

# RAPPORT DE STAGE

**Théo BOUTROUX**

02/05/2023 – 02/06/2023

**Tuteur :** Nicolas NOEL

**Responsable de formation :** Clara DULAC

**Formation :** EPSI Nantes – SNI (option BTS SIO)

**Entreprise d'accueil :** **OMR Infogérance** – 14 Av. Jules Verne,  
44230 **Saint-Sébastien-sur-Loire**

# Table des matières

<b>Remerciements</b>	<b>2</b>
<b>Introduction</b>	<b>3</b>
<b>I – Présentation du groupe VFLIT</b>	<b>4</b>
A. Le Groupe VFLIT	4
B. Les offres	5
C. Les fournisseurs et partenaires	6
D. Les clients	6
<b>II – Présentation de l’entreprise</b>	<b>6</b>
A. OMR Infogérance	6
B. Services	8
C. Organisation	9
D. Politique de l’entreprise	10
<b>III – Présentation de l’activité</b>	<b>10</b>
A. Domaine d’activité	10
B. Services proposés	11
<b>IV– Les Missions</b>	<b>12</b>
A. Projet SentinelOne	12
💡 Qu’est-ce que SentinelOne ?	12
Fonctionnement de l’application	13
En quoi cette application est utile ?	13
Déroulement de la mission	13
Difficultés rencontrées	21
<b>V – Conclusion</b>	<b>23</b>
<b>VI – Bibliographie</b>	<b>24</b>
<b>VII – Annexes</b>	<b>26</b>

# Remerciements

Avant de commencer à parler de mon expérience durant mon stage, je tiens à remercier toutes les personnes qui m'ont accompagné durant ce dernier, et qui m'ont permis d'enrichir mon expérience professionnelle.

Je souhaite exprimer ma reconnaissance envers :

**Jean-Emmanuel URIEN**, directeur général d'OMR Infogérance.

**Nicolas NOËL**, responsable de la sécurité du système informatique (RSSI), pour son accueil et sa sympathie.

**Jérémy ROUSSEAU**, expert en cybersécurité, qui m'a permis de réaliser ce stage et qui m'a aidé lors de mon intégration.

**Kieran LE PENDEVEN**, expert sécurité des Systèmes d'Information, pour son aide précieuse, ses conseils et son expérience qu'il m'a apportée tout au long de mes missions.

**L'ensemble du service cybersécurité**, pour leur accueil, leurs conseils et leurs précieuses suggestions durant le stage.

**Le personnel de mon école (EPSI - Nantes)**, sans qui je n'aurais pas eu la chance de faire ce stage.

Merci encore à toutes ces personnes qui ont été présentes et qui ont rendu cette expérience de stage si enrichissante et passionnante.

# Introduction

Le présent rapport vise à rendre compte de mon expérience professionnelle durant mon stage de première année. Ce dernier s'est déroulé pendant 5 semaines (du 02/05/2023 au 02/06/2023) dans le cadre de ma formation à EPSI - Nantes.

J'ai réalisé mon stage chez OMR Infogérance, une entreprise du groupe VFLIT spécialisée dans le domaine de l'infogérance depuis sa fondation en 2008. Elle offre des services de gestion et de maintenance des systèmes informatiques pour une clientèle très diversifiée. Durant les cinq semaines, j'ai eu l'occasion de découvrir le service cybersécurité dans lequel j'ai réalisé un projet important.

Pour mener à bien mon stage, j'ai adopté une approche méthodique. J'ai commencé par me familiariser avec les outils utilisés par le service de cybersécurité ainsi qu'avec les processus internes de l'entreprise. J'ai également suivi les directives données par mon tuteur pour réaliser mes missions afin de répondre à ses besoins.

Dans le cadre des missions qui m'ont été confiées, j'ai utilisé les ressources qui m'étaient mises à disposition par OMR Infogérance ainsi que celles disponibles sur le Web. J'ai également adopté une approche collaborative en travaillant avec mes collègues et en les sollicitant pour leur expertise. Enfin, j'ai également fait preuve d'autonomie en prenant des initiatives et en proposant des solutions.

