28/12/2022

MODULE ELK

Rapport SUPDEVINCI

TABSISSI Hamdy – THURAIRAJASINGAM Keshiyan
SUPDEVINCI

SOMMAIRE

1 OBJECTIF

Dans le cadre de la validation de la matière ELK (Elasticsearch, Logstach, Kibana) il est demandé aux élèves de Master 1 Sup de Vinci de réaliser la création d'une attaque sur une des machines de tests (Windows ou Ubuntu) par le biais d'une infection ou d'une attaque via votre machine Kali.

L'objectif principal est par le biais du SIEM de détecter et qualifier l'attaque en mettant en corrélation les différents évènements.

L'attaque doit être lié à un TTP (référentiel Mitre Att&ck) et doit faire ressortir les évènements par le biais d'une kill chain (évènement, visualisation…).

L'objectif est de vous placer dans le rôle d'un analyste SOC de N1 (création des règles, intégration des logs, création d'un ticket d'incident, lever les faux positifs...) à N3 (expertise forensique et réponse à incident, CTI...) en passant par du N2 (détection et qualification des attaques).

BONUS : Dans le cadre de l'association des outils SIEM (ELK) & SOAR (via thehive & cortex) l'objectif est de créer des use-case d'analyses (via des Analyzer gratuit) intéressant ainsi que des automatisations permettant de réaliser une réponse à incident « responder » (exemple : envoyer un mail automatique via thehive/cortex).

2 SIEM - ELASTIC CLOUD

Un SIEM (Security Information and Event Management) est une solution de sécurité qui collecte et analyse les données de sécurité de différentes sources dans un réseau pour détecter et gérer les menaces potentielles. Le SIEM peut être utilisé pour surveiller les activités du réseau, identifier les anomalies et les comportements suspects, et générer des alertes en cas de menace détectée.

Nous avons utilisé la solution Elastic Cloud, c'est une plateforme en nuage qui permet de déployer, gérer des applications basées sur Elasticsearch, un moteur de recherche et de gestion de données open source. Elastic Cloud peut être utilisé pour stocker et analyser les données de sécurité collectées par un SIEM, en offrant une plateforme de stockage et d'analyse hautement scalable et disponible.

En utilisant Elastic Cloud comme plateforme de stockage et d'analyse pour les données de sécurité collectées par un SIEM, il est possible de bénéficier de la puissance de Elasticsearch pour effectuer des recherches en temps réel sur ces données et obtenir une vue complète de la sécurité de l'entreprise. De plus, en utilisant Elastic Cloud, il est possible de déployer et gérer facilement le SIEM, ce qui peut être particulièrement utile pour les entreprises qui n'ont pas les ressources ou les compétences nécessaires pour gérer ces systèmes en interne.

3 Agent Elastic Cloud

L'agent Elastic Cloud est un logiciel qui collecte et envoie des données de sécurité à Elastic Cloud, une plateforme en nuage qui permet de déployer, gérer et des applications basées sur Elasticsearch, un moteur de recherche et de gestion de données open source.

L'agent Elastic Cloud peut être installé sur différents types de systèmes d'exploitation, y compris Windows, Linux et MacOS. Une fois installé, l'agent se connecte au cluster Elastic Cloud en utilisant l'URL et les informations d'identification fournies lors de la configuration de l'agent. L'agent envoie alors les données de sécurité collectées à Elastic Cloud en utilisant une API RESTful sécurisée.

L'agent Elastic Cloud peut être utilisé pour collecter et envoyer différents types de données de sécurité, notamment les journaux de sécurité, les données de performance et les données de réseau. En utilisant Elastic Cloud comme plateforme de stockage et d'analyse pour les données de sécurité collectées par l'agent, il est possible de bénéficier de la puissance de Elasticsearch pour effectuer des recherches en temps réel sur ces données et obtenir une vue complète de la sécurité de l'entreprise.

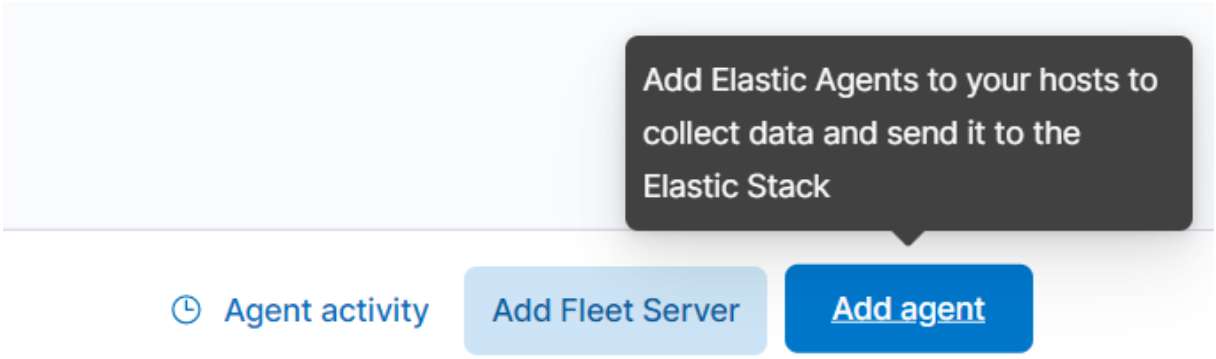
Nous utiliserons des agents sur les machines Windows Server 2019 et Debian 10.

Voici comment on s'y prend pour créer un agent sur Elastic Cloud.

