/malware/ directory.</description>  
  </rule>  
</group>
```

Figure 113 : Règles

Le premier groupe nommé syscheck comprend deux règles avec les identifiants 100300 et 100301. Ces règles sont déclenchées lorsqu'un fichier est modifié ou ajouté au répertoire /tmp/yara/malware/, respectivement. Les deux règles ont un niveau de gravité de 7, ce qui correspond à un niveau d'avertissement.

Le deuxième groupe nommé yara comprend deux règles avec les identifiants 108000 et 108001. Ces règles sont liées à la réponse active Yara qui utilise le script yara.sh mentionné précédemment.

- La règle 108000 est une règle de regroupement utilisée pour regrouper tous les événements liés à Yara.
- La règle 108001 est déclenchée lorsque le script yara.sh détecte une correspondance positive avec une règle Yara pour un fichier analysé. Cette règle a un niveau de gravité de 12, c'est-à-dire un niveau critique.

2. L'ajout de décodeurs au fichier /var/ossec/etc/decoders/local_decoder.xml permet d'extraire les informations des résultats de l'analyse YARA.

```
<decoder name="yara">
  <prematch>wazuh-yara:</prematch>
</decoder>

<!-- wazuh-yara: INFO - Scan result: SUSP_Just_EICAR
[description="Just an EICAR test file - this is boring but users
asked for it",author="Florian
Roth",reference="http://2016.eicar.org/85-0-Download.html",date="
2019-03-24",score
=40,hash1="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538a
abf651fd0f"] /var/www/html/upload/test.txt -->

<decoder name="yara_decoder1">
  <parent>yara</parent>
  <regex>wazuh-yara: (\S+) - Scan result: (\S+)
[description\p\p(\.*")\.*] (\S+)</regex>
  <order>log_type, yara_rule, yara_description,
yara_scanned_file</order>
</decoder>
```

Le décodeur nommé "yara_decoder" a une règle de pré-match qui correspond à la chaîne "wazuh-yara:". Ce décodeur pourrait être utilisé pour identifier les lignes de journal qui correspondent aux journaux de réponse active de Yara. Le deuxième décodeur nommé "yara_decoder1" est un enfant de "yara_decoder". Ce décodeur pourrait être utilisé pour extraire des informations pertinentes des journaux de réponse active de Yara, telles que la règle de Yara qui a déclenché la réponse et le fichier qui a été analysé.

3. Pour configurer le module de réponse active afin qu'il se déclenche après le déclenchement des règles 100300 et 100301, modifiez le fichier /var/ossec/etc/ossec.conf

```
<command>
<name>yara_linux</name>
<executable>yara.sh</executable>
<extra_args>-yara_path /usr/local/bin -yara_rules /tmp/yara/rules/yara_rules.yar</extra_args>
<timeout_allowed>no</timeout_allowed>
</command>

<!--active response-->
<active-response>
<command>yara_linux</command>
<location>local</location>
<rules_id>100300,100301</rules_id>
</active-response>
```

Figure 114 : Règles

Cette configuration met en place une réponse active qui utilisera Yara pour rechercher des logiciels malveillants chaque fois qu'un fichier est modifié ou ajouté dans ce répertoire, à l'aide des règles Yara situées dans /var/ossec/etc/ossec.conf.

4. Redémarrer wazuh manager

```
sudo systemctl restart wazuh-manager
```

X. Intégration de SURICATA

1. Aperçu général

Lorsque Suricata est intégré à Wazuh, il envoie des alertes au serveur Wazuh dès qu'il détecte un trafic réseau suspect ou malveillant. Ces alertes sont ensuite traitées et analysées par le moteur de gestion et de corrélation des journaux de Wazuh, qui les met en corrélation avec d'autres événements et données de sécurité collectés à partir de diverses sources, telles que les systèmes de détection d'intrusion basés sur l'hôte (HIDS), les journaux du système et les scanners de vulnérabilité.

Wazuh peut également enrichir les alertes de Suricata avec un contexte supplémentaire, tel que les adresses IP source et destination, les ports et les protocoles impliqués dans le trafic réseau.

Ces informations contextuelles aident les équipes de sécurité à comprendre la portée et la gravité de l'alerte et à hiérarchiser leur réponse en conséquence.

L'intégration de Suricata avec Wazuh améliore les capacités de détection des menaces en fournissant une solution complète de surveillance de la sécurité qui exploite les forces des NIDS et HIDS.

2. Résumé du fonctionnement de Suricata avec Wazuh :

- L'agent Wazuh installé sur chaque hôte collecte les données du journal et les alertes, y compris les alertes Suricata, et les transmet au serveur de gestion Wazuh pour traitement.
- Le serveur de gestion traite ensuite les données à l'aide du moteur de corrélation et d'analyse, qui met en corrélation les alertes avec d'autres événements et données de sécurité collectés à partir de diverses sources.
- Enfin, le serveur de gestion envoie des alertes au tableau de bord de l'utilisateur, ce qui permet aux équipes de sécurité de visualiser les événements et les menaces de sécurité en temps réel et d'y répondre

Configuration :

1. Installer la version 6.0.8 de Suricata :