En choisissant OMR, j'avais pour objectif de mettre en œuvre l'ensemble des connaissances que j'ai pu apprendre à l'EPSI. Ce stage représentait également une opportunité d'acquérir une expérience professionnelle dans une entreprise du numérique. Enfin, il m'a permis de confirmer mon intérêt pour le développement et de développer mes connaissances dans le domaine de l'informatique.

# I – Présentation du groupe VFLIT

## A. Le Groupe VFLIT

Créé en 2000, VFLIT (Vous faciliter l'IT) a grandi rapidement par le biais de croissances organiques et externes, et est donc dans une démarche d'industrialisation de ses processus. Le but est de définir un cadre pour tous les processus métiers afin de gagner du temps et d'harmoniser les actions des collaborateurs. Depuis 2010, leurs sociétés se rapprochent progressivement pour créer un acteur unique qui offre une solution globale pour le management des systèmes d'information et de communication.

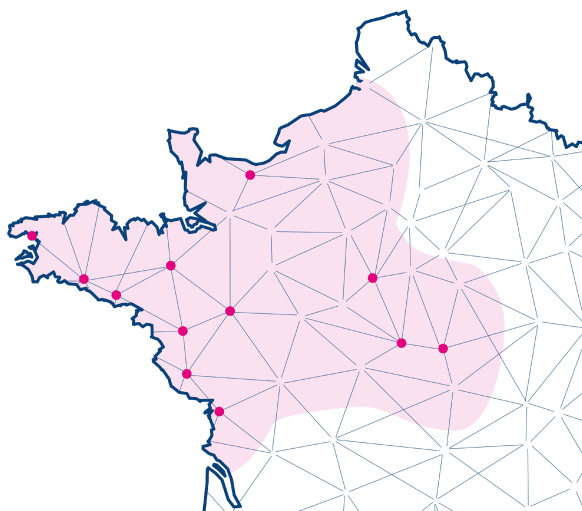
VFLIT propose de nombreux services d'infogérance tels que :

- L'hébergement CLOUD et de l'installation
- La maintenance et de la gestion préventive des infrastructures systèmes et réseaux
- Des infrastructures téléphoniques et FAI
- Des applications de gestion et de la sûreté

Le groupe VFLIT, comprenant OMR Infogérance et cinq autres entreprises toutes travaillant dans l'infogérance, est aujourd'hui constitué de 13 agences réparties surtout dans le Nord-Ouest de la France, mais aussi dans le Centre.

**OMR DACTYL MEDIS SIREN ESPACE com CTV**

Les six entreprises du groupe



## Pourquoi avoir choisi ces régions ?

Si le groupe est implanté dans le Grand Ouest de la France et dans le Centre, c'est parce qu'il ont choisi de travailler avec des petites et moyennes entreprises de proximité pour déployer leur expertise.

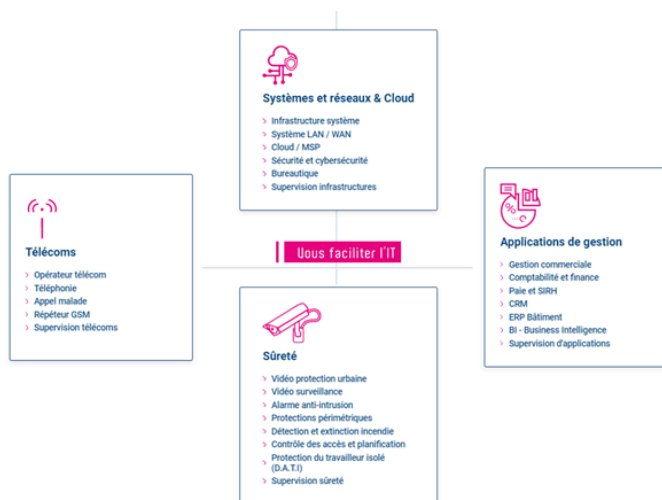
(Carte représentant les agences VFLIT et leur localisation)

Les dirigeants actuels du groupe sont Dave LECOMTE et Jean-Emmanuel URIEN, accompagnés par Marc SEVESTRE, un actionnaire du groupe. VFLIT compte aujourd'hui plus de 250 salariés répartis dans toutes les agences et a généré un chiffre d'affaires dépassant les 32 millions d'euros sur l'exercice comptable 2022.