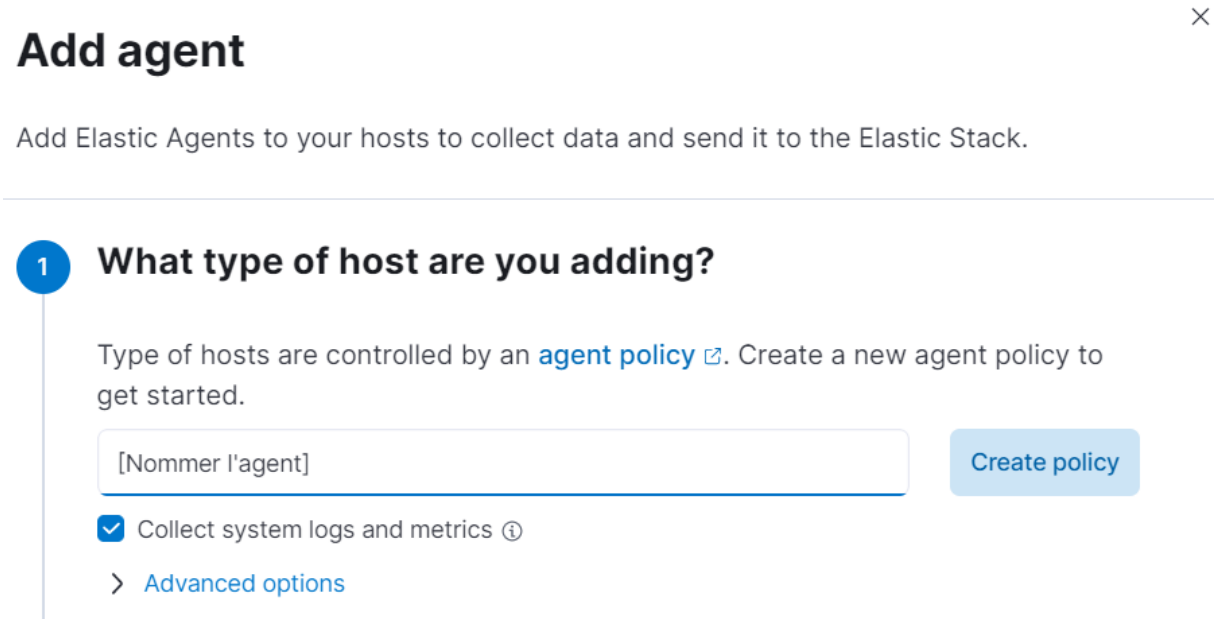
Tout d'abord, nous allons sur ce lien :

https://my-deployment-d17aee.kb.us-central1.gcp.cloud.es.io:9243/app/fleet/agents

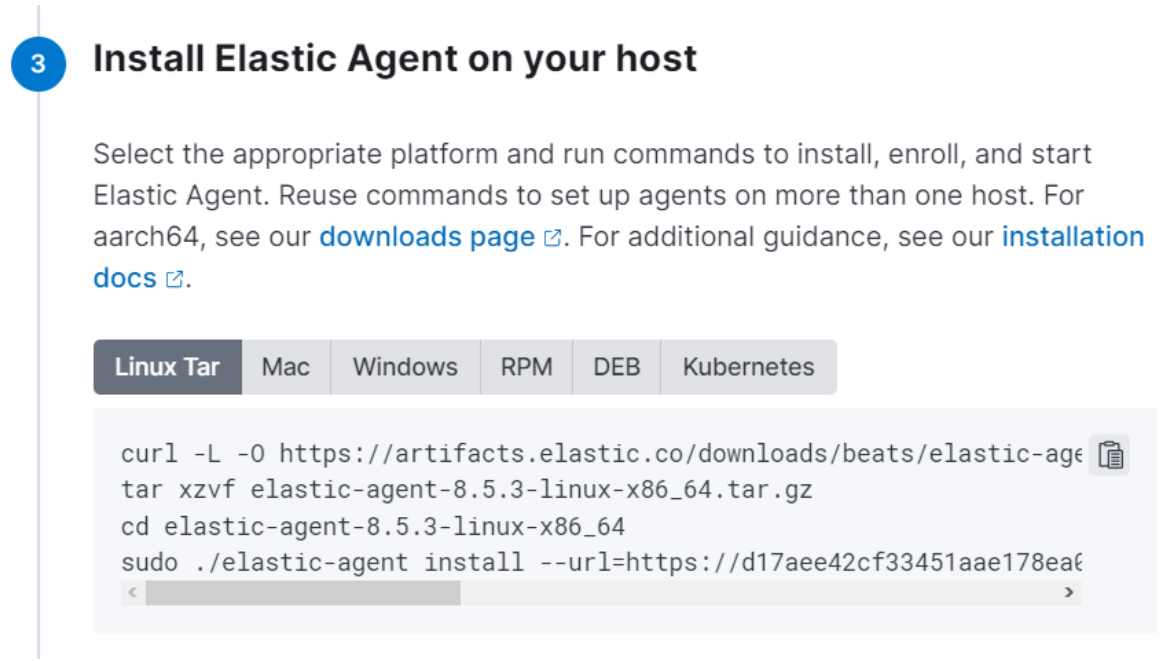
Puis



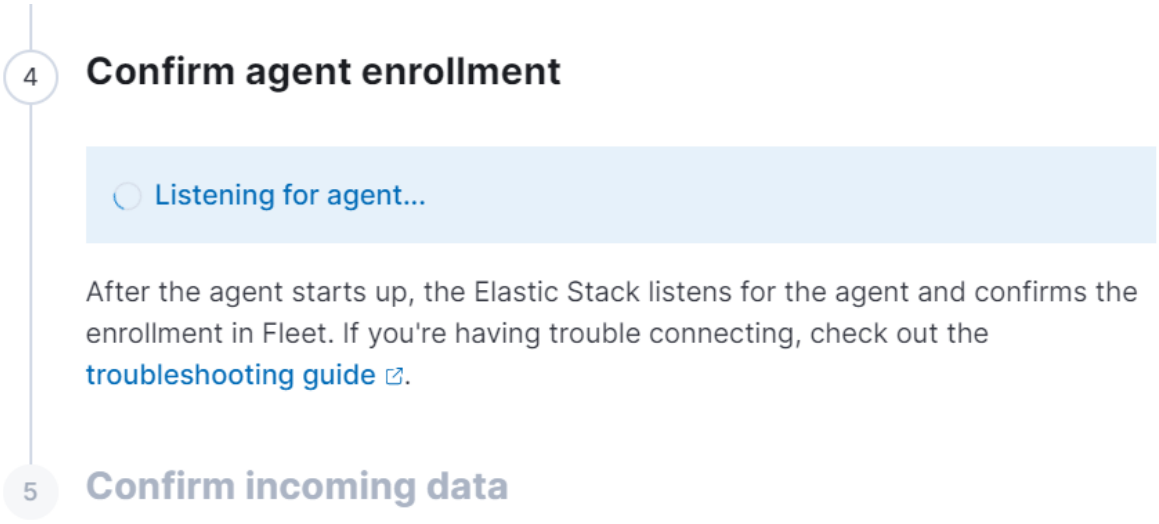
Créer l'agent en cliquant sur 'Create new agent policy' :