```
#sudo add-apt-repository ppa:oisf/suricata-stable  
#sudo apt-get update  
#sudo apt-get install suricata -y
```

2. Télécharger et extraire le jeu de règles Emerging Threats Suricata :

```
#cd /tmp/ && curl -LO  
https://rules.emergingthreats.net/open/suricata6.0.8/emerging.rules.tar.gz  
  
#sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules  
/etc/suricata/rules/  
  
#sudo chmod 640 /etc/suricata/rules/*.rules
```

3. Personnaliser le comportement de Suricata en éditant le fichier /etc/suricata/suricata.yaml

4. Redémarrer suricat
5. Redémarrer l'Agent wazuh

```
sudo systemctl restart suricata
sudo systemctl restart wazuh-agent
```

Simulation d'attaque

Voici un ping depuis ma machine physique vers le debian endpoint et on remarque des alerts générés :

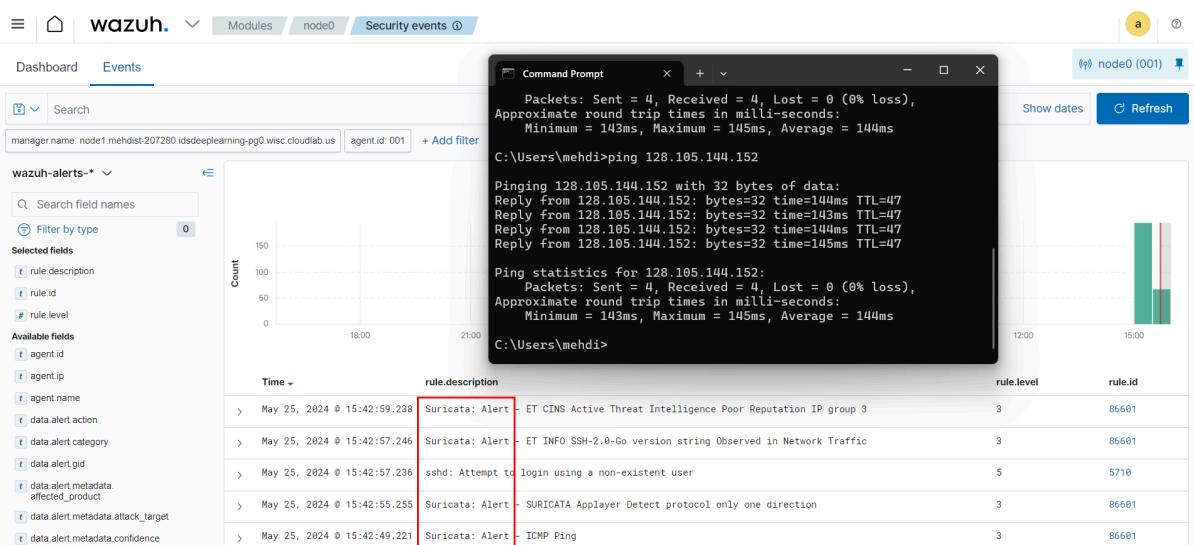


Figure 115 : Alert suricata

XI. Mise en place de TheHIVE

1. Installation docker :

```

sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o
/etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc

echo \
  "deb [arch=$(dpkg --print-architecture)
signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update

```

2. Deploiement Cortex et theHive avec docker :

On commence par créer un dossier vide

```

mkdir thehive-cortex
cd thehive-cortex

```

Puis on clone le fichier docker compose suivant et on build :