Le groupe est en constante croissance car le CA augmente en moyenne de 2 millions d'euros par an. En effet, il était de 28 M d'euros en 2020 et de 30 M d'euros en 2021.

## B. Les offres

L'objectif principal du groupe VFLIT est de proposer avant tout un panel d'offres suffisant pour couvrir l'ensemble des besoins dans le secteur de l'informatique des PME, TPE et collectivités.



Les offres proposées par le groupe

## **C. Les fournisseurs et partenaires**

Au fil des années, le groupe a pu collaborer avec de nombreux partenaires. Parmi eux, on peut citer Microsoft (Gold Partner), Veeam, Fujitsu, Kaspersky, Sonicwall, NetApp, VadeSecure et Alcatel Lucent. La stratégie du groupe est de préconiser une seule solution par équipement afin d'avoir une maîtrise totale sur les solutions et pour pouvoir être formé régulièrement. Le groupe priorise la formation pour toujours améliorer l'expertise de ses techniciens terrain ou support.

## **D. Les clients**

Depuis sa création, le nombre de clients actifs du groupe n'a cessé d'être en constante augmentation, jusqu'à atteindre environ 7800 clients en juin 2020. Ces derniers viennent de différents types d'organisation, allant de l'association à des entreprises dans l'industrie, en passant par des ehpad, des collectivités, des professions libérales ou encore des métiers de l'éducation.

# **II – Présentation de l'entreprise**

## **A. OMR Infogérance**

OMR Infogérance et OMR Impression ont été créés en 1989 sous le nom d'une même entité "OMR". En 2008, l'actionnaire majoritaire a décidé de séparer les deux entités afin de fusionner OMR Impression avec Dactyl Buro et OMR Infogérance avec Dactyl Informatique.

Par la suite, les actionnaires Marc Sevestre et Michel Tatin ont décidé de vendre la partie impression (OMR Impression) à Konika Minolta, une société japonaise de solutions d'impression et de services informatiques.

Depuis, OMR Infogérance et Dactyl Informatique sont restés indépendants avec trois actionnaires, Marc Sevestre, Jean-Emmanuel Urien et Dave Lecomte.

L'entreprise a développé son activité principalement autour de l'hébergement, de la téléphonie, de l'activité FAI\* et des MSP\*\*.

OMR Infogérance est aujourd'hui présent sur 7 agences du groupe VFLIT et son siège social est basé à Saint-Sébastien-sur-Loire, au Sud-Est de Nantes, en Loire-Atlantique. L'entreprise représente un acteur économique majeur du groupe car elle représente à elle seule environ un tiers du chiffre d'affaires annuel (environ 11 millions d'euros en 2022) de VFLIT et elle regroupe également environ un tiers des salariés (environ 80).

FAI\* : Fournisseur d'accès internet

MSP\*\* : Une MSP (Managed Service Provider) désigne une entreprise qui gère les systèmes informatiques de ses clients à distance.

## **B. Services**

La société OMR Infogérance propose des solutions principalement dans deux domaines majeurs, l'infogérance et la téléphonie.

### **1) Infogérance**

OMR propose des services hébergés aux professionnels. Ces derniers comprennent des offres packagées Antivirus, antispam, la sauvegarde et l'hébergement de serveurs. L'entreprise commercialise des contrats d'infogérance et des maintiens en condition opérationnelle du système d'information.

La société propose également du matériel comme des serveurs, des ordinateurs ou encore des baies de stockage. La sécurité informatique est l'une des préoccupations majeures de l'entreprise.