Copier ces lignes de commandes et les entrer directement sur le powershell (windows) ou le terminal (linux) :

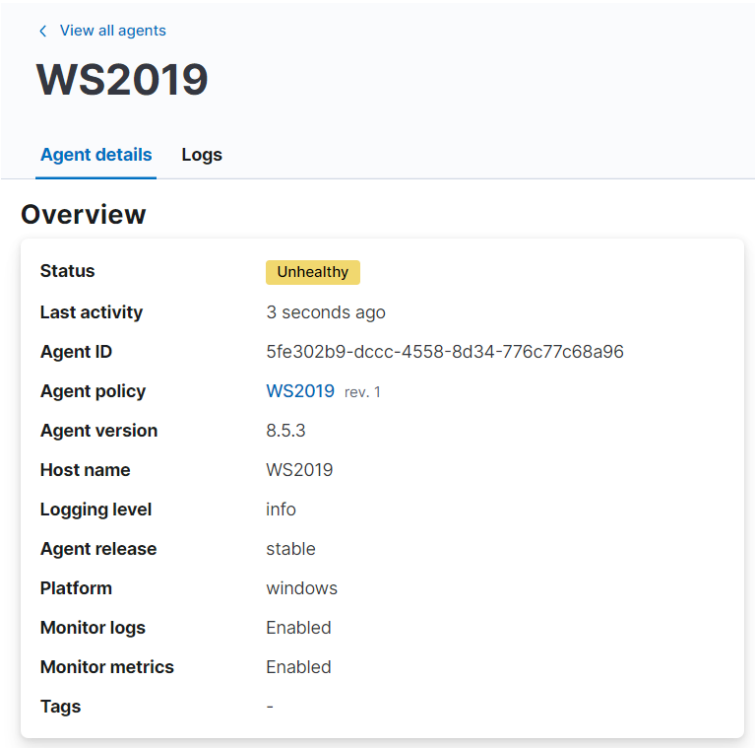


Ensuite il faut attendre quelque minute afin que l'agent envoie ses données sur Elastic Cloud via une API RESTful sécurisée :



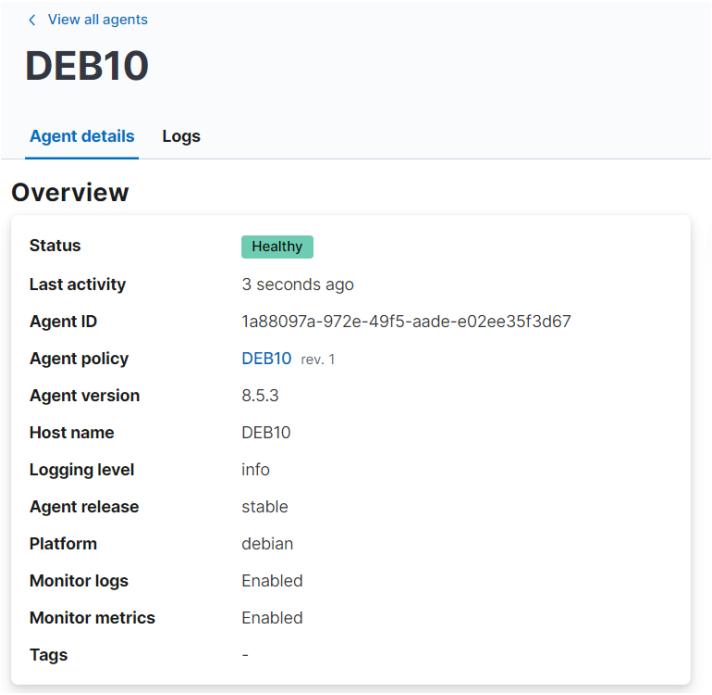
3.1.1 WS2019 (client windows)

Nous pouvons voir, sur Elastic Cloud, que la machine Windows Server 2019 remonte bien :

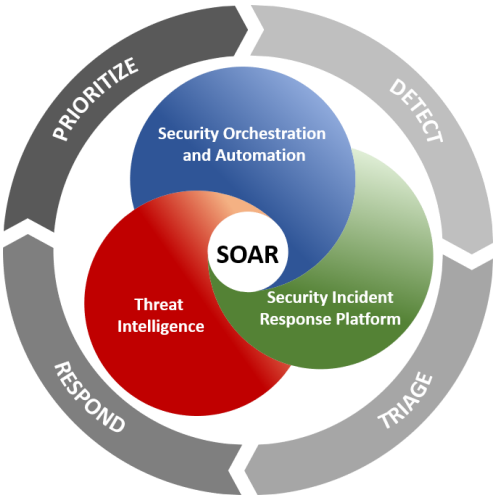


3.1.2 DEB10 (client linux)

De même pour la machine Debian 11, elle remonte bien :



