RAPPORT DE STAGE DE FIN MODULE

Threat Hunting : Détection d'un Brute Force Réussi suivi d'une Exfiltration de Données

Réalisé par : Mme LABIED Chayma, Mr GHRISSE Oussama, Mr Jaber Oussama

Tuteur (s) :

Encadrant Professionnel : M. ABDELBARY EBady

Au sein de l'entreprise DataProtect :

DATAPROTECT
Security is our commitment

Année universitaire : 2025/2026

Avant-propos

Nom et Prénom Des Stagiaires : LABIED Chayma, GHRISSE Oussama, Jaber Oussama

Etablissement d'accueil : DATAPROTECT

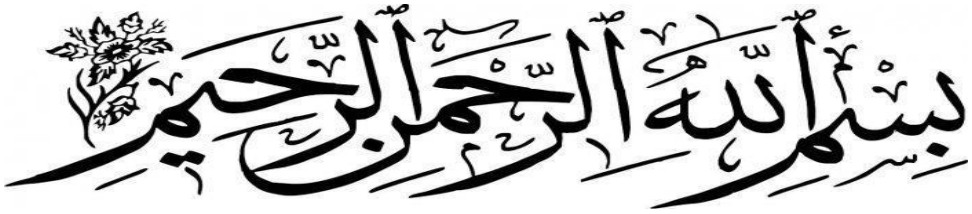
Adresse de l'organisme d'accueil : CASANEARSHORE, Boulevard Al

Qods, Shore 4, Quartier Sidi Maarouf, 20270 Casablanca – Maroc

Encadrant (DATA PROTECT): M. ABDELBARY EBady

Date de début et de fin du stage : Du 11 Décembre 2025 au 02 janvier 2026

Dédicaces



Louange à Dieu tout puissant mon créateur

À nos chers parents,

Ce travail est avant tout pour vous. Aucune parole ne saurait traduire toute ma reconnaissance pour votre amour, vos sacrifices, et votre présence rassurante à chaque étape de ma vie. Votre soutien m'a donné la force d'aller toujours plus loin. Que Dieu vous comble de santé, de paix et de bonheur

À nos familles,

Merci pour vos affections sincères, vos écoutes et votre bienveillance. Vos tendresse et vos énergie positive m'ont toujours accompagnée, même dans les moments les plus compliqués. Je vous dédie ce travail avec tout mon amour

À nos amies,

Votre amitié précieuse et votre soutien inestimable ont été d'un grand réconfort durant ce parcours. Vous êtes bien plus que nos amies : nos sœur de cœur, toujours présente. Que votre lien reste aussi fort, et que la vie vous offre autant de bonheur que vous en sèmes autour de vous.

À nos chers professeurs, et membres du jury,

Merci à tous pour le savoir transmis, et tout particulièrement à M. Abdelbary ebady pour leur présence et leur bienveillance.

À tous ceux qui me sont chers, à vous tous

Merci

Remerciement

Nous tenons à exprimer notre sincère gratitude à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet.

À notre encadrant pédagogique

Nos vifs remerciements pour son suivi rigoureux, ses conseils éclairés et sa grande disponibilité tout au long de ce projet. Son expertise a été précieuse pour orienter nos travaux.

À l'équipe DataProtect-Jobintech

Nous adressons toute notre reconnaissance pour votre accueil chaleureux, votre partage d'expertise et votre soutien technique constant. Votre accompagnement sur la plateforme Elastic Security a été déterminant pour la réussite de ce projet.

Aux membres du jury

Nous vous remercions par avance pour le temps que vous consacrerez à l'évaluation de notre travail. Vos retours et vos critiques constructives seront précieux pour la suite de notre parcours.

À nos familles et proches

Enfin, un merci tout particulier à nos familles et amis pour leur soutien indéfectible, leur patience et leurs encouragements tout au long de cette formation

Résumé

Le présent document retrace le travail réalisé dans le cadre de notre projet intitulé **« Mise en place d'un processus de Threat Hunting sur un environnement Windows à travers la simulation d'une attaque réelle »**, mené au sein de **DataProtect**, entreprise reconnue pour son expertise en cybersécurité et en surveillance des infrastructures IT.

L'objectif principal de ce projet est de **simuler une attaque complète sur un serveur Windows**, puis d'analyser et de détecter cette compromission en se basant exclusivement sur les **logs collectés par un SIEM**, reproduisant ainsi les conditions opérationnelles d'un centre de supervision de la sécurité (SOC).

Pour atteindre cet objectif, nous avons mis en place un environnement composé d'un **Windows Server (cible)**, d'une machine **Kali Linux (attaquant)** et d'un **SIEM**, configuré pour collecter des journaux critiques tels que les **Windows Event Logs, Sysmon, logs PowerShell et données réseau/DNS**.

L'attaque simulée couvre plusieurs étapes clés : accès initial (par brute-force RDP ou exécution de commandes PowerShell), exécution et enchaînement de commandes malveillantes, mise en place de techniques de persistance, collecte de données sensibles et exfiltration vers la machine contrôlée par l'attaquant.

Une démarche structurée de **Threat Hunting** a ensuite été menée pour formuler des hypothèses d'investigation, identifier les comportements suspects, corréler les événements et **reconstituer la timeline complète de l'attaque**, en reliant chaque action aux tactiques et techniques du **Framework MITRE ATT&CK**.

Ce projet a permis d'évaluer la visibilité offerte par la journalisation Windows, d'identifier les capacités et limites de détection, et de proposer des **cas d'usage SIEM supplémentaires** afin de renforcer la détection précoce, la corrélation et la réponse aux incidents de sécurité sur des environnements Windows.

Ce travail s'inscrit pleinement dans les enjeux opérationnels d'un SOC, en mettant en pratique des techniques modernes de **Threat Hunting et de défense proactive** contre les cybermenaces.

Keywords : Threat Hunting, DataProtect, SIEM, Windows Server, Sysmon, PowerShell, MITRE ATT&CK, Journalisation, Exfiltration, Analyse des incidents, Sécurité informatique, SOC.

Abstract

This document presents the work carried out as part of our project entitled **"Implementation of a Threat Hunting Process on a Windows Environment through Realistic Attack Simulation,"** conducted within **DataProtect**, a company recognized for its expertise in cybersecurity and IT infrastructure monitoring.

The main objective of this project is to **simulate a full attack on a Windows Server** and to analyze and detect the compromise **exclusively through SIEM-collected logs**, replicating the operational conditions of a Security Operations Center (SOC).

To achieve this goal, we deployed an environment consisting of a **Windows Server (victim)**, a **Kali Linux machine (attacker)**, and a **SIEM** configured to collect critical logs such as **Windows Security Event Logs, Sysmon events, PowerShell logs, and Network/DNS data**.

The simulated attack covers several key phases: initial access (via RDP brute force or malicious PowerShell execution), execution of attacker commands, implementation of persistence mechanisms, collection of sensitive data, and exfiltration to the attacker-controlled machine.

A structured **Threat Hunting methodology** was then applied to develop investigation hypotheses, identify suspicious activities, correlate events, and **reconstruct the complete attack timeline**, mapping every action to the tactics and techniques of the **MITRE ATT&CK Framework**.

This project enabled us to assess the visibility provided by Windows logging, identify detection capabilities and limitations, and propose **additional SIEM use cases** to strengthen early detection, correlation, and incident response capabilities within Windows environments.

Our work aligns with real SOC operational challenges, applying modern **Threat Hunting practices and proactive defense techniques** to better understand and detect advanced cyber threats.

Keywords: Threat Hunting, DataProtect, SIEM, Windows Server, Sysmon, PowerShell, MITRE ATT&CK, Logging, Data Exfiltration, Incident Analysis, Cybersecurity, SOC.

Table des matières

Liste des figures

Liste des Tableaux

Liste des abréviations

Abréviation	Désignation
SOC	Security Operations Center
SIEM	Security Information and Event Management
MITRE ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
IOC	Indicator of Compromise
IOA	Indicator of Attack
TTP	Tactics, Techniques and Procedures

RDP	Remote Desktop Protocol
VM	Virtual Machine
OS	Operating System
AD	Active Directory
DNS	Domain Name System
IP	Internet Protocol
TCP	Transmission Control Protocol
SSH	Secure Shell
CMD	Command Prompt
PS	PowerShell
Sysmon	System Monitor (Sysinternals)
EDR	Endpoint Detection and Response
APT	Advanced Persistent Threat
PID	Process Identifier
GPO	Group Policy Object
FTP	File Transfer Protocol

Introduction générale

De nos jours, les cyberattaques deviennent de plus en plus sophistiquées et ciblent fréquemment les infrastructures critiques des organisations. Dans ce contexte, la **détection proactive des menaces** et la capacité à **analyser les comportements malveillants** constituent des enjeux stratégiques majeurs pour renforcer la sécurité des systèmes d'information. Les entreprises doivent non seulement protéger leurs environnements, mais également mettre en place des mécanismes avancés de surveillance afin d'identifier rapidement toute activité suspecte.

C'est dans ce cadre que s'inscrit le présent projet, réalisé au sein de **DataProtect**, acteur de référence dans la cybersécurité au Maroc. L'entreprise accompagne les organisations dans l'amélioration de leur posture de

sécurité, notamment à travers le déploiement de plateformes de journalisation, d'outils SIEM et de mécanismes de détection avancée. Le **Threat Hunting**, discipline consistant à rechercher activement des signes de compromission au sein des systèmes d'information, occupe désormais une place centrale dans les stratégies modernes de défense.

Notre projet s'inscrit pleinement dans cette dynamique. Il porte sur la **mise en place d'un processus complet de Threat Hunting** basé sur la **simulation d'une attaque réelle** contre un environnement Windows. L'objectif principal est double :
d'une part, **simuler une chaîne d'attaque complète** incluant accès initial, exécution de commandes, persistance, collecte et exfiltration de données ;
d'autre part, **analyser et reconstruire l'ensemble de cette attaque exclusivement à travers les logs collectés par un SIEM**, en s'appuyant sur des sources critiques telles que Windows Event Logs, Sysmon, PowerShell Logs et données réseau/DNS.

Le projet vise également à **mapper les différentes étapes de l'attaque au Framework MITRE ATT&CK**, permettant ainsi de mesurer la couverture de détection et d'identifier d'éventuelles lacunes. Grâce à cette démarche, il devient possible de proposer des recommandations et de nouveaux cas d'usage SIEM visant à renforcer les capacités de surveillance et de réponse aux incidents.

Le présent rapport retrace l'ensemble des travaux menés dans le cadre de ce projet. Il s'articule autour de cinq chapitres :

- **Chapitre 1 :** Contexte général du projet
- **Chapitre 2 :** Environnement de travail, outils et technologies utilisés
- **Chapitre 3 :** Threat Hunting En Cybersécurité
- **Chapitre 4 :** Déploiement d'Elastic Security dans le Cloud
- **Chapitre 5 :** Tests, expérimentation et processus de Threat Hunting

Chapitre 1 : Contexte général du projet

Introduction :

Dans ce chapitre, nous allons présenter le cadre général du projet, à savoir :

- L'organisme d'accueil
- Le contexte du projet
- Les objectifs et la démarche de la réalisation du projet

1. Présentation de l'organisme d'accueil

1.1 DATAPROTECT en quelques mots

Figure 1: Logo de l'entreprise

DATAPROTECT est une entreprise spécialisée en sécurité de l'information. Fondée par Ali EL AZZOUZI, un expert en sécurité de l'information ayant mené plusieurs projets de conseil et d'intégration de solutions de sécurité au Maroc et à l'étranger, DATAPROTECT appuie son offre sur une vision unifiée de la sécurité de l'information. Dotée d'un réservoir de compétences pointues en sécurité lui permettant d'assurer une expertise unique sur le marché local et régional.