## **2) Téléphonie** 📞

OMR commercialise également des solutions de téléphonie, voix sur IP, couplage téléphonique et mise en réseau de centraux privés. Elle conseille à ses clients les technologies les plus adaptées à leurs besoins avec le souci constant de leur satisfaction et de leur pérennité.

La qualité de ses études et du choix du matériel qu'elle propose est un gage de satisfaction pour les entreprises qui lui ont fait confiance. En 2019, la société a commercialisé plus de 550 liens FAI et 900 postes IP téléphoniques.

## **C. Organisation**

L'entreprise est décomposée en plusieurs services différents ayant chacun leur rôle.

### **1) Service MSP**

Le service MSP est très important dans l'entreprise. Il administre et supervise tous les services managés du groupe ainsi que tout son Système d'Information. Le nombre de collaborateurs ne cesse d'augmenter dans ce service : le responsable de service a récemment changé et il coordonne 10 personnes dont des techniciens en supervisions et des administrateurs systèmes et réseaux.

### **2) Service ADV**

Le service Administration Des Ventes gère la partie commande, facturation et planification des interventions du groupe.

### **3) Service Support**

L'équipe support résout les problèmes de l'ensemble du groupe ainsi que ceux des clients. Le service est composé du responsable et d'une dizaine d'administrateurs.

### **4) Service CRM**

Ce service est composé de 3 membres chargés de démarcher les clients, de gérer le fichier client, de présenter et de communiquer sur le groupe VFLIT.

### **5) Les équipes terrains**

De nombreux Administrateurs et Ingénieurs Technico-Commerciaux itinérants sont en permanence sur le terrain pour installer, maintenir, administrer et conseiller les systèmes d'information des clients.

### **6) Service Projet**

Ce service a pour mission de gérer les différents projets en cours au sein de l'entreprise.

### **7) Service Cybersécurité**

Le service Cybersécurité est celui dans lequel j'ai réalisé l'intégralité de mon stage. Sa création remonte à septembre 2021 et le service est aujourd'hui composé de 6 personnes.

## **D. Politique de l'entreprise**

### **1) Sécurité**

OMR Infogérance donne une grande importance à sa politique de sécurité et de confidentialité en respectant notamment le RGPD (Règlement Général sur la Protection des Données). L'entreprise utilise un coffre-fort de gestion des mots de passe appelé Do4Safe afin de permettre aux collaborateurs de protéger leurs mots de passe pour éviter les menaces malveillantes.

## 2) Environnement

En 2022, le groupe VFLIT a reçu un certificat de la part de Itancia Again pour les attester de leurs économies de CO2. Ils ont au total pu économiser plus de 8300 kg de dioxyde de carbone sur l'année civile 2022.

# III – Présentation de l'activité

## A. Domaine d'activité

Le domaine de l'infogérance joue un rôle essentiel dans le fonctionnement et la performance des entreprises actuelles. Au cours de mon stage chez OMR Infogérance, j'ai pu découvrir ce domaine en constante évolution.

L'infogérance consiste à externaliser la gestion des systèmes informatiques d'une entreprise à un prestataire spécialisé (comme OMR). Cela permet aux entreprises de se concentrer sur le cœur de leurs activités tout en bénéficiant d'une expertise technique avancée. Ce domaine peut couvrir un large éventail de services, adaptés aux besoins spécifiques de chaque entreprise. Cela peut inclure la surveillance proactive des systèmes pour détecter et résoudre les problèmes, la gestion des sauvegardes et la récupération des données, la gestion de la sécurité informatique (pare-feu, antivirus...), ou encore la gestion des utilisateurs et des accès.

### Quelques chiffres clés sur le marché de l'infogérance :

- Capitalisation du marché en France en 2020 : 13 milliards d'euros
- La valeur annuelle des entreprises a augmenté en moyenne de 15,5% entre 2021 et 2022.
- En 2021, 70% des entreprises font appel à une entreprise spécialisée dans l'infogérance.