4 SOAR - THE HIVE et CORTEX - the hive gere et cortex elimine

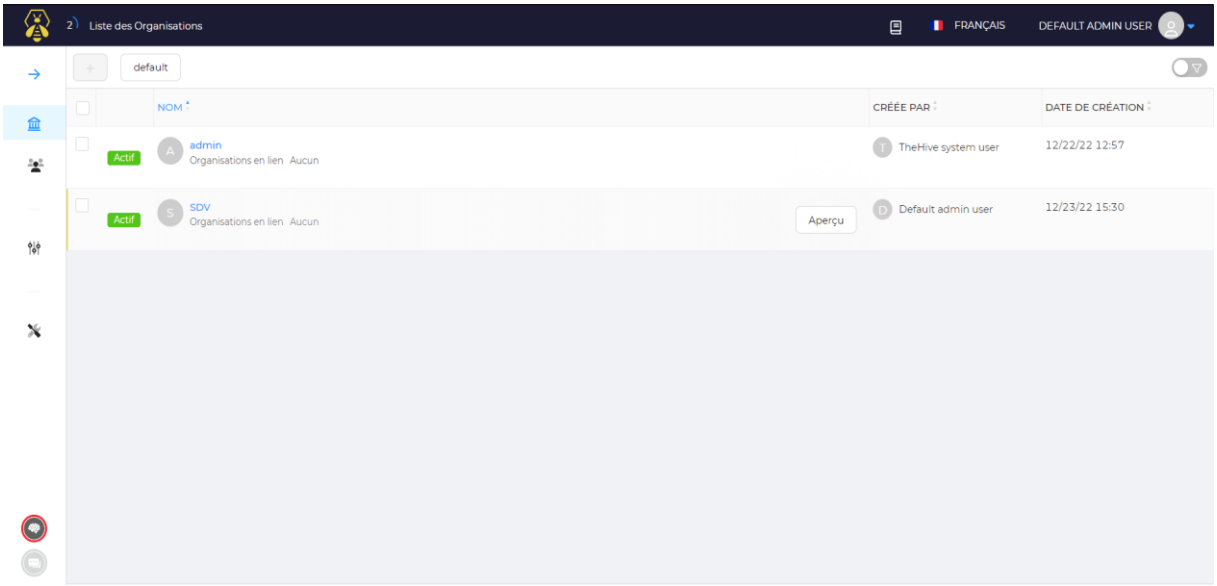


SOAR (Security Orchestration, Automation and Response) et Cortex sont des plateformes de sécurité de l'entreprise développées par la société Elastic. SOAR est une plateforme de gestion de la sécurité qui permet aux équipes de sécurité de gérer et d'automatiser les processus de réponse aux menaces. Cortex est une plateforme d'analyse de sécurité qui permet aux équipes de sécurité de collecter, de traiter et d'analyser les données de sécurité de différentes sources.

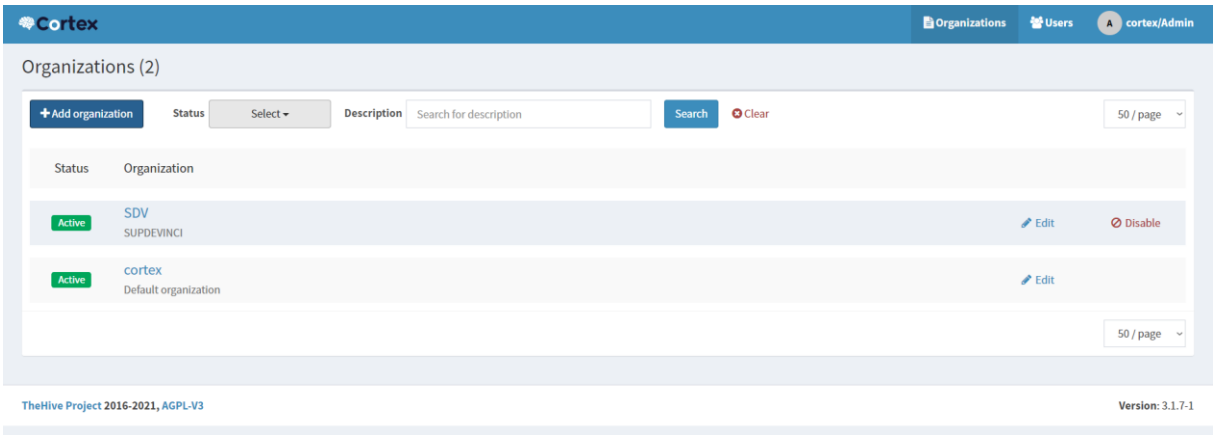
The Hive est une plateforme de collaboration développée par Elastic qui peut être utilisée conjointement avec SOAR et Cortex. The Hive offre une interface web simple qui permet aux équipes de sécurité de travailler ensemble et de partager des informations de manière efficace.

Voici l’interface web de :