```

git clone
https://github.com/l3l11-cybersec/thehive-cortex-misp-docker-compose-lab1update/blob/main/docker-compose.yml#L1
docker compose -d

```

Après quelques minutes, theHive et Cortex seront disponibles.

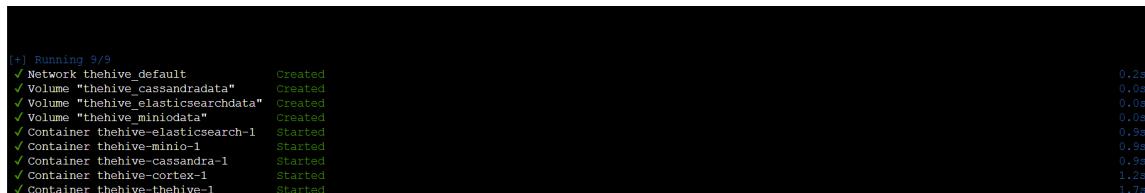


Figure 11+ : conteneurs TheHive et Cortex actives

The hive sera accessible sur le port 9000

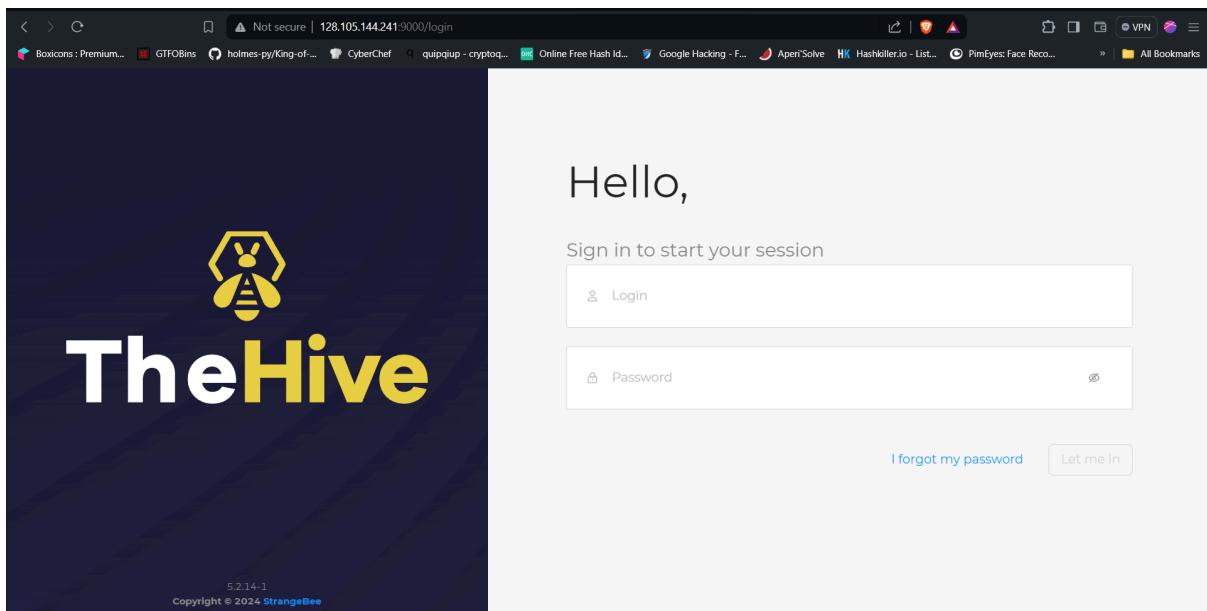


Figure 117 : TheHive dashboard

Cortex sera accessible sur le port 9001

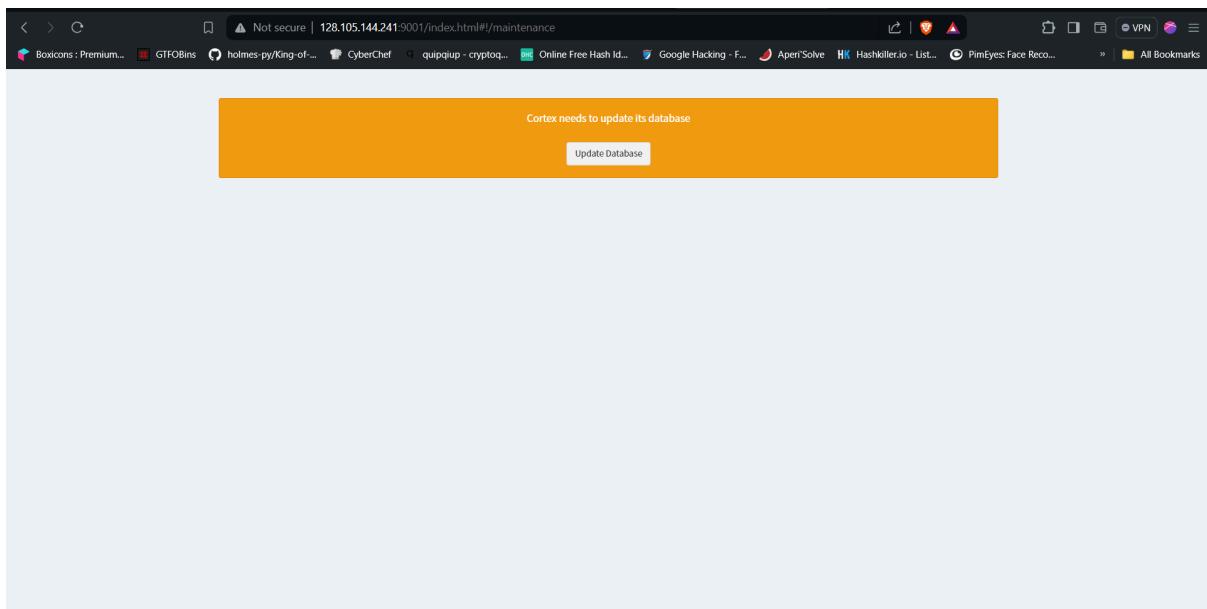


Figure 118 : Cortex Dashboard

Après configuration :

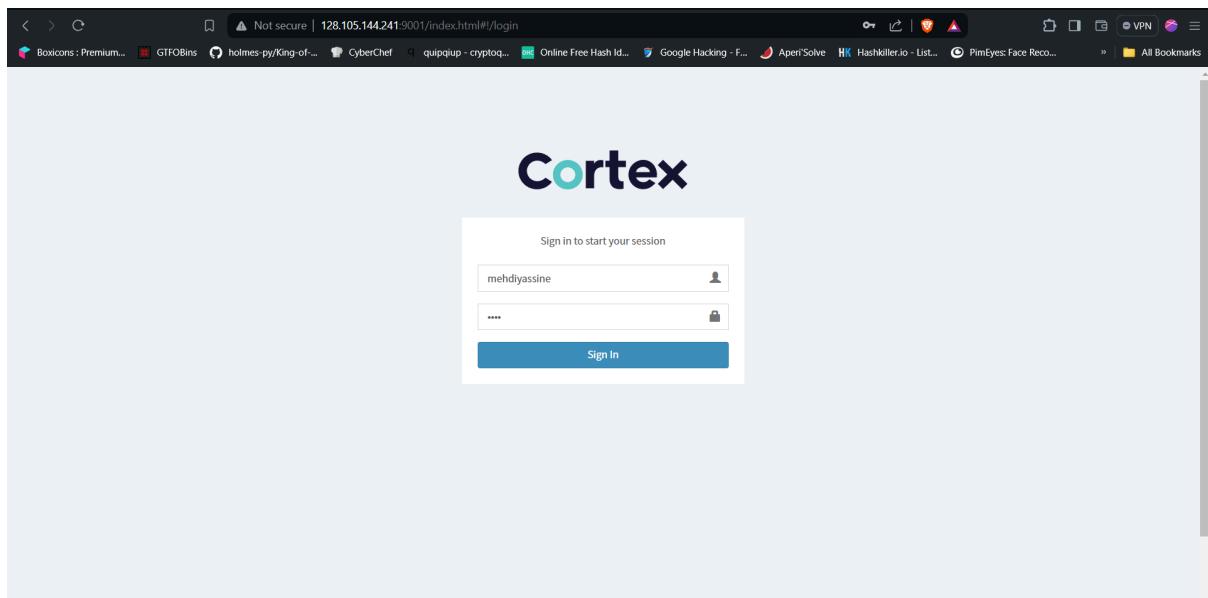


Figure 119 : Cortex Dashboard

3. Configuration de Cortex :

On commence par créer un nouvel utilisateur:

Status	User details	Password	API Key
Active	Login: mehdlyassine Organization: cortex Full name: mehdlyassine Roles: superadmin	Edit password	Create API Key

Figure 120: Cortex users

Figure 121 : Cortex new user

Puis on génère un clé API de cet utilisateur

The screenshot shows the Cortex web interface at the URL `128.105.144.241:9001/index.html#/admin/users`. The title bar says "Cortex". The main content area is titled "Users (2)". It has a search bar and a dropdown for "50 / page". There are two rows of user information:

Status	User details	Password	API Key
Active	Login: mehdly Organization: Mehdi Yassine Full name: Mehdi Yassine Roles: read, analyze, orgadmin	Edit password	Renew Revoke uC3JEQe4N0TPNxqh1702LJ0NTRETTI Edit Lock
Active	Login: mehdlyassine Organization: cortex Full name: mehdlyassine Roles: superadmin	Edit password	Create API Key Edit

Figure 122: new user api key

Configuration VirusTotal et MalwareBazaar avec Cortex :

On crée un compte sur virus total et on copie notre API key