## B. Services proposés

OMR Infogérance offre une gamme complète de services liés à l'infogérance mais également des services orientés sécurité, afin de sensibiliser les collaborateurs et les clients, mais aussi pour sécuriser et évaluer les systèmes informatiques.

On peut retrouver tout d'abord des campagnes de sensibilisation au phishing<sup>1</sup>. Pour ce faire, l'équipe cybersécurité d'OMR va se déplacer chez les clients dans le but de sensibiliser les clients et leurs collaborateurs sur cette cyberattaque.

OMR propose également des audits de vulnérabilité à ses clients. Ses audits sont utilisés pour évaluer les vulnérabilités présentes dans un système informatique, un réseau ou une application. Cette démarche permet d'identifier et de quantifier les faiblesses potentielles en termes de sécurité, afin de mettre en place des mesures correctives appropriées.

En plus des services de prévention et de détection de failles comme vu précédemment, OMR propose à ses clients des services de pentest<sup>2</sup>. Cela inclut à la fois des tests d'intrusion à distance, donc des simulations de cyberattaques, ou bien aussi des intrusions physiques. Ces dernières permettent d'évaluer la sécurité d'une organisation en simulant une tentative d'accès à ses installations physiques, ses locaux ou ses équipements.

Enfin, on peut retrouver d'autres missions réalisées dans le domaine de la sécurité comme par exemple la rédaction de Politique de sécurité du Système d'Information (PSSI) qui vise à définir des règles et des mesures pour protéger les informations et les ressources d'un système. Il y a également des projets réalisés comme par exemple la réalisation d'une console permettant de visualiser les appareils déconnectés du réseau par un EDR<sup>3</sup>.

**Phishing<sup>1</sup>** : Il s'agit d'une forme de cyberattaque qui consiste à usurper l'identité de quelqu'un, ou à se faire passer pour un organisme légitime, dans le but de tromper ses victimes en les faisant ouvrir une pièce jointe frauduleuse ou un fichier contenant un script malveillant, pouvant récupérer des informations personnelles ou encore injecter un virus.

**Pentest<sup>2</sup>** : Il s'agit d'une méthode d'évaluation de la sécurité informatique qui vise à tester la résistance d'un système, d'un réseau ou d'une application aux attaques et aux intrusions. C'est une pratique proactive qui consiste à simuler des attaques réelles sur un système pour identifier ses vulnérabilités et ses failles de sécurité.

**EDR<sup>3</sup>** : il s'agit d'une technologie visant à détecter, enquêter et répondre aux menaces reçues sur les appareils (aussi appelés endpoints) d'un réseau. L'objectif principal d'un EDR est d'améliorer la détection d'incidents de sécurité et de permettre une réponse rapide et efficace.

## IV- Les Missions

L'objectif principal de mon stage de première année était de me familiariser avec l'environnement professionnel et de mettre en pratique l'ensemble des connaissances que j'ai pu acquérir en autodidacte et au cours de ma formation à l'EPSI.

 **Certaines informations présentes dans les images seront pixelisées dans le but de préserver les informations sensibles.**

### A. Projet SentinelOne

J'ai été amené à réaliser une mission consistant au développement d'une application en interne pour recueillir les informations en temps réel sur les machines déconnectées du réseau par l'EDR SentinelOne.

#### **Qu'est-ce que SentinelOne ?**

SentinelOne est une entreprise israélienne spécialisée dans la cybersécurité fondée en 2013 et dont le siège est basé en Californie, aux États-Unis. Le produit de cette entreprise est une plateforme de sécurité autonome basée sur l'intelligence artificielle et l'apprentissage automatique (EDR). Cet EDR est conçu pour détecter, prévenir et neutraliser les attaques de logiciels malveillants, y compris les ransomwares

(rançongiciel en français), les exploits de vulnérabilités et les attaques sans fichier.