Depuis sa création, DATAPROTECT ne cesse d'évoluer pour délivrer ses prestations d'excellence à travers une équipe d'experts pluridisciplinaires dotée d'un sens unique de l'intimité client. Aussi, son statut de première entité accréditée PCI QSA au Maroc par le consortium Payment Card Industry Security Standards Council pour les certifications PCI DSS et PA DSS, fait d'elle un cas d'école unique dans la région.

Avec une centaine de clients en Afrique du Nord, en Afrique Subsaharienne et au Moyen Orient, DATAPROTECT est aujourd'hui capable de délivrer ses services en toute agilité, pour des multinationales comme pour des entreprises locales, avec à la clé une réputation établie de pionnier sur la thématique de la sécurité de l'Information.

1.2 DATAPROTECT : Un acteur clé dans le marché de la cybersécurité

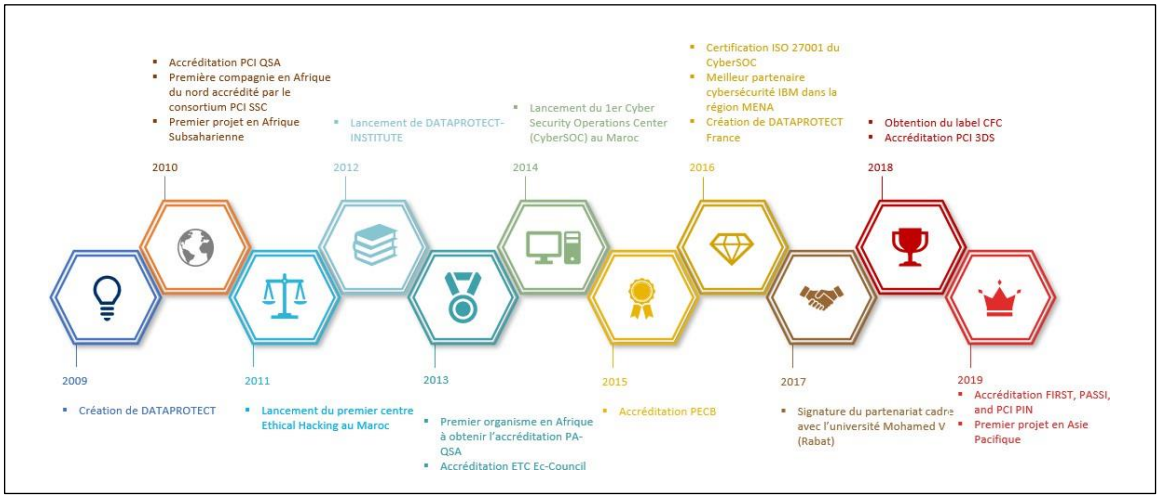


Figure 2:Chiffres clés

Créée en 2009, DATAPROTECT, aujourd'hui c'est :

- +150 employés dont 110 consultants « Full Security »
- +200 certifications sécurité
- +350 clients actifs dont une centaine de banques
- +1500 projets à travers 35 pays
- +16 M Euro de chiffre d'affaires dont 80% à l'international (chiffre 2020)
- Une filiale en France depuis 2016
- Une équipe dédiée au développement des solutions innovantes en Cybersécurité

1.3 organigramme de l’entreprise

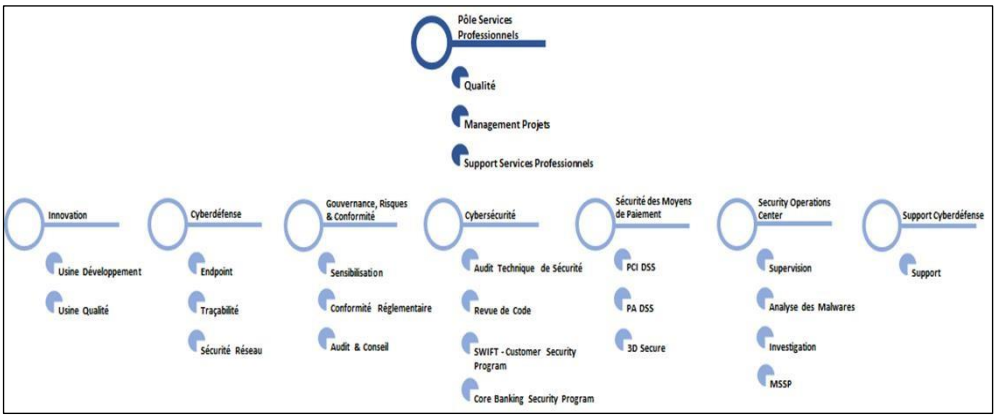


Figure 3:Organigramme de l'entreprise

1.4 Références

DATAPROTECT fait de la satisfaction client une priorité, elle a été sollicitée par plusieurs organismes pour mettre en place les solutions de sécurisation des postes de travail.

Figure 4:Les Clients DATAPROTE

1.5 Activités de DATAPROTECT

DATAPROTECT est organisée autour de cinq pôles d'activités :

Figure 5:Pôles d'activités de DATAPROTECT

Cyberdefense – Intégration :

DATAPROTECT offre l'intégration de solutions pour la sécurisation du poste de travail qui se matérialise par :

- La mise en place de l'antivirus
- La mise en place de solution de gestion de vulnérabilités
- La mise en place de solution de gestion des correctifs
- La mise en place de solution de prévention de fuite d'informations sensibles
- La mise en place d'outils de cryptage de données
- Définition des programmes de formation adaptés à chaque profil du personnel exploitant identifié, etc.

Gouvernance, Risk & Compliance Conseil :

Ayant mené une centaine de missions d'audit de sécurité des systèmes d'information pour le compte d'organisations exerçants dans divers domaines d'activité, DATAPROTECT dispose aujourd'hui d'un retour d'expérience très riche et varié en la matière. Des tests d'intrusion externes jusqu'à l'audit de code applicatif, en passant par les tests d'intrusion internes, l'audit des configurations, l'audit d'architecture de sécurité, l'audit de sécurité de poste de travail et l'audit organisationnel de sécurité, l'équipe DATAPROTECT est en mesure d'évaluer les différentes dimensions de la sécurité de l'information.

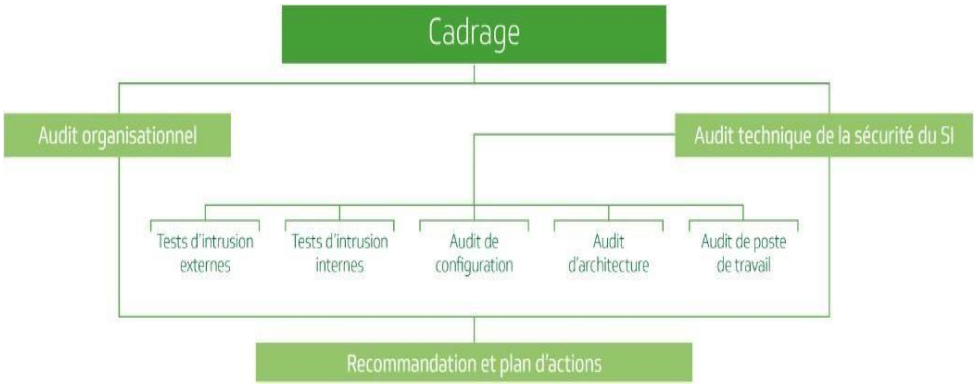


Figure 6:: Le pôle de conseil de DATAPROTECT

MSSP – Infogérance :

A la demande de plusieurs de ses clients, DATAPROTECT a mis en place un « Security Operations Center » (SOC) dont la fonction principale est de fournir des services de détection et de traitement des incidents de sécurité. Le centre de sécurité collecte ainsi les événements (sous forme de logs notamment) remontés par les composants de sécurité, les analyse, détecte les anomalies et définit des réactions en cas d'émission d'alerte. Ceci permet à DATAPROTECT d'offrir aux entreprises la possibilité d'administrer la sécurité de leur parc informatique à distance en collectant et corrélant les logs de ses différents équipements et applicatifs de sécurité (pare-feu, IDS/IPS, VPN, antivirus, etc.)

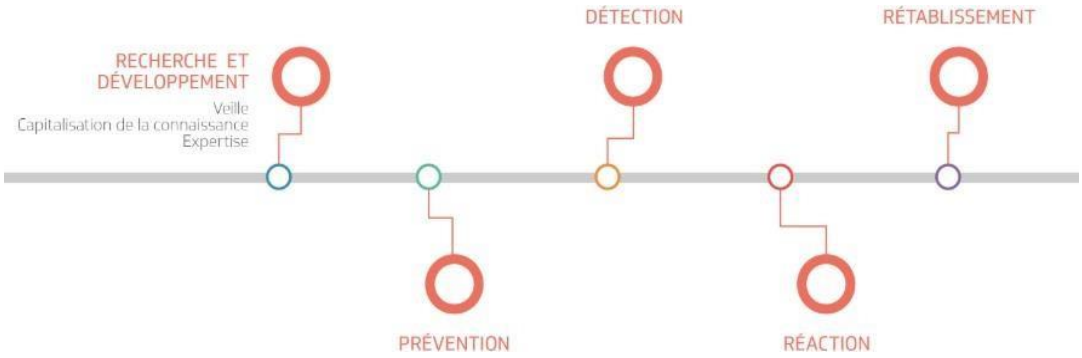


Figure 7:Le Pôle d'Infogérance de DATAPROTECT

Formation :

Les formations proposées sont particulièrement adaptées aux besoins du marché. En effet, elles touchent tous les domaines liés à la sécurité du système d'information. La liste non exhaustive suivante présente les formations dispensées par DATAPROTECT- INSTITUTE :

- Sécurité de l'information
- Management des risques IT
- Services IT
- Sécurité applicative
- Continuité d'activité
- Préparation aux Certifications
- Sensibilisation et Audit
- Protection des Données à Caractère Personnel
- Ateliers Pratiques

Recherche et développement :

Pole R et D qui s'étale sur l'ensemble de leur processus, allant de la veille des nouvelles vulnérabilités jusqu''a l'innovation de solutions spécifiques pour répondre aux différentes particularités de nos clients. Le Pole R et D permet actuellement d'améliorer l'efficacité des interventions et fait de DATAPROTECT un acteur différentiateur sur le marché de la sécurité des systèmes d'information avec une réelle valeur ajoutée.

Security Intelligence (SOC) :

DATAPROTECT a ouvert le premier SOC au Maroc en 2014 afin de répondre à une vague d'incidents parmi les opérateurs d'importance vitale. Le centre disposait alors d'une petite salle avec cinq positions de travail et trois employés à plein temps. Il assurait une veille non décalée tous les jours de 8h00 à 19h00 avec astreinte et réponse. Cette première infrastructure a cédé la place en février 2017 à une salle dotée de 12 positions et 17 collaborateurs à plein temps qui assurent une veille 24 heures sur 24 et sept jours sur sept. Aujourd'hui le SOC compte 24 collaborateurs à plein temps.