The screenshot shows the VirusTotal API interface. On the left, there's a sidebar with "Profile", "API Key" (which is selected), "Settings", and "Sign Out". The main content area is titled "API KEY". It contains a message about the API key being personal and subject to terms of service. Below this is a "API QUOTA ALLOWANCES FOR YOUR USER" section with usage statistics and upgrade options. To the right, there are icons for various API clients and services.

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

Figure 123 : virustotal api

On fait le même pour MalwareBazaar

Display name *

Email address

Pushover Key

First Login

Last Login

Your API-Key Regenerate

of submissions

Your public profile <https://bazaar.abuse.ch/user/13939/>

Hide public profile On

Upload a YARA Rule

Figure 124 : malwarebazaar api

Ensuite on télécharge VirusTotal sur Cortex en suivant les étapes :

1.

Analyzer	Max TLP	Max PAP	Rate Limit	Cache
VirusTotal_DownloadSample_3_1 Version: 3.1 Author: LDO-CERT License: AGPL-V3 Type: Docker				
Use VirusTotal to download the original file for an hash.				
+ Enable				
VirusTotal_GetReport_3_1 Version: 3.1 Author: CERT-BDF, StrangeBee License: AGPL-V3 Type: Docker				
Get the latest VirusTotal report for a file, hash, domain or an IP address.				
+ Enable				
VirusTotal_Rescan_3_1 Version: 3.1 Author: CERT-LDO License: AGPL-V3 Type: Docker				
Use VirusTotal to run new analysis on hash.				
+ Enable				
VirusTotal_Scan_3_1 Version: 3.1 Author: CERT-BDF, StrangeBee License: AGPL-V3 Type: Docker				
Scan a file, hash, domain or IP address with VirusTotal.				
+ Enable				

Figure 125 : VirusTotal sur Cortex

2.On configure avec notre clé API générée

Figure 126 : VirusTotal sur Cortex API

On fait le même pour MalwareBazaar

1.

Figure 127 : MalwareBazaar sur Cortex

2. On configure avec notre clé API générée

Organization: Mehdi Yassine

Available analyzers (222)

Analyzer

- EmergingThreats_MalwareInfo_1_0** Version: 1.0 Author: Davide Arcuri and Andrea Garavaglia