- The Hive

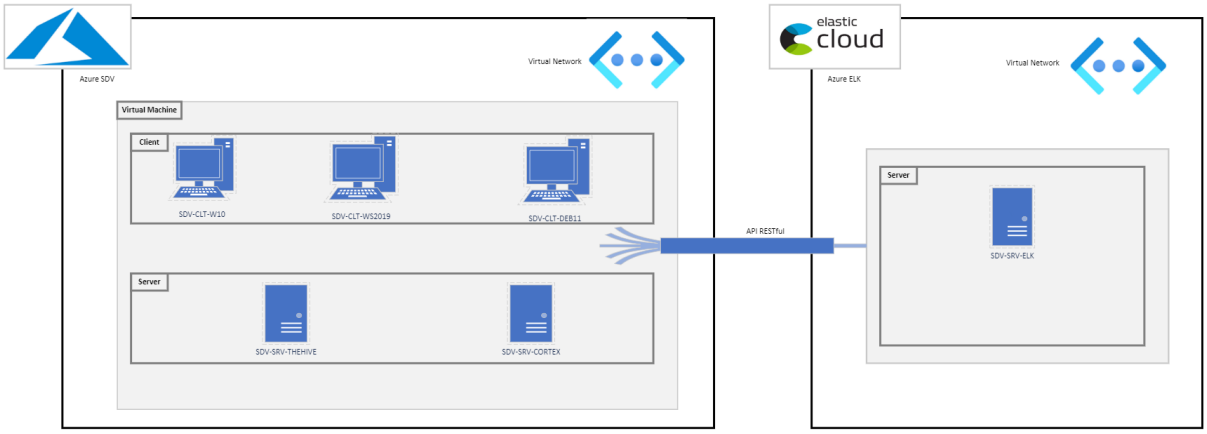


- Cortex



Ces différentes solutions peuvent être utilisées de manière conjointe pour gérer et automatiser les processus de réponse aux menaces en utilisant les données de sécurité collectées par Cortex. SOAR utilise les données de sécurité collectées par Cortex pour automatiser les processus de réponse aux menaces, tandis que The Hive permet aux équipes de sécurité de travailler ensemble et de partager des informations de manière efficace. Ensemble, ces plateformes permettent aux équipes de sécurité de réagir rapidement aux menaces et de protéger l'entreprise contre les attaques potentielles.

5 INFRASTRUCTURE



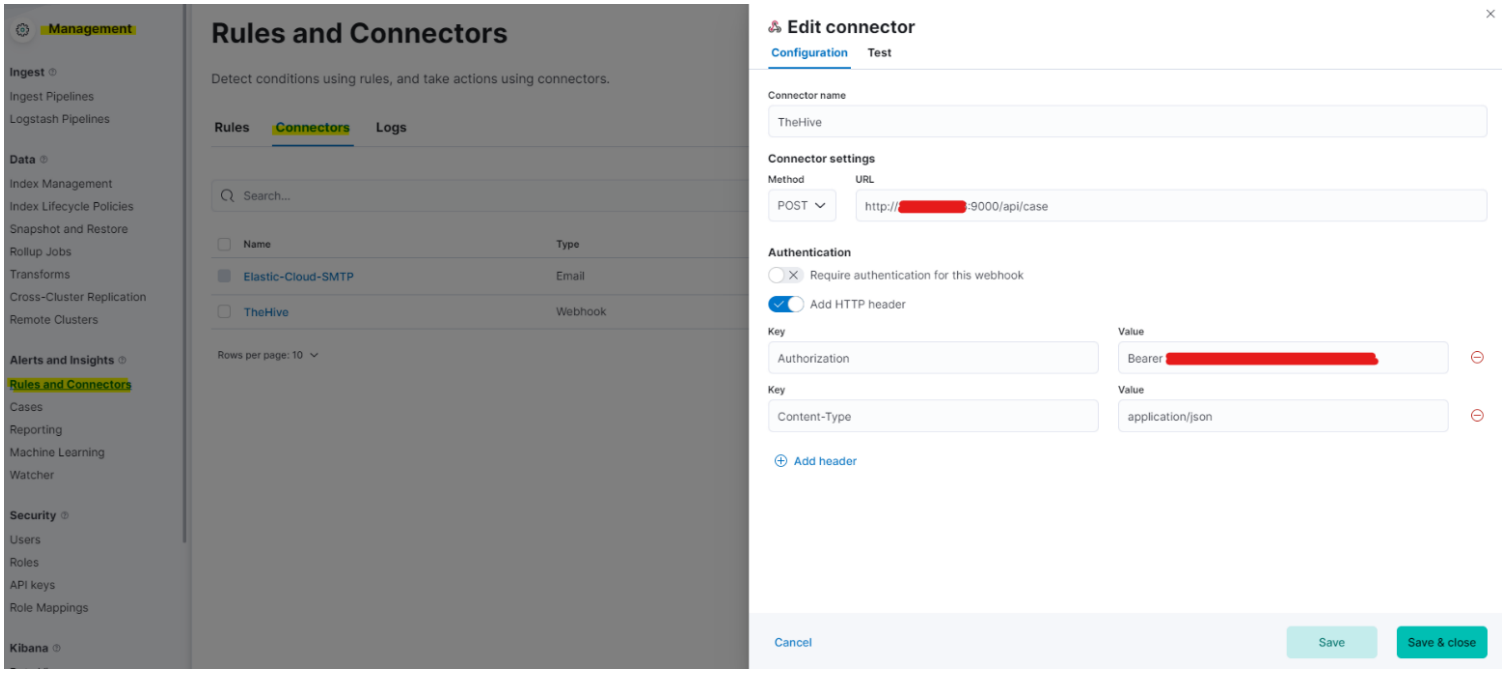
Voici donc notre SIEM.

Tout d'abord, nous avons Azure Cloud avec dedans des clients Windows et Linux et les serveurs The Hive et Cortex.

Ensuite, relié par un API RESTful à notre serveur ELK (Elasticsearch, Logstash, and Kibana).

Une API RESTful est une interface de programmation d'application qui permet aux applications de communiquer entre elles en utilisant des requêtes HTTP et des réponses HTTP pour manipuler des ressources de manière uniforme. Elle est souvent utilisée pour construire des interfaces de programmation d'application pour les services Web et est basée sur l'architecture client-serveur, l'utilisation de cache et l'absence d'état.

La communication entre ELK et TheHive est configuré de cette manière :



6 Mise en place des règles via MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est un framework de référence pour la gestion des menaces de sécurité qui décrit les tactiques, les techniques et les procédures couramment utilisées par les attaquants pour compromettre les systèmes et les réseaux. Ce framework est développé et maintenu par MITRE, un organisme de recherche sans but lucratif qui travaille en étroite collaboration avec le gouvernement américain et les entreprises du secteur privé.

Le framework MITRE ATT&CK est divisé en plusieurs matrices, qui décrivent les différentes phases du cycle de vie de la menace (préparation, entreprise, exécution, persistence, pivotion et évasion). Chaque matrice décrit les tactiques et les techniques couramment utilisées par les attaquants pour atteindre leurs objectifs, ainsi que les points de contrôle et les indicateurs de compromis (IOC) qui peuvent être utilisés pour détecter et prévenir ces attaques.