Les principales activités du SOC DATAPROTECT sont :

- Surveillance des incidents sécurité 24/7
- Assistance à la réponse aux incidents
- Ingénierie SIEM
- Infogérance des solutions de sécurité
- Maintenance préventive et curative
- Investigation et Compromise Assessment
- Veille et publication des bulletins de sécurité
- Analyse des malwares

2. Présentation du projet

2.1 Etude de l'existant :

Une étape essentielle de tout projet consiste à effectuer une étude préalable. Cette étude consiste à examiner la problématique que nous allons attaquer afin de déclarer les défaillances et les insuffisances du système. En effet, dans le cas général la mise en place d'un projet est due à un problème ou un manque. Il faut donc bien étudier l'existant pour obtenir des résultats efficaces. Afin d'approfondir notre compréhension du sujet et avoir une idée plus claire sur notre projet et ses fonctions attendues

2.2 Problématique :

Bien que les centres opérationnels de sécurité (SOC) s'appuient largement sur les outils SIEM pour surveiller les environnements Windows, la **détection réelle des attaques avancées reste un défi majeur**. Les attaquants utilisent aujourd'hui des techniques de plus en plus furtives, basées notamment sur **PowerShell, Sysmon bypassing, living-off-the-land**, ou encore des mécanismes d'exfiltration discrets difficiles à identifier dans les journaux traditionnels.

Dans ce contexte, les organisations se trouvent confrontées à une problématique centrale :
Comment détecter efficacement une attaque lorsqu'elle est menée de manière silencieuse, progressive et en utilisant des outils légitimes du système Windows ?

De plus, malgré la richesse des logs Windows (Event Logs, Sysmon, PowerShell), la **corrélation entre ces données reste complexe**, et les analystes peinent souvent à reconstruire le chemin d'attaque complet à partir des seuls journaux collectés par le SIEM.

La difficulté s'accentue face à :

- la **volumétrie importante** des événements collectés,
- la **variabilité** des formats de logs,
- l'absence de **cas d'usage SIEM suffisamment précis**,
- et l'évolution constante des techniques d'attaque documentées dans **MITRE ATT&CK**.

Ainsi, il devient essentiel d'adopter une démarche structurée de **Threat Hunting**, permettant :

- de formuler des hypothèses d'investigation,
- de rechercher activement les comportements suspects,
- de corréler les actions observées dans les logs,
- et de reconstituer une **timeline d'attaque exploitable**.

L'absence de processus standardisés pour ce type d'investigation limite considérablement la capacité des équipes SOC à réagir rapidement et efficacement. Le défi consiste alors à **simuler une attaque réelle**, à **analyser son déroulement uniquement via les logs du SIEM**, puis à **proposer des cas d'usage et recommandations capables d'améliorer la détection future**.

2.3 Gestion du projet :

Planificarion du projet :

La gestion de projet joue un rôle essentiel dans la réussite de tout travail technique. Elle permet d'assurer un bon déroulement des différentes phases, en définissant à l'avance les étapes, les délais, et les livrables associés. Dans le cadre de mon projet, j'ai adopté une planification structurée**,** reposant sur l'outil **Gantt Project**, afin de visualiser clairement l'enchaînement des tâches et de gérer efficacement le temps imparti.

Ce diagramme m'a permis de découper le projet en plusieurs phases clés : étude du besoin, analyse, conception de l'environnement, mise en œuvre technique, tests, validation et rédaction du rapport. Pour chaque tâche, j'ai défini une durée, des dates de début et de fin, ainsi que les dépendances entre les étapes.

Grâce à cette méthode, j'ai pu suivre l'avancement du projet de manière continue**,** identifier les retards potentiels, et ajuster mon planning si nécessaire. Le diagramme de Gantt constitue donc un outil de pilotage central, qui m'a accompagnée tout au long de la réalisation de ce projet.

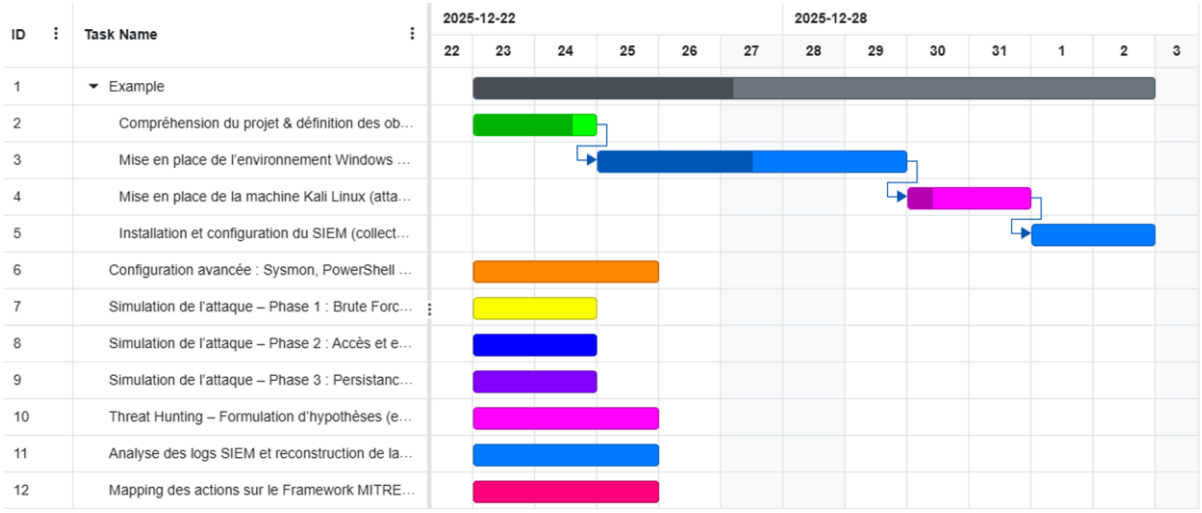


Figure 8:Representation de la liste des taches sous forme de diagramme de Gant

2.4 Objectifs du stage :

Dans un contexte où les cyberattaques deviennent de plus en plus sophistiquées, **DataProtect** vise à renforcer la détection des incidents sur les environnements Windows. Ce projet consiste à **simuler et analyser une attaque de type brute force suivie d'exfiltration de données**, en exploitant uniquement les **logs collectés par le SIEM** (Event Logs, Sysmon, PowerShell, réseau). L'objectif est de **reconstituer la timeline de l'attaque, identifier les comportements suspects et proposer des règles SIEM efficaces**, tout en améliorant la réactivité et la couverture de détection des analystes SOC.

Conclusion :

À l'issue de ce premier chapitre, notre projet de **Threat Hunting sur un environnement Windows** est clairement ancré dans son contexte. Nous avons présenté l'organisation d'accueil, **DataProtect**, et défini les enjeux liés à la détection des attaques sophistiquées, telles que les **brute force suivis d'exfiltration de données**. Nous avons également exposé la **démarche adoptée pour simuler l'attaque, analyser les logs via le SIEM et reconstruire la timeline des événements**, afin de renforcer la visibilité et la réactivité des analystes SOC. Les chapitres suivants détailleront les besoins, les objectifs et les étapes techniques pour atteindre une couverture optimale de détection et proposer des cas d'usage SIEM adaptés.

Chapitre 2 : Environnement de travail, outils Et technologies utilisées

Introduction :

Ce chapitre présente l'environnement technique mis en place pour la réalisation de notre projet. Il détaille les machines virtuelles utilisées, les outils de virtualisation, ainsi que les logiciels et framework déployés pour assurer la collecte, l'analyse et la visualisation des journaux système.

L'objectif est de montrer comment ces composants interagissent pour former un environnement cohérent, propice à la détection d'anomalies de sécurité dans un système. Nous décrivons également les technologies de journalisation et les référentiels de cybersécurité utilisés pour évaluer et améliorer la visibilité des activités système.

1. Virtual Machines (VM) :

Les machines virtuelles permettent de créer un environnement de test isolé, sécurisé et entièrement contrôlé. Dans ce projet, les VM ont été utilisées pour simuler une attaque réelle sans impacter un système physique. Elles facilitent également la reproduction des scénarios d'attaque, l'analyse des logs et la reconstruction de la timeline.

VM utilisées :

- **Windows Server** : machine victime de l'attaque brute force et de l'exfiltration.
- **Kali Linux** : machine attaquante utilisée pour lancer les attaques et générer l'activité malveillante.

2. Windows server (VM) :

Windows Server constitue la machine cible dans notre scénario.
Il s'agit d'un système très répandu dans les environnements professionnels, souvent exposé à des attaques RDP et à des tentatives d'accès non autorisées.

3. Kali linux (VM) :

Kali Linux est une distribution dédiée au pentesting et à l'audit de sécurité.
Elle intègre de nombreux outils offensifs permettant de simuler différents types d'attaques.

4. Hydra :

Hydra est un outil de force brute très connu, capable de tester rapidement un grand nombre de mots de passe sur différents protocoles (SSH, FTP, RDP…).

5. Sysmon :

Sysmon est un composant de la suite Sysinternals permettant d'améliorer la visibilité sur les comportements système.
Il offre une journalisation avancée, notamment sur :

- la création de processus,
- les connexions réseau,
- les modifications de fichiers,
- les chargements de DLL,
- et les hash des exécutables.

6. Framework MITRE ATT&CK :

Le **framework MITRE ATT&CK** est une base de connaissances des techniques d'attaque utilisées par les cybercriminels. Il est largement adopté dans le monde de la cybersécurité pour **cartographier les événements** à des comportements malveillants connus.Dans ce projet, MITRE ATT&CK a été utilisé comme **référentiel** pour analyser les journaux collectés et les associer à des techniques d'attaque précises (ex : T1078 – Valid Accounts, T1053 – Scheduled Task/Job). Cela permet d'**évaluer la couverture de détection** et d'identifier les lacunes dans la supervision des systèmes Linux.

Figure 9:une capture du site MITRE ATT&CK avec un exemple de technique mappée

Conclusion :

L'environnement de travail mis en place repose sur une architecture flexible et réaliste, permettant de simuler un poste Linux supervisé dans un contexte de SOC. L'utilisation de machines virtuelles, combinée à des outils comme Filebeat, Elastic Stack et Auditd, a permis de collecter efficacement les événements système et de les analyser en profondeur.
Le recours au framework MITRE ATT&CK a renforcé cette approche en fournissant une grille de lecture normalisée des comportements malveillants. Ces fondations techniques constituent un socle solide pour les chapitres suivants, orientés vers la détection des anomalies et les réponses automatisées.

Chapitre 3 : Threat Hunting En Cybersécurité

1) Introduction :

Le **Threat Hunting**, ou chasse aux menaces, est une approche proactive de la cybersécurité qui consiste à rechercher activement des signes d'attaques, de comportements anormaux ou de compromissions potentielles *avant même qu'une alerte ne soit déclenchée* par les outils traditionnels.

Contrairement aux systèmes automatisés comme les SIEM, IDS/IPS ou antivirus, qui attendent qu'un évènement se produise pour le signaler, le Threat Hunting adopte une posture **active et anticipative**. L'objectif est d'identifier des menaces **cachées, avancées ou silencieuses**, souvent difficiles à détecter par des alertes classiques.

Le threat hunter s'appuie sur :

- L'analyse comportementale,
- L'intuition et l'expertise,
- Des hypothèses basées sur les renseignements de menaces,
- La corrélation de données massives (SIEM, logs système, réseau, EDR…),
- Des techniques structurées comme **l'ACH**, MITRE ATT&CK, Sigma, YARA…

En résumé :

Le Threat Hunting transforme la cybersécurité de réactive à proactive.

2) Analysis of Competing Hypotheses (ACH):

- **Définition :**

Est une technique analytique structurée qui vous permet de prendre des décisions solides grâce à un raisonnement logique et une évaluation critique. Elle consiste à comparer et à confronter plusieurs hypothèses afin de produire une explication la plus complète possible, basée sur les preuves disponibles.

3) Les 8 étapes de la méthode ACH :

- **Identifier les hypothèses possibles**

Formule toutes les explications plausibles d'un événement ou d'un problème.
Ne pas chercher *une seule* hypothèse, mais **toutes** les hypothèses réalistes

- **Lister toutes les preuves et informations disponibles**

Rassemble les données, indicateurs, preuves, logs, renseignements ou témoignages.
Inclut aussi les **informations manquantes ou incertaines**.