- MalwareBazaar_1_0** Version: 1.0 Author: Andrea Garavaglia, Davide Arcuri
- MalwareClustering_Search_1_0** Version: 1.0 Author: LDO-CERT License: AGPL-V3
- Malwares_GetReport_1_0** Version: 1.0 Author: LDO-CERT License: AGPL-V3

Base details

Name: MalwareBazaar_1_0

Configuration

api_key *

MalwareBazaar api key

Options

Enable TLP check: True Max TLP: AMBER

Enable PAP check: True Max PAP: AMBER

HTTP Proxy:

HTTPS Proxy:

CA Certs:

Job cache: 10

Job timeout: 30

Refresh analyzers

Figure 127 : MalwareBazaar sur Cortex API

Voici les deux outils téléchargés:

Cortex

+ New Analysis

Analyzers (2)

Data Types (6) Analyzer

Select ▾ Search for analyzer description Search Clear

Page size 50 / page

MalwareBazaar_1_0 Version: 1.0 Author: Andrea Garavaglia, Davide Arcuri - LDO-CERT License: AGPL-V3

Search hashes on MalwareBazaar.

Run

Applies to: hash

VirusTotal_GetReport_3_1 Version: 3.1 Author: CERT-BDF, StrangeBee License: AGPL-V3

Get the latest VirusTotal report for a file, hash, domain or an IP address.

Run

Applies to: file hash domain fqdn ip url

TheHive Project 2016-2021, AGPL-V3

Version: 3.1.7-1

Figure 128 : VirusTotal + MalwareBazaar

Réalisation d'un test:

On donne un hash d'un malware connu dans le marché et on choisit nos analyseurs (MalwareBazaar et VirusTotal)

TheHive Project 2016-2021, AGPL-V3 Version: 3.1.7

Figure 129 : Test avec un hash

après quelques minutes, le status est succès

TheHive Project 2016-2021, AGPL-V3 Version: 3.1.7

Figure 130 : le test est terminé

Voici un rapport sur le malware analysé:

The screenshot shows the Cortex interface with a job titled "VirusTotal_GetReport_3_1". The job details include an artifact hash, date, TLP (TLP:AMBER), PAP (PAP:AMBER), and status (Success). The report summary indicates "3 contacted domain(s)". The main panel displays the "Job report" section with parameters and a large JSON report body.