Le framework MITRE ATT&CK est largement utilisé par les professionnels de la sécurité pour évaluer les risques de sécurité, élaborer des stratégies de défense et valider les capacités de détection et de réponse aux menaces. Il est également utilisé par les développeurs de logiciels de sécurité pour améliorer la détection et la prévention des attaques.

Il comprend 14 matrices qui décrivent chacune les différentes phases du cycle de vie de la menace avec les tactiques et les techniques utilisées par les attaquants pour atteindre leurs objectifs, ainsi que les points de contrôle et les indicateurs de compromis (IOC) qui peuvent être utilisés pour détecter et prévenir ces attaques.

Nous nous sommes basés sur ce référentiel pour créer nos règles et alerte de sécurités.

Ainsi que sur la méthodologie par le biais d’une kill chain

6.1 REGLES MIS EN PLACE

6.1.1 Credential Access

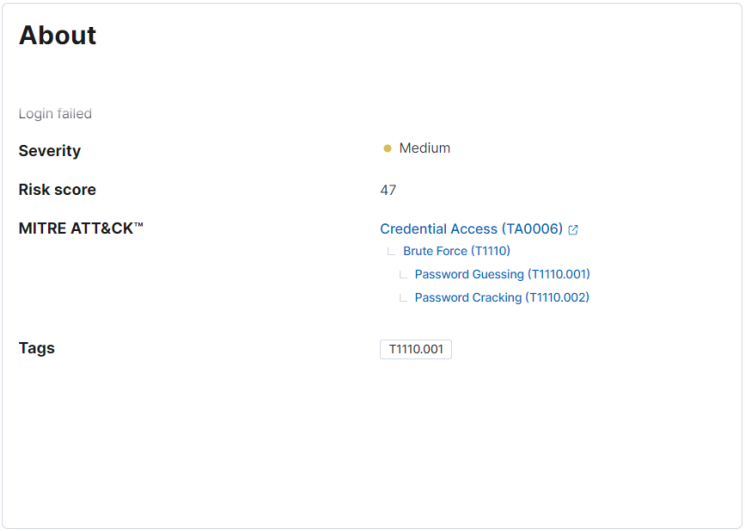
6.1.1.1 Objectif

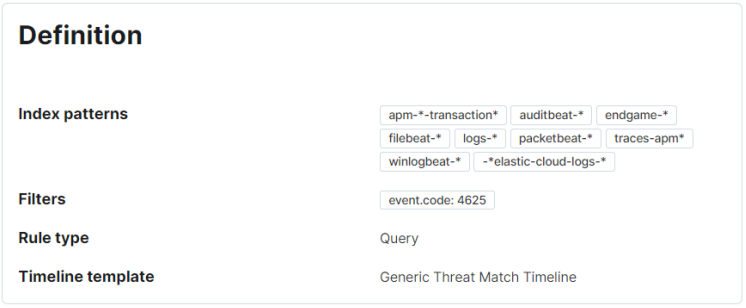
L'accès aux informations d'identification consiste en des techniques permettant de voler des informations d'identification comme les noms de comptes et les mots de passe. Parmi les techniques utilisées pour obtenir des informations d'identification, on peut citer le keylogging ou le credential dumping. L'utilisation d'informations d'identification légitimes peut permettre aux adversaires d'accéder aux systèmes, les rendre plus difficiles à détecter et leur donner la possibilité de créer d'autres comptes pour atteindre leurs objectifs.

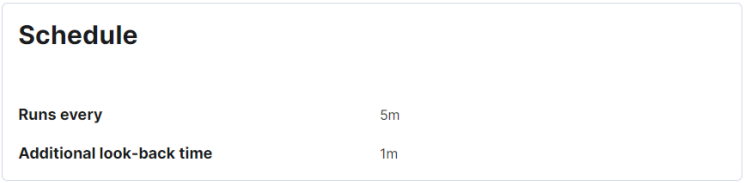
6.1.1.2 Attaquant

L'adversaire essaie de voler des noms de comptes et des mots de passe.