- **Examiner la cohérence de chaque preuve avec chaque hypothèse**

Crée un tableau où tu compares :

- chaque **preuve**
- avec chaque **hypothèse**

Objectif : savoir si la preuve **confirme**, **réfute**, ou **n'a pas d'impact** sur l'hypothèse

- **Chercher les preuves qui réfutent plutôt que celles qui confirment**

L'ACH donne plus d'importance aux **éléments qui contredisent une hypothèse**, car :

- un élément contradictoire peut éliminer une hypothèse
- un élément confirmant ne suffit pas pour dire qu'elle est vraie

C'est la logique du **diagnostic différentiel**.

- **Éliminer les hypothèses incompatibles avec les preuves**

Écarte d'abord les hypothèses qui présentent **le plus d'incohérences**.
Conserve celles qui **résistent** le mieux à la confrontation des preuves.

- **Déterminer la probabilité relative de chaque hypothèse restante**

Les hypothèses non éliminées sont classées selon :

- leur cohérence
- la solidité des preuves
- les incertitudes restantes

On n'obtient jamais une certitude à 100 %, mais une **probabilité relative**.

- **Documenter les conclusions et les justifier**

Formule un rapport clair indiquant :

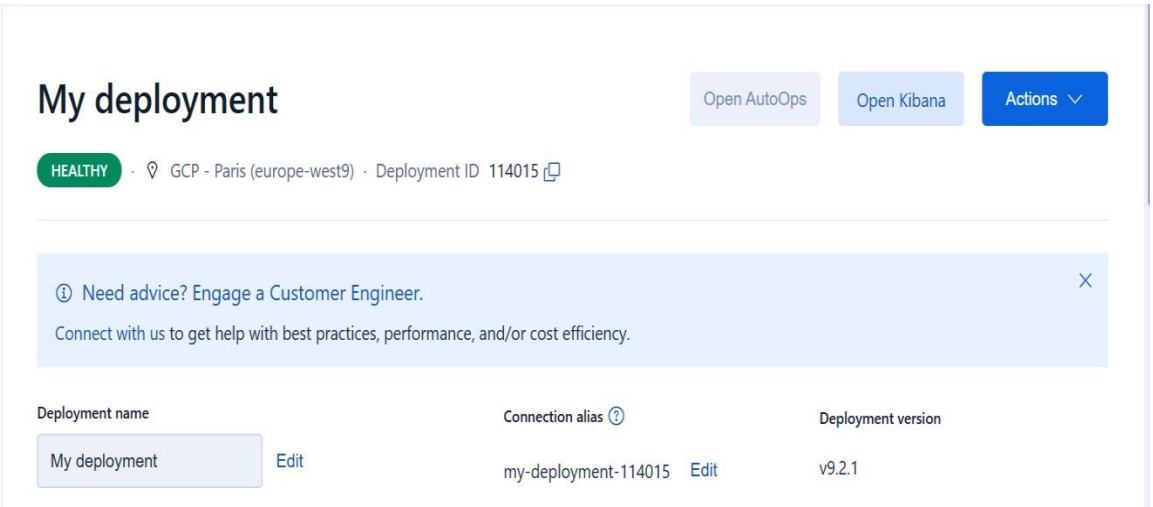
- l'hypothèse la plus probable
- celles rejetées et pourquoi
- les preuves clés
- les limites et incertitudes

C'est essentiel dans la cyber threat intelligence, le renseignement ou la prise de décision

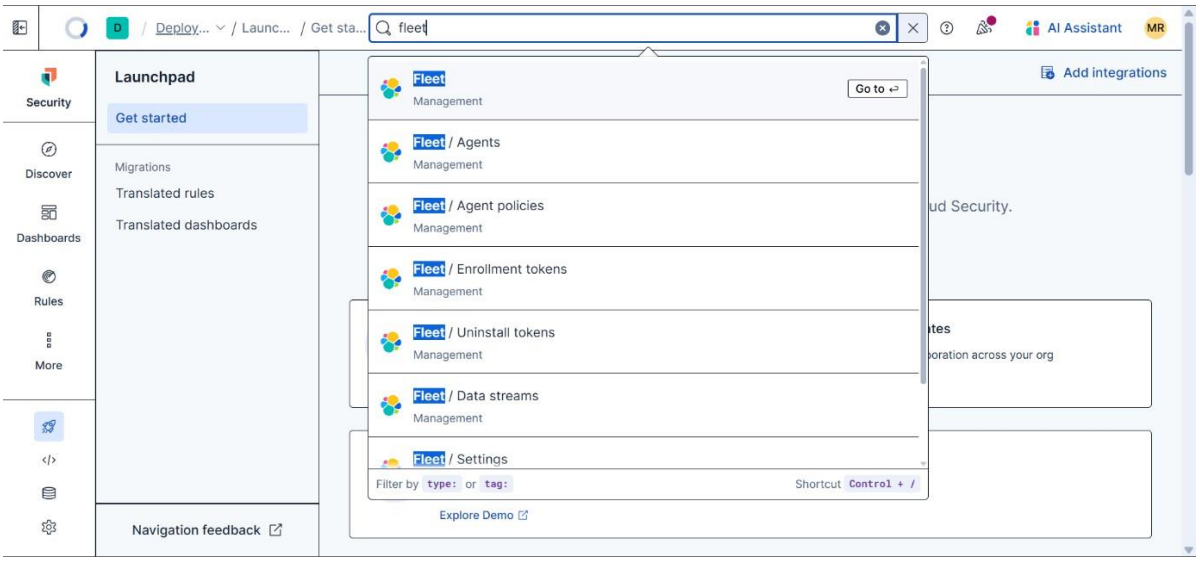
Chapitre 4 : Déploiement d'Elastic Security dans le Cloud

1. Création du déploiement Cloud

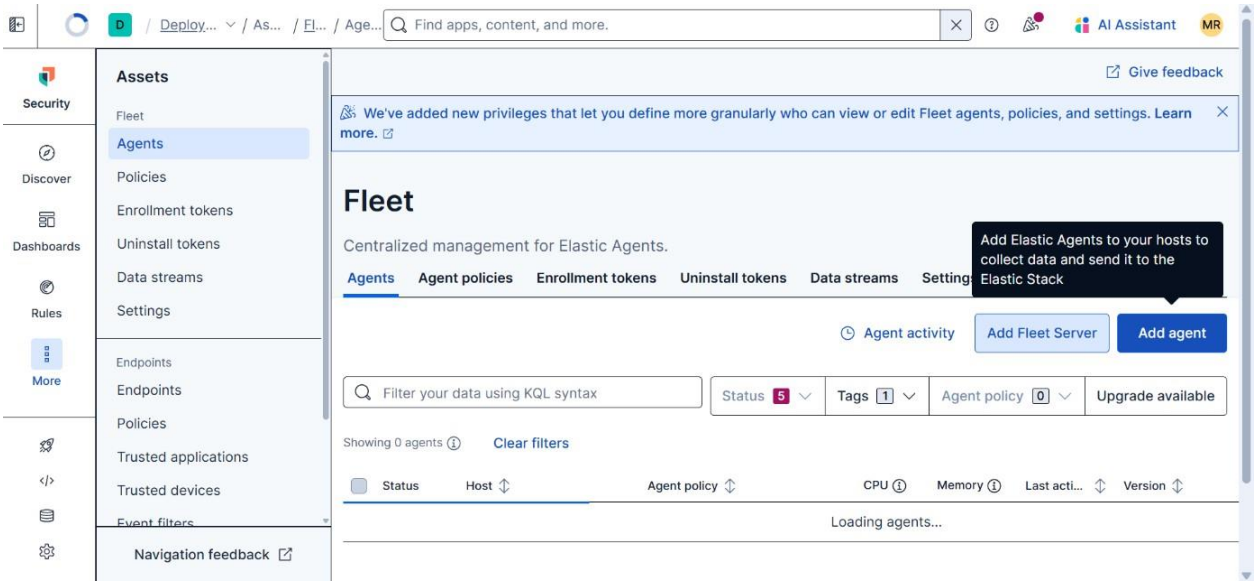
Activation centralisée de la suite de sécurité via le portail Elastic Cloud. Configuration unifiée des modules SIEM, Endpoint Security et détection cloud



Fleet est l'interface centrale de Kibana pour déployer et gérer facilement vos agents Elastic à grande échelle. Idéale pour collecter, surveiller et sécuriser vos données via une console unifiée et intuitive.

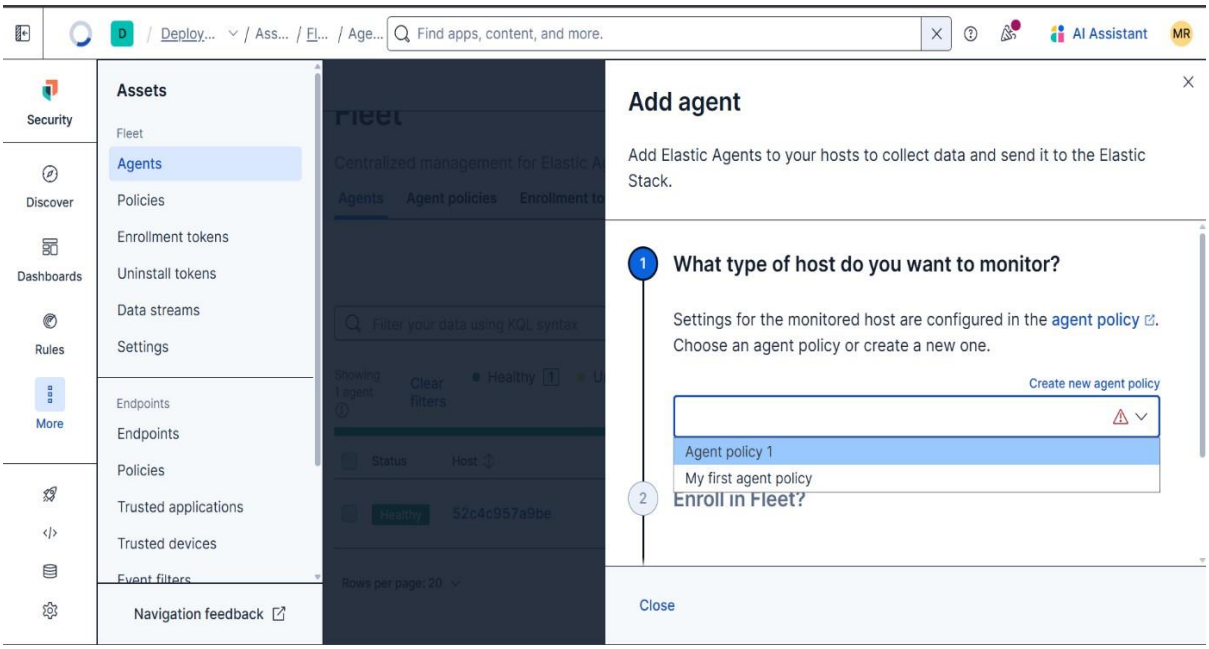


Fleet est le centre de contrôle pour déployer et superviser vos **Elastic Agents** depuis une interface unique. Ajoutez des agents à vos hôtes pour collecter des données et les envoyer vers la Stack Elastic de manière centralisée et sécurisée