```

{
  "summary": {
    "taxonomies": [
      {
        "level": "malicious",
        "namespace": "VI",
        "predicate": "GetReport",
        "value": "61/78"
      },
      {
        "level": "suspicious",
        "namespace": "VI",
        "predicate": "GetReport",
        "value": "3 contacted domain(s)"
      }
    ],
    "full": {
      "type": "file",
      "attributes": {
        "authentihash": "aeddccf92ff47f7b02aa98118e152ba71a3995b9fe439ee1e37c1d4c1b7d56f0c",
        "vhash": "925066551d1d751510195017z11z13z21z31z1az1"
      }
    }
  }
}

```

Figure 131 : rapport généré

4. Configuration de Cortex avec TheHive :

Sur TheHive, on ajoute un utilisateur “API USER” qui servira comme un lien entre Cortex et TheHive,

The screenshot shows the TheHive administration interface for adding a new user. The dialog box is titled "Adding a User" and contains fields for "Login" (wazuhapi@gatosoc.local), "Name" (API USER), and "Organisations" (admin and Mehdi Yassine). The background shows a list of existing users: Default admin user (admin@thehive.local) and Mehdi (mehdi@gatosoc.local).

Figure 132: new TheHive user

on lui donne l’API key qu’on a créé pour l’utilisateur dans Cortex :

Figure 133 : config new user avec API

Finalement, on remarque les alertes qui sont générés sur TheHive

Figure 134 : Les alertes générés sur TheHive

XII. Conclusion:

A travers ce dernier chapitre, nous avons pu démontrer l'implémentation de la solution proposée et les résultats obtenus à la fin du projet. Nous pouvons affirmer que les résultats obtenus ont dépassé nos attentes et qu'ils ont répondu avec succès à tous les objectifs initialement définis. A cet égard, l'intégration des fonctionnalités avancées des outils présentés a grandement amélioré la visibilité, la corrélation et l'élimination des tâches.

récurrentes, facilitant ainsi la détection précoce des menaces et une réponse rapide et automatisée.

Conclusion générale

Ce projet a pour ambition d'établir un centre opérationnel de sécurité, permettant à l'équipe Blue Team de surveiller et d'intervenir face aux cybermenaces avancées de manière continue. En intégrant les outils Wazuh, ELK et TheHive, nous avons conçu une plateforme complète, dotée de fonctionnalités avancées et d'une visualisation des données optimale, renforçant ainsi la posture de sécurité de notre entreprise. Toutefois, notre parcours n'a pas été sans embûches. Des contraintes matérielles et temporelles, ainsi qu'un manque de documentation sur MISP, ont impacté notre avancement. Bien que la partie liée à MISP n'ait pu être intégrée dans le projet et que l'envoi d'alertes entre les outils n'ait pu être achevé, notre détermination et notre capacité d'adaptation ont été mises en lumière. Malgré ces défis, nous avons réussi à accomplir les principaux objectifs, illustrant notre engagement indéfectible envers la sécurité de l'entreprise et notre volonté de dépasser les obstacles pour assurer sa protection contre les menaces actuelles et futures.

Références :

Intégration graylog-wazuh:

<https://community.graylog.org/t/integrating-wazuh-indexer-with-graylog/26430>

Documentation wazuh:

<https://documentation.wazuh.com/current/installation-guide/index.html>

Docker:

<https://docs.docker.com/engine/install/ubuntu/>

TheHive:

<https://github.com/TheHive-Project/TheHive>

Cortex:

<https://github.com/TheHive-Project/Cortex>

Misp:

https://en.wikipedia.org/wiki/MISP_Threat_Sharing

VirusTotal:

<https://fr.wikipedia.org/wiki/VirusTotal>

Généralités:

<https://www.ibm.com/topics/security-operations-center>

<https://www.oracle.com/fr/cloud/soc-security-operations-center/>

https://www.splunk.com/fr_fr/data-insider/what-is-siem.html

<https://www.techtarget.com/searchsecurity/definition/SOAR>