6.1.1.3 Solution



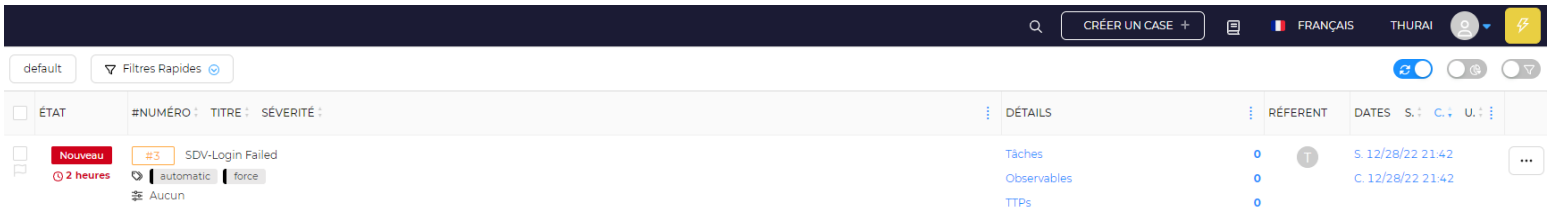


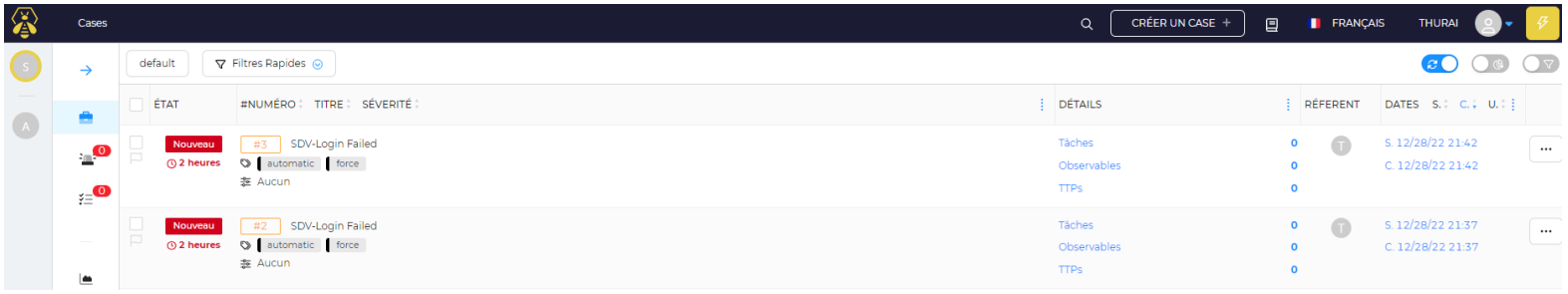


L'événement de code 4625 est un événement de journal d'audit de sécurité qui indique qu'une tentative de connexion a échoué sur le système. Cet événement est enregistré lorsqu'un utilisateur essaie de se connecter au système avec un nom d'utilisateur ou un mot de passe incorrect.

Ils peuvent indiquer une activité suspecte, comme une tentative de compromission de compte ou une attaque de force brute.

Pour se protéger contre ces menaces, il est recommandé de mettre en place des contrôles d'accès stricts et de sécuriser les comptes en utilisant des mots de passe forts et en activant la double authentification. Il est également recommandé de surveiller les événements de code 4625 et de détecter toute activité suspecte.





6.2 REGLES A METTRE EN PLACE

6.2.1 Reconnaissance

6.2.1.1 Objectif

La reconnaissance consiste en des techniques qui impliquent que les adversaires recueillent activement ou passivement des informations qui peuvent être utilisées pour soutenir le ciblage. Ces informations peuvent comprendre des détails sur l'organisation, l'infrastructure ou le personnel de la victime. Ces informations peuvent être exploitées par l'adversaire pour d'autres phases du cycle de vie de l'adversaire, comme l'utilisation des informations recueillies pour planifier et exécuter l'accès initial, pour définir la portée et la priorité des objectifs post-compromission, ou pour diriger d'autres efforts de reconnaissance.

6.2.1.2 Attaquant

L'adversaire essaie de recueillir des informations qu'il peut utiliser pour planifier de futures opérations.

6.2.2 Resource Development

6.2.2.1 Objectif

Le développement de ressources consiste en des techniques qui impliquent que les adversaires créent, achètent, ou compromettent/volent des ressources qui peuvent être utilisées pour soutenir le ciblage. Ces ressources peuvent être des infrastructures, des

comptes ou des capacités. Ces ressources peuvent être exploitées par l'adversaire pour contribuer à d'autres phases du cycle de vie de l'adversaire, comme l'utilisation de domaines achetés pour soutenir le commandement et le contrôle, de comptes de messagerie pour le phishing dans le cadre de l'accès initial, ou le vol de certificats de signature de code pour aider à l'évasion de défense.

6.2.2.2 Attaquant

L'adversaire essaie d'établir des ressources qu'il peut utiliser pour soutenir les opérations.

6.2.3 Initial Access

6.2.3.1 Objectif

L'accès initial consiste en des techniques qui utilisent divers vecteurs d'entrée pour prendre pied dans un réseau. Parmi les techniques utilisées pour prendre pied, citons l'hameçonnage ciblé et l'exploitation des faiblesses des serveurs Web accessibles au public. Les points d'appui obtenus par l'accès initial peuvent permettre un accès continu, comme des comptes valides et l'utilisation de services externes à distance, ou peuvent être à usage limité en raison du changement de mots de passe.

6.2.3.2 Attaquant

L'adversaire essaie de pénétrer dans votre réseau.

6.2.4 Execution

6.2.4.1 Objectif

L'exécution consiste en des techniques qui aboutissent à l'exécution d'un code contrôlé par l'adversaire sur un système local ou distant. Les techniques d'exécution de code malveillant sont souvent associées à des techniques appartenant à toutes les autres tactiques pour atteindre des objectifs plus larges, comme l'exploration d'un réseau ou le vol de données. Par exemple, un adversaire peut utiliser un outil d'accès à distance pour exécuter un script PowerShell qui effectue une découverte du système à distance.

6.2.4.2 Attaquant

L'adversaire essaie d'exécuter un code malveillant.

6.2.5 Persistence

6.2.5.1 Objectif

La persistance consiste en des techniques que les adversaires utilisent pour garder l'accès aux systèmes malgré les redémarrages, les changements d'identifiants et autres interruptions qui pourraient leur couper l'accès. Les techniques utilisées pour la persistance comprennent toute modification d'accès, d'action ou de configuration qui leur permet de maintenir leur emprise sur les systèmes, comme le remplacement ou le détournement de code légitime ou l'ajout de code de démarrage.

6.2.5.2 Attaquant

L'adversaire essaie de maintenir son emprise.

6.2.6 Privilege Escalation

6.2.6.1 Objectif

L'escalade de privilèges consiste en des techniques que les adversaires utilisent pour obtenir des autorisations de niveau supérieur sur un système ou un réseau. Les adversaires peuvent souvent pénétrer et explorer un réseau avec un accès non privilégié, mais ils ont besoin d'autorisations plus élevées pour atteindre leurs objectifs. Les approches courantes consistent à tirer parti des faiblesses, des mauvaises configurations et des vulnérabilités du système. Voici quelques exemples d'accès élevé :

- Niveau SYSTEM/root
- Administrateur local
- Compte d'utilisateur avec un accès de type administrateur
- Comptes d'utilisateurs ayant accès à un système spécifique ou exécutant une fonction spécifique

Ces techniques se recoupent souvent avec les techniques de persistance, car les fonctions du système d'exploitation qui permettent à un adversaire de persister peuvent s'exécuter dans un contexte élevé.