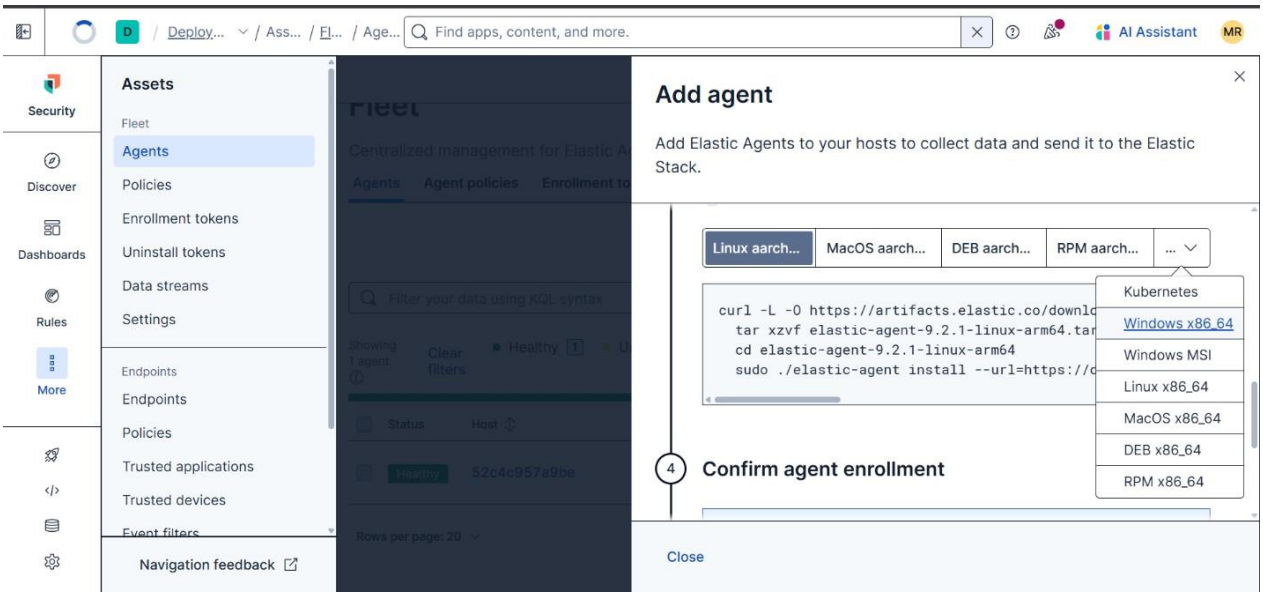


1. Installation et configuration des agents sur Windows 10

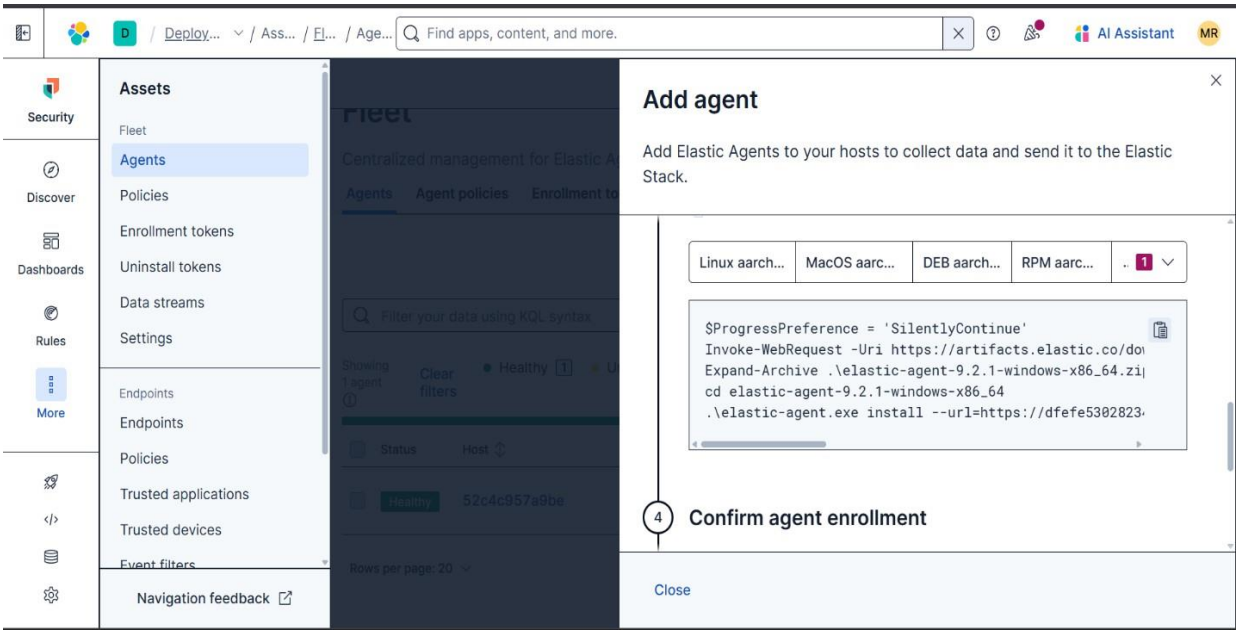
Après avoir sélectionné la politique d'agent souhaitée, vous configurez les paramètres nécessaires avant d'enrôler l'hôte dans Fleet. Une fois l'enrôlement effectué, l'agent commence à collecter les données et à les envoyer vers l'Elastic Stack.



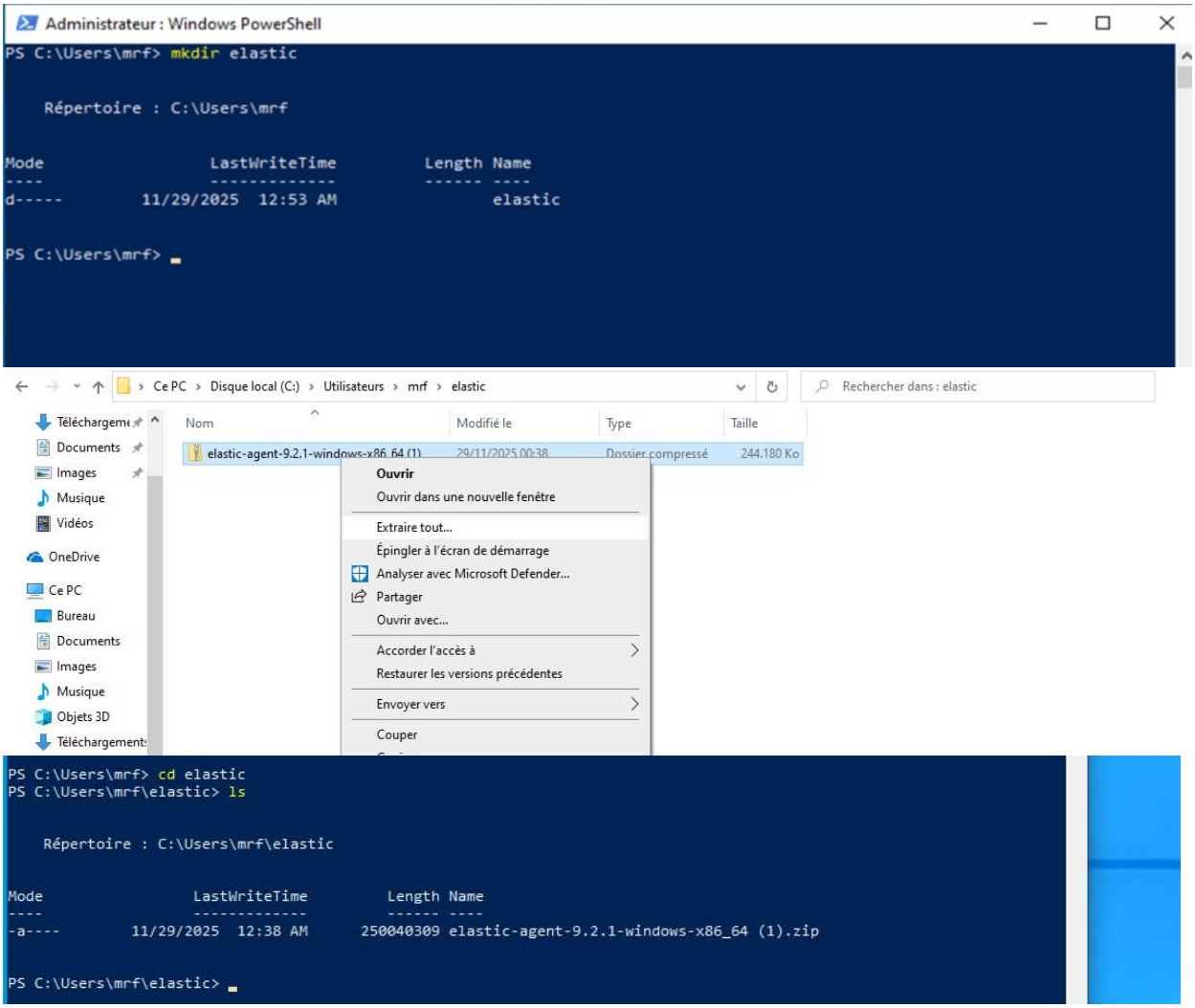
Une fois que l'option **Windows x86_64** est sélectionnée, il suffit d'exécuter la commande d'installation de l'agent Elastic sur votre machine Windows. Cette étape permet à l'agent de commencer à collecter des données et de les envoyer vers l'Elastic Stack pour une gestion centralisée.



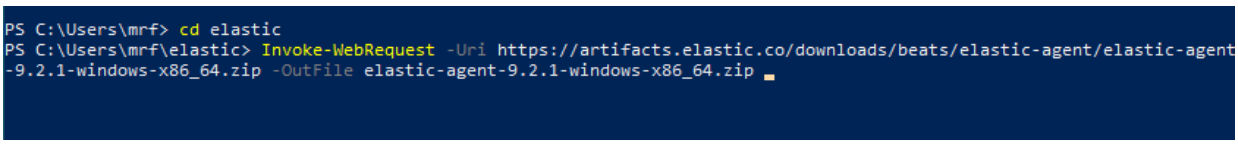
Une fois l'option Windows x86_64 sélectionnée, vous devez exécuter la commande PowerShell affichée, qui télécharge et extrait l'agent Elastic sur votre machine. Après cela, l'agent est installé et configuré pour envoyer des données vers l'Elastic Stack, vous permettant ainsi de surveiller et de collecter des informations en temps réel.



Exécute la commande PowerShell mkdir elastic pour créer un répertoire nommé "elastic" dans le dossier C:\Users\mrf. Ce répertoire servira à stocker les fichiers nécessaires à l'installation de l'agent Elastic, préparant ainsi le système à recevoir et à déployer l'agent.

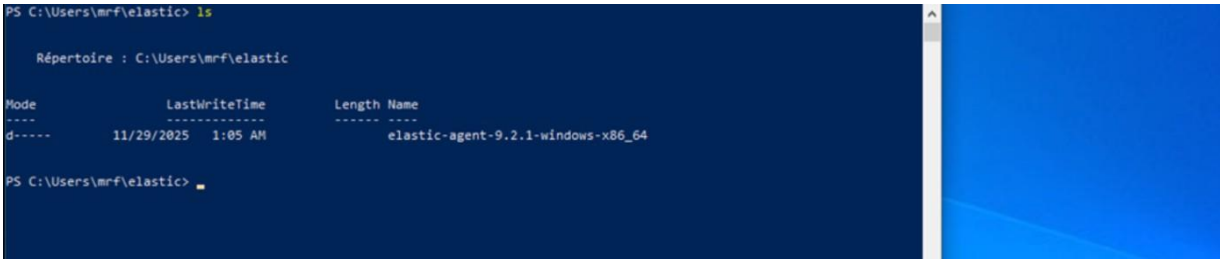


L'utilisateur télécharge l'archive de l'agent Elastic en exécutant la commande Invoke-WebRequest dans le répertoire "elastic". Ce fichier sera utilisé pour l'installation de l'agent sur la machine.

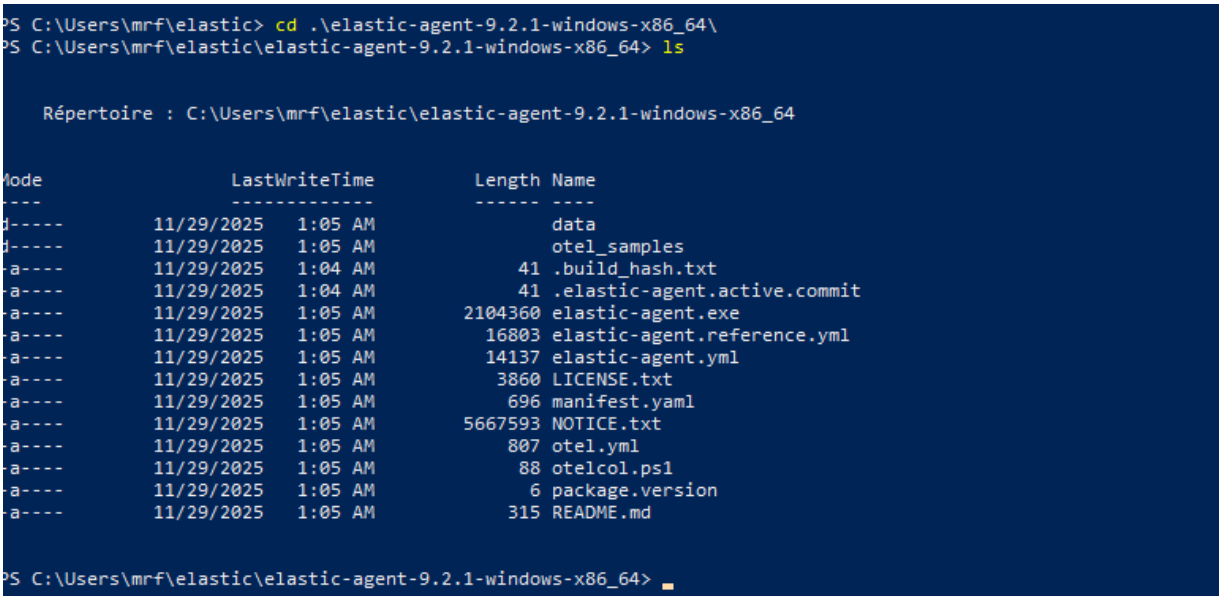


Vérifie le répertoire "elastic" avec la commande ls pour s'assurer que le fichier téléchargé, "elastic- agent-9.2.1-windows-x86_64.zip", est bien présent. Le fichier est prêt à être extrait et installé.

Clic droit sur le fichier compressé "elastic-agent-9.2.1-windows-x86_64.zip" et sélectionne l'option "Extraire tout..." pour décompresser le fichier et préparer l'installation de l'agent Elastic.



Vérifie le répertoire "elastic" avec la commande ls pour s'assurer que l'archive décompressée "elastic- agent-9.2.1-windows-x86_64" est présente. Cela confirme que l'extraction a réussi et que les fichiers nécessaires à l'installation de l'agent sont prêts.

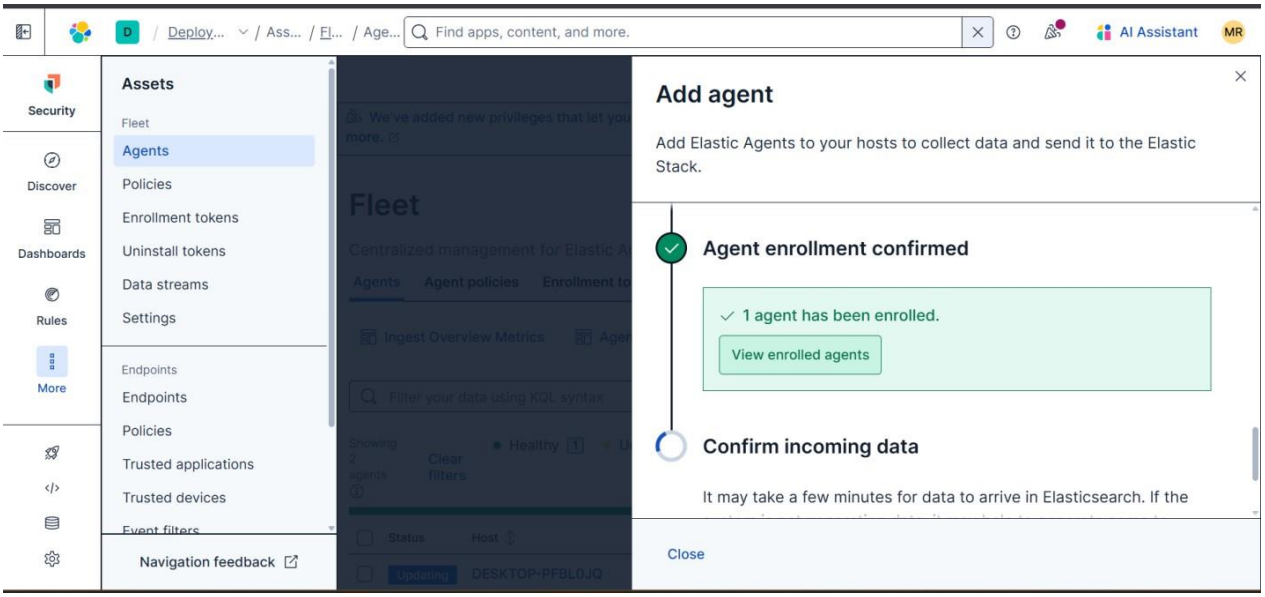


Accède au répertoire décompressé de l'agent Elastic et utilise la commande ls pour afficher son contenu. Ce répertoire contient plusieurs fichiers nécessaires à l'exécution et à la configuration de l'agent, y compris "elastic-agent.exe" et divers fichiers de configuration.

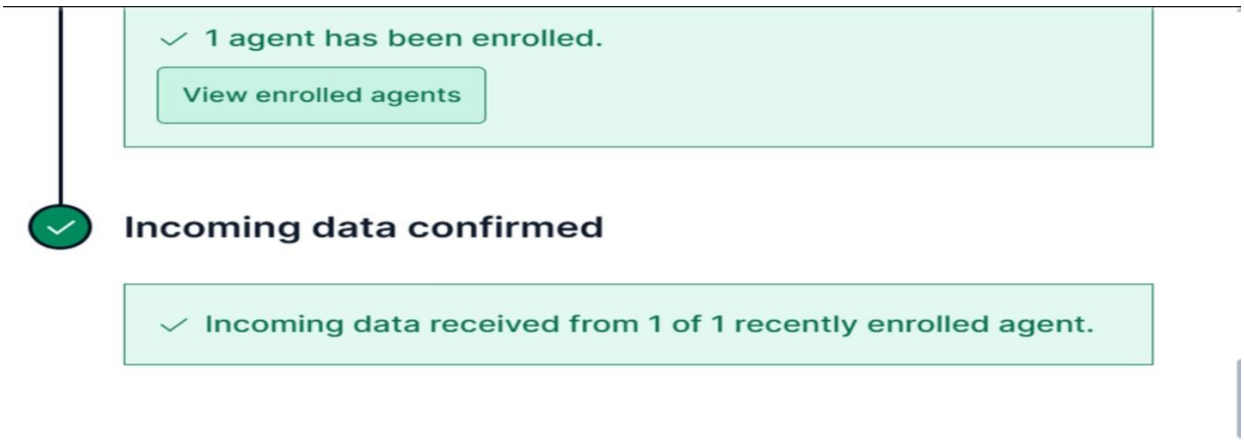
Exécute la commande elastic-agent.exe installé dans PowerShell pour installer l'agent Elastic, en spécifiant l'URL du serveur Fleet et un jeton d'enrôlement pour connecter l'agent au système. Cette étape finalise l'installation et lie l'agent à l'Elastic Stack.

```
S C:\Users\mrf\elastic\elastic-agent-9.2.1-windows-x86_64> .\elastic-agent.exe install --url=https://dfefe53028234619a
5bee58a0315f6.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=dUdGbXlwb0JXUExobzdOek9MS0U6eVNpbXUzbG1zLWxid1Z
1hRRHlIZw==
lastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [
n]:Y
 ===] Service Started  [4s] Elastic Agent successfully installed, starting enrollment.
==   ] Waiting For Enroll...  [5s] {"log.level":"info","@timestamp":"2025-11-29T01:09:43.073+0100","log.origin":{"funct
n":"github.com/elastic/elastic-agent/internal/pkg/agent/application/enroll.EnrollWithBackoff","file.name":"enroll/enro
.go","file.line":86},"message":"Starting enrollment to URL: https://dfefe53028234619a715bee58a0315f6.fleet.us-central1
cp.cloud.es.io:443/","ecs.version":"1.6.0"}
=    ] Waiting For Enroll...  [5s]
```

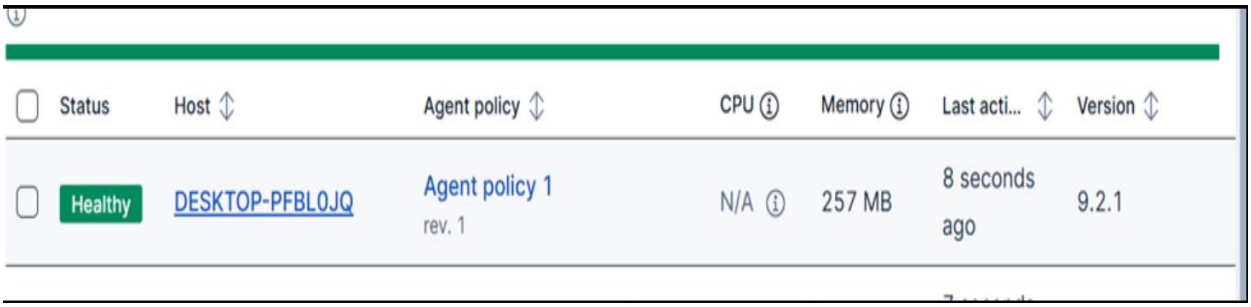
Confirme l'installation de l'agent Elastic, qui sera exécuté en tant que service sur la machine. L'agent commence le processus d'enrôlement en se connectant à l'URL du serveur Fleet spécifiée.