6.2.6.2 Attaquant

L'adversaire essaie d'obtenir des autorisations de niveau supérieur.

6.2.7 Defense Evasion

6.2.7.1 Objectif

L'évasion de défense consiste en des techniques que les adversaires utilisent pour éviter la détection tout au long de leur compromission. Les techniques utilisées pour l'évasion de défense comprennent la désinstallation/la désactivation des logiciels de sécurité ou l'obscurcissement/le cryptage des données et des scripts. Les adversaires exploitent et abusent également des processus de confiance pour cacher et masquer leurs logiciels malveillants. Les techniques d'autres tactiques sont répertoriées ici lorsque ces techniques présentent l'avantage supplémentaire de contourner les défenses.

6.2.7.2 Attaquant

L'adversaire essaie d'éviter d'être détecté.

6.2.8 Discovery

6.2.8.1 Objectif

La découverte consiste en des techniques qu'un adversaire peut utiliser pour acquérir des connaissances sur le système et le réseau interne. Ces techniques aident les adversaires à

observer l'environnement et à s'orienter avant de décider comment agir. Elles permettent également aux adversaires d'explorer ce qu'ils peuvent contrôler et ce qui se trouve autour de leur point d'entrée afin de découvrir comment cela pourrait profiter à leur objectif actuel. Les outils natifs du système d'exploitation sont souvent utilisés pour atteindre cet objectif de collecte d'informations après une compromission.

6.2.8.2 Attaquant

L'adversaire essaie de comprendre votre environnement.

6.2.9 Lateral Movement

6.2.9.1 Objectif

Le mouvement latéral consiste en des techniques que les adversaires utilisent pour entrer et contrôler des systèmes distants sur un réseau. Pour atteindre leur objectif principal, ils doivent souvent explorer le réseau pour trouver leur cible et y accéder. Atteindre leur objectif implique souvent de pivoter à travers de multiples systèmes et comptes pour gagner. Les adversaires peuvent installer leurs propres outils d'accès à distance pour réaliser un mouvement latéral ou utiliser des informations d'identification légitimes avec des outils de réseau et de système d'exploitation natifs, qui peuvent être plus furtifs.

6.2.9.2 Attaquant

L'adversaire essaie de se déplacer dans votre environnement.

6.2.10 Collection

6.2.10.1 Objectif

La collecte consiste en des techniques que les adversaires peuvent utiliser pour recueillir des informations et les sources auprès desquelles les informations sont recueillies qui sont pertinentes pour poursuivre les objectifs de l'adversaire. Souvent, l'objectif suivant la collecte de données est de voler (exfiltrer) les données. Les sources cibles courantes sont les différents types de disques, les navigateurs, les fichiers audio et vidéo et les courriels. Les méthodes de collecte courantes comprennent les captures d'écran et les saisies au clavier.

6.2.10.2 Attaquant

L'adversaire essaie de recueillir des données qui présentent un intérêt pour son objectif.

6.2.11 Command and Control

6.2.11.1 Objectif

Le commandement et le contrôle consistent en des techniques que les adversaires peuvent utiliser pour communiquer avec les systèmes sous leur contrôle au sein d'un réseau victime. Les adversaires tentent généralement d'imiter le trafic normal et attendu pour éviter la détection. Il existe de nombreuses façons pour un adversaire d'établir un système de commande et de contrôle avec différents niveaux de furtivité en fonction de la structure et des défenses du réseau de la victime.

6.2.11.2 Attaquant

L'adversaire essaie de communiquer avec les systèmes compromis pour les contrôler.

6.2.12 Exfiltration

6.2.12.1 Objectif

L'exfiltration consiste en des techniques que les adversaires peuvent utiliser pour voler des données sur votre réseau. Une fois qu'ils ont collecté les données, les adversaires les conditionnent souvent pour éviter la détection tout en les supprimant. Cela peut inclure la compression et le cryptage. Les techniques d'exfiltration des données d'un réseau cible consistent généralement à les transférer sur leur canal de commande et de contrôle ou sur un canal alternatif et peuvent également inclure des limites de taille sur la transmission.

6.2.12.2 Attaquant

L'adversaire essaie de voler des données.

6.2.13 Impact

6.2.13.1 Objectif

L'impact consiste en des techniques que les adversaires utilisent pour perturber la disponibilité ou compromettre l'intégrité en manipulant les processus commerciaux et opérationnels. Les techniques utilisées pour l'impact peuvent inclure la destruction ou l'altération des données. Dans certains cas, les processus opérationnels peuvent sembler corrects, mais avoir été modifiés pour servir les objectifs des adversaires. Ces techniques peuvent être utilisées par les adversaires pour atteindre leur objectif final ou pour couvrir une violation de la confidentialité.

6.2.13.2 Attaquant

L'adversaire essaie de manipuler, d'interrompre ou de détruire vos systèmes et vos données.

7 Conclusion

Dans ce travail de pratique, nous avons utilisé Elastic Cloud pour mettre en place des règles de sécurité et surveiller les activités du système afin de protéger contre les 14 domaines d'attaque du MITRE ATT&CK. Nous avons constaté que Elastic Cloud était une solution efficace pour détecter et prévenir les menaces, grâce à sa capacité à analyser et à visualiser les données de sécurité en temps réel.

Cependant, il est important de noter que Elastic Cloud n'est pas une solution infaillible et qu'il est recommandé de mettre en place une stratégie de sécurité globale qui utilise plusieurs outils et technologies de sécurité. Par exemple, il pourrait être judicieux de compléter Elastic Cloud avec un pare-feu de réseau ou un système de détection et de réponse aux incidents pour renforcer la sécurité du système.

En conclusion, Elastic Cloud s'est avéré être une solution efficace pour protéger contre les 14 domaines d'attaque du MITRE ATT&CK, mais il est recommandé de l'utiliser en complément d'autres outils et technologies de sécurité pour une protection optimale.