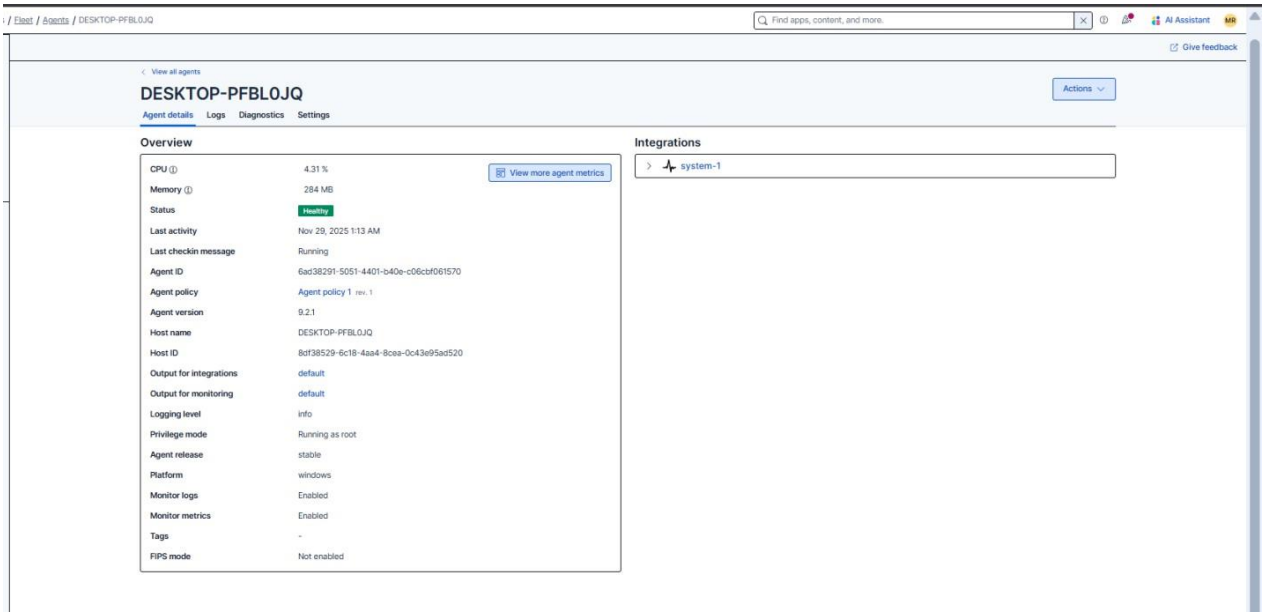
Reçoit la confirmation que l'agent a été enrôlé avec succès dans Fleet, comme indiqué par le message "1 agent has been enrolled". L'enrôlement est maintenant terminé et l'agent commence à envoyer des données vers l'Elastic Stack.



Reçoit la confirmation que les données de l'agent récemment enrôlé ont été reçues avec succès par le système. Cela indique que l'agent fonctionne correctement et transmet les données vers l'Elastic Stack.



L'agent Elastic est maintenant actif et en bonne santé, comme indiqué par le statut "Healthy" dans l'interface Fleet. L'agent a été associé à la politique "Agent policy 1" et fonctionne correctement sur l'hôte spécifié.



Consulte maintenant l'interface de gestion de l'agent Elastic, où les détails de l'agent "DESKTOP- PFBLOJQ" sont affichés, confirmant son statut "Healthy". L'agent fonctionne sous la version 9.2.1 et est correctement intégré pour la collecte de données

2. Activation des intégrations (Winlogbeat, Sysmon, PowerShell)

Navigue vers le répertoire "downloads" et utilise la commande ls pour afficher les fichiers présents. Je vois l'archive "elastic-agent-9.2.1-windows-x86_64.zip" ainsi qu'un autre fichier nommé "Sysmon.zip".

```
PS C:\Users\mrf> cd downloads
PS C:\Users\mrf\downloads> ls


    Répertoire : C:\Users\mrf\downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/29/2025  12:38 AM      250040309 elastic-agent-9.2.1-windows-x86_64 (1).zip
-a----         11/28/2025   7:09 PM        4866436 Sysmon.zip


PS C:\Users\mrf\downloads>
```

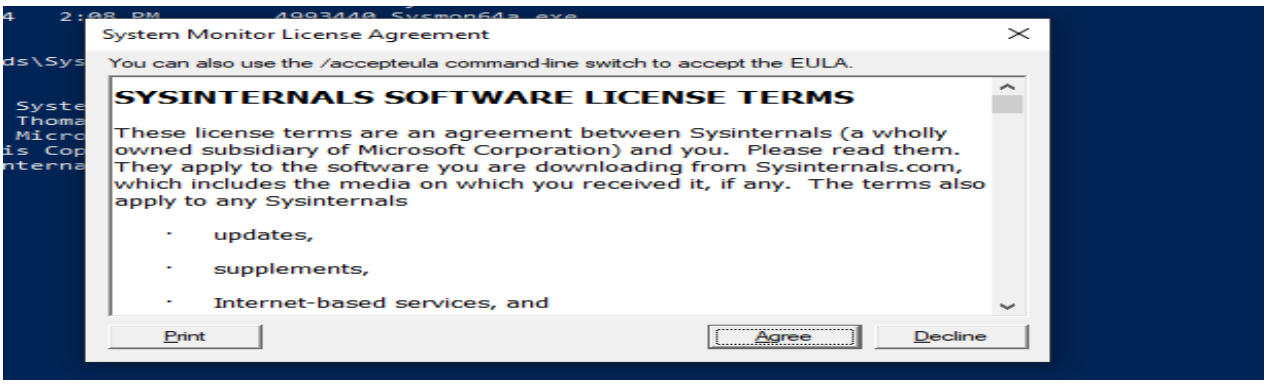
Décompresse le fichier "Sysmon.zip" à l'aide de la commande Expand-Archive, puis je me déplace dans le répertoire décompressé "Sysmon". Cela prépare les fichiers nécessaires pour l'installation ou la configuration de Sysmon.

```
PS C:\Users\mrf\downloads> Expand-Archive .\Sysmon.zip
PS C:\Users\mrf\downloads> ls


    Répertoire : C:\Users\mrf\downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         11/29/2025   1:17 AM                Sysmon
-a----         11/29/2025  12:38 AM      250040309 elastic-agent-9.2.1-windows-x86_64 (1).zip
-a----         11/28/2025   7:09 PM        4866436 Sysmon.zip


PS C:\Users\mrf\downloads> cd .\Sysmon\
PS C:\Users\mrf\downloads\Sysmon>
```

Je lance l'exécution de "Sysmon64.exe" avec l'option -i pour installer Sysmon sur la machine. Ce processus permet de configurer le monitoring des activités système à l'aide de Sysmon.

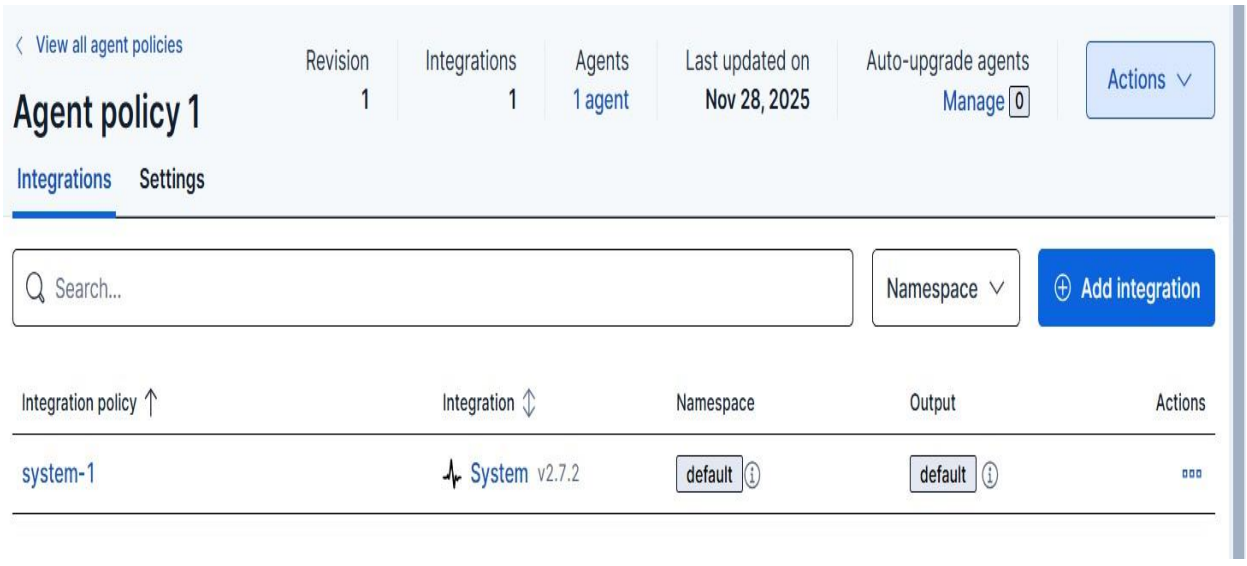
```
PS C:\Users\mrf\downloads\Sysmon> .\Sysmon64.exe -i

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
```

Je vois que le processus d'installation de Sysmon a été complété avec succès, après avoir accepté le contrat de licence. Ensuite, Sysmon et ses composants ont été démarrés sur la machine, et l'installation est maintenant terminée.



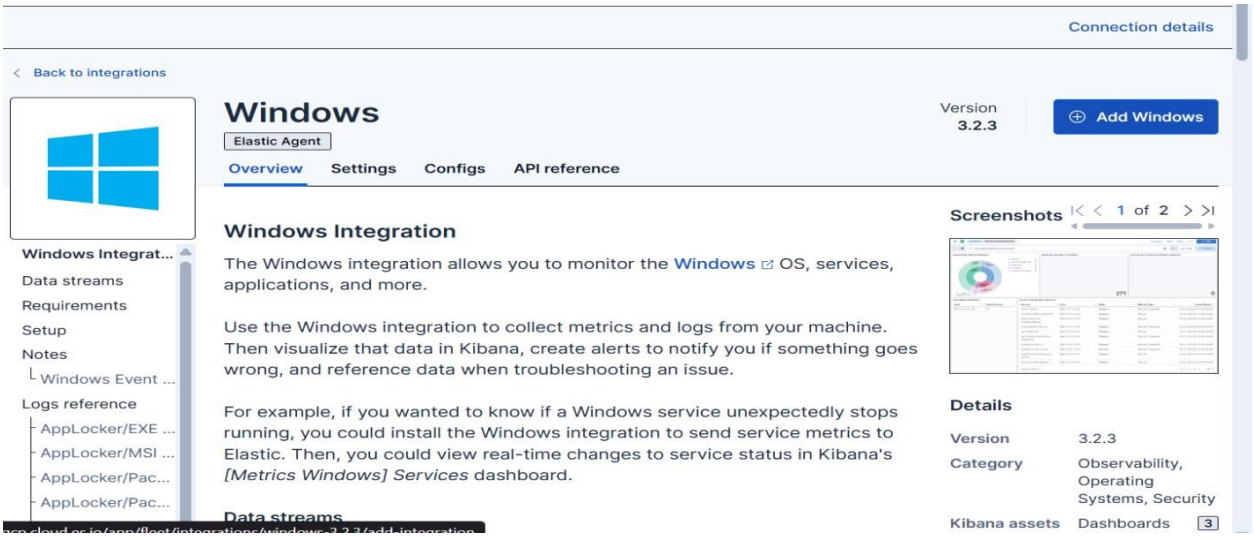
Dans ces captures, je vérifie que le service Sysmon est en cours d'exécution en utilisant la commande Get-Service dans PowerShell. Cela confirme que le service Sysmon a été correctement démarré et est actif sur la machine.

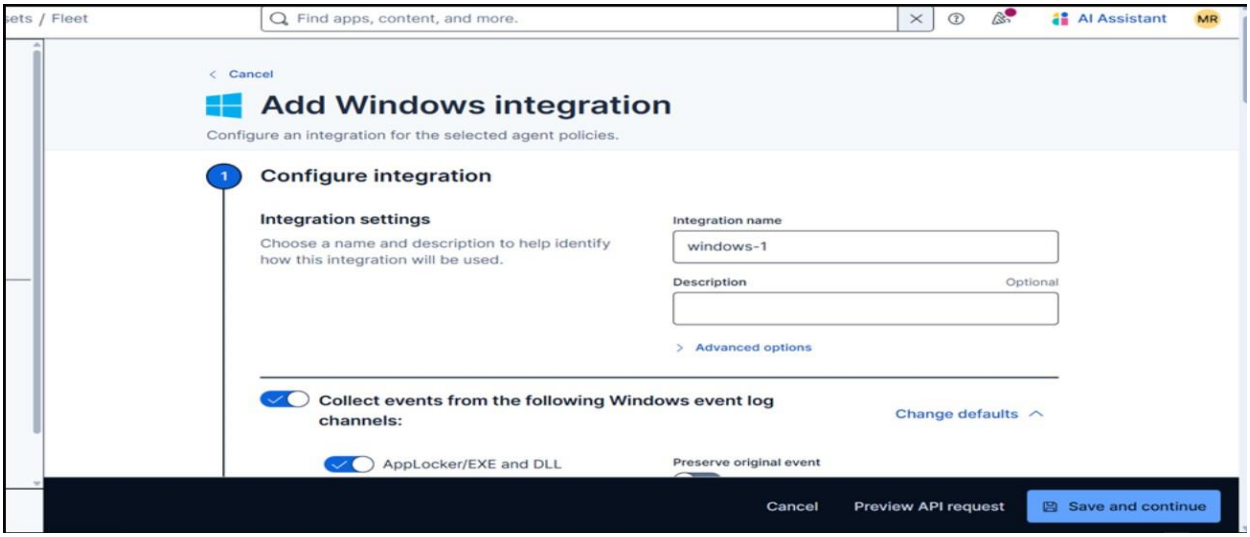
Je consulte les politiques d'agents dans l'interface Fleet. Dans la première image, je vois que la politique "Agent Policy 1" inclut l'intégration "system-1". Dans la deuxième image, je vérifie les différentes politiques d'agents, où "Agent Policy 1" est mise à jour avec la dernière version.



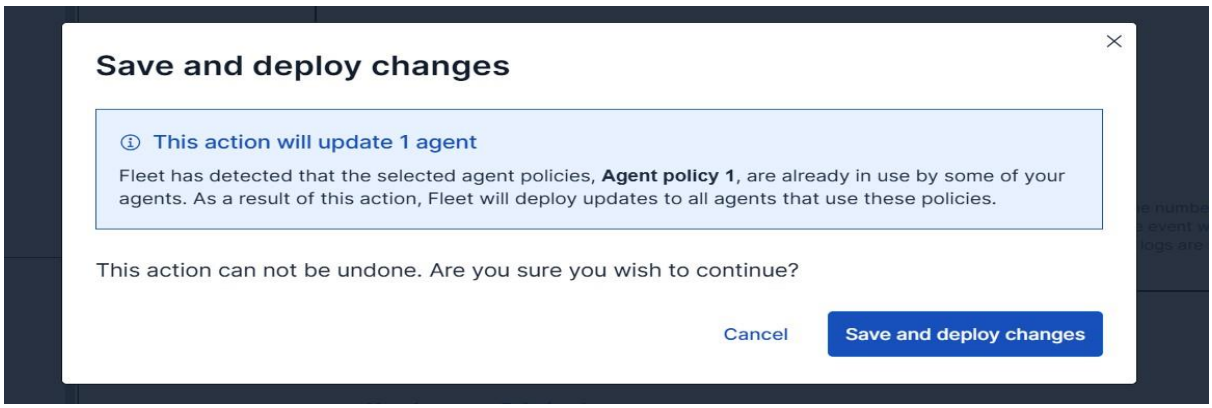
3. Intégration de la machine Windows dans le SIEM

Je consulte l'intégration Windows pour l'Elastic Agent. Dans la première image, je vois une vue d'ensemble de l'intégration Windows, permettant de collecter des métriques et des journaux système. Dans la deuxième image, je configure l'intégration Windows pour collecter des événements depuis les canaux de journalisation, en activant l'option "AppLocker/EXE et DLL" pour le suivi des événements liés à la sécurité.





Je vois un message de confirmation dans l'interface Fleet, indiquant que l'action de déploiement mettra à jour la politique d'agent "Agent policy 1" déjà utilisée par un agent. Je dois confirmer si je souhaite continuer à déployer ces changements sur les agents existants.



Chapitre 5 : Tests, expérimentation et processus de Threat Hunting

Introduction :

Ce chapitre présente en détail la phase de mise en œuvre technique du projet. Après avoir défini l'architecture et les composants nécessaires dans les chapitres précédents, il est désormais question de passer à la réalisation concrète du système.

Cette partie inclut l'installation et la configuration des environnements virtuels (Ubuntu, Windows), l'intégration des outils de collecte et de visualisation de logs comme Wazuh, Filebeat et Elasticsearch

1) Scénario De Notre Attaque :

- Les hypothèses possibles (ACH – Phase 1)

H1 — Activité administrative légitime
L'activité observée pourrait être celle d'un administrateur effectuant une maintenance.

H2 — Activité automatisée ou mauvaise configuration
Un processus automatique, tâche planifiée ou un service système pourrait être responsable.

H3 — Accès non autorisé utilisant des identifiants valides
Un attaquant externe a pu utiliser des identifiants compromis pour effectuer une connexion puis une compromission.

H4 — Malware ou exploitation automatique
Une infection ou un exploit automatique pourrait avoir déclenché l'activité.

- Liste complète des preuves et informations disponibles (ACH – Phase 2)

Voici **toutes les preuves**, extraites de ton texte :

P1 — Logons depuis une source inhabituelle
(= pas un poste admin connu)

P2 — PowerShell encodé / obfusqué
(= pas normal pour un admin)

P3 — Activité ne correspondant pas aux procédures administratives

P4 — PowerShell interactif détecté
(= pas automatisé)

P5 — Commandes reflétant une reconnaissance manuelle

P6 — Aucun scheduled task légitime associé à l'activité

P7 — Kerberos PreAuthType = 0 (AS-REP Roasting possible)

P8 — Authentifications interactives réussies sur le Domain Controller

P9 — PowerShell encodé immédiatement après l'authentification

P10 — Reconnaissance : énumération des privilèges, recherche de backups

P11 — Création d'une scheduled task pour persistance

P12 — Exfiltration de données par petites portions

P13 — Aucun binaire malveillant détecté

P14 — Activité utilisant uniquement des outils natifs (Living-off-the-land)

P15 — Comportement "hands-on-keyboard" (= humain, pas malware)

- ## Tableau ACH complet (ACH – Phase 3 : preuve vs hypothèse)

  ✔ = cohérent
  ✘ = contredit l'hypothèse
  — = neutre

Preuve / Hypothèse	H1 Admin légitime	H2 Automatique / misconfig	H3 Attaquant externe	H4 Malware / exploit
P1 **Logons source inconnue**	✘	✘	✔	—
P2 **PowerShell encodé**	✘	✘	✔	—
P3 **Non conforme aux procédures admin**	✘	—	✔	—
P4 **PowerShell interactif**	✘	✘	✔	✘
P5 **Reconnaissance manuelle**	✘	✘	✔	✘
P6 **Pas de tâche planifiée légitime**	✔	✘	✔	—
P7 **PreAuthType 0 (AS-REP Roasting)**	✘	—	✔	—
P8 **Logon interactif sur DC**	✘	✘	✔	✘
P9 **PowerShell encodé après logon**	✘	✘	✔	—
P10 **Reconnaissance Active Directory**	✘	✘	✔	✘
P11 **Création d'une tâche malveillante**	✘	✘	✔	—
P12 **Exfiltration de données**	✘	✘	✔	✔
P13 **Aucun malware trouvé**	✔	✔	✔	✘
P14 **Living-off-the-land**	✘	✘	✔	✘
P15 **Interaction humaine (hands-on-keyboard)**	✘	✘	✔	✘

- ## Synthèse rapide(ACH – Phase 4)

- **H1 – Activité admin légitime** → ✘ rejetée (incohérence totale)
- **H2 – Processus automatique** → ✘ rejetée (activité humaine détectée)
- **H3 – Accès non autorisé (valid credentials)** → ✔ **hypothèse la plus soutenue**
- **H4 – Malware/exploit** → possible mais peu cohérent

- ## Conclusion (ACH – Phase 5)

L'hypothèse la plus probable est H3 : accès non autorisé avec identifiants valides, suivi d'une compromission du serveur.
Toutes les preuves convergent vers une attaque **réelle, interactive et manuelle**, avec :

- Exploitation Kerberos
- Logons interactifs
- Reconnaissance PowerShell
- Création de persistance
- Exfiltration lente et discrète

Perspectives

À l'issue de ce projet, plusieurs perspectives d'évolution se dégagent afin de renforcer la qualité du threat hunting et d'améliorer la posture globale de détection au sein d'un SOC. Une première piste consiste à **élargir le périmètre des attaques simulées**. En effet, si ce travail s'est concentré sur un scénario complet allant du brute force à l'exfiltration de données, d'autres techniques pourraient être explorées telles que le mouvement latéral, l'élévation de privilèges, la création de mécanismes de persistance ou encore la compromission via scripts PowerShell plus avancés.
L'intégration d'un **automate de réponse orchestrée (SOAR)** constitue également une évolution naturelle. Cela permettrait de déclencher des actions automatiques, comme le blocage d'adresses IP suspectes, la suspension d'un compte compromis ou l'isolation de la machine victime, réduisant ainsi drastiquement le temps de réaction des équipes SOC.

Par ailleurs, l'utilisation de **modèles d'analyse comportementale** et d'outils basés sur l'intelligence artificielle pourrait être introduite pour détecter de manière proactive les anomalies subtiles qui échappent aux règles SIEM classiques. L'ajout de techniques de machine learning, notamment pour la détection des comportements inhabituels ou des anomalies réseau, permettrait d'améliorer encore la précision et la pertinence des alertes.
Une autre perspective concerne l'**enrichissement des logs collectés**. L'intégration de sources additionnelles telles que les journaux de pare-feu, les flux NetFlow ou les traces d'EDR permettrait d'obtenir une visibilité plus complète et de faciliter la corrélation inter-systèmes.

Enfin, la mise en place d'une **plateforme de simulation d'attaques (Breach & Attack Simulation – BAS)** pourrait permettre d'évaluer de manière continue l'efficacité des règles SIEM, de tester automatiquement la résilience du système face à des scénarios variés et de renforcer la maturité opérationnelle du SOC.
L'ensemble de ces perspectives ouvre de nombreuses opportunités pour poursuivre ce travail et contribuer à une détection plus avancée, plus rapide et plus intelligente des cybermenaces dans des environnements toujours plus complexes.

Bibliographie

DataProtect – À propos de l'entreprise
https://www.dataprotect.ma/about.html
Consulté le 22 décembre 2025

MITRE ATT&CK Navigator – Cartographie des techniques d'attaque
https://mitre-attack.github.io/attack-navigator/
Consulté le 23 décembre 2025

Crowdstrike – Journaux d'audit et SIEM nouvelle génération
https://www.crowdstrike.com/fr-fr/cybersecurity-101/next-gen-siem/audit-logs/
Consulté le 23 décembre 2025

AtooBlog – Techniques d'analyse avancée de logs sous Unix/Linux
https://atooblog.com/actu/quelles-techniques-utiliser-pour-lanalyse-avancee-de-logs-dans-les-systemes-unix-linux/
Consulté le 24 décembre 2025

Elastic Security – Guide des détections et permissions
https://www.elastic.co/guide/en/security/8.18/detections-permissions-section.html
Consulté le 26 décembre 2025

Elastic Cloud – Connexion à la plateforme
https://cloud.elastic.co/login?redirectTo=%2Fhome
Consulté le 27 décembre 2025

Elastic Cloud – Fleet & Agents (gestion des agents)
https://my-security-project-c4d12f.kb.europe-west1.gcp.elastic.cloud/app/fleet/agents
Consulté le 28 décembre 2025

Interface Kibana – Accès local via IP
http://192.168.73.135:5601
Consulté le 29 décembre 2025

Analysis of competing hypothese (Video YouTube)
https://youtu.be/KsgYbZK7Yyk?si=K9jtrwd7MNNSJl4T

Consulté le 1 janvier 2026