## **Fonctionnement de l'application**

L'application appelée "SentinelOne Vision" a donc pour but de récupérer des données importantes sur les machines déconnectées du réseau par l'EDR. Nous avons utilisé l'API mise à disposition par SentinelOne afin de collecter l'ensemble des données pour les traiter par la suite. Le stockage des données se fait grâce à un script développé en Python, qui permet de récupérer les réponses de l'API suite aux requêtes envoyées, avant de mettre les données dans des fichiers JSON (JavaScript Object Notation). Ces données sont ensuite affichées dans une interface Web. (Voir les schémas de fonctionnement dans l'annexe 2)

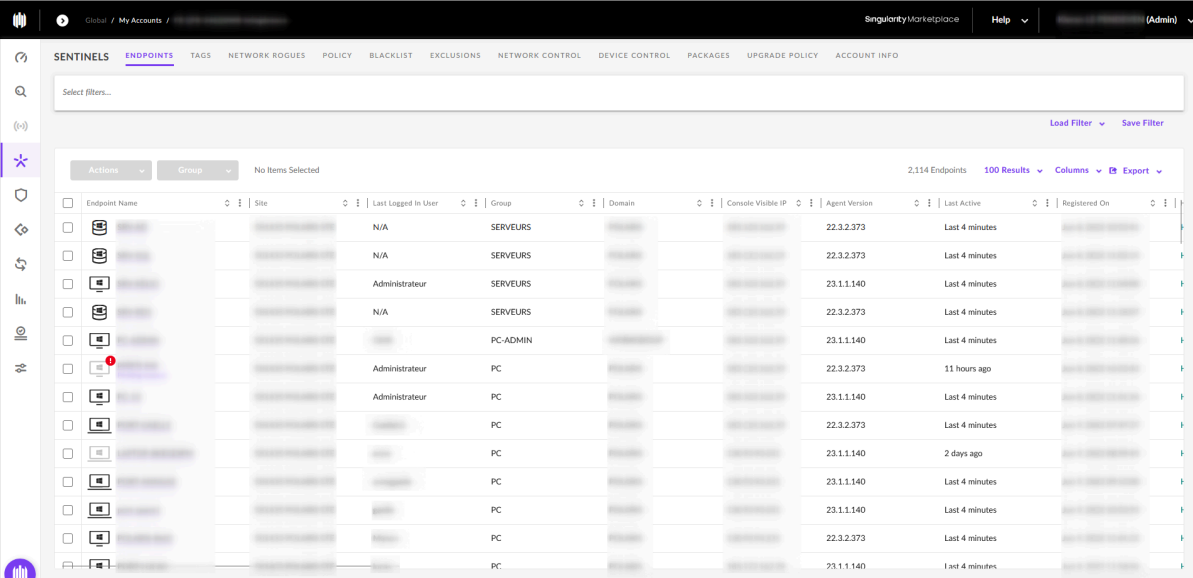
## **En quoi cette application est utile ?**

Lorsque une alerte est reçue de la part de SentinelOne, cette application permet à l'équipe de cybersécurité de pouvoir voir quelle machine est impactée. Cette dernière contient également un système sonore permettant de déclencher un son d'alerte si un nouveau problème vient d'être détecté, ou bien un son de fin d'alerte si un problème a été résolu. Celui-ci permet donc à l'équipe de se concentrer pleinement sur leurs tâches sans avoir besoin de regarder régulièrement la console SentinelOne, mais aussi de pouvoir vite réagir en cas d'alerte.

## **Déroulement de la mission**

Lors du lendemain de mon arrivée, je me suis entretenu avec Nicolas Noel et Jérémy Rousseau afin que l'on puisse s'accorder sur un cahier des charges pour cette mission. Nous avons donc décidé de réaliser une partie front-end en HTML et CSS et une partie backend en Python. La partie front-end représente ce qui est visible pour l'utilisateur alors que le backend quant à lui désigne l'algorithme qui fonctionne en continu pour récupérer les données.

La première semaine a été plutôt axée sur la mise en place de mon environnement de travail, la découverte de l'API SentinelOne, et le développement des fonctions permettant d'envoyer des requêtes à l'API pour recevoir et traiter les données. J'ai choisi de travailler avec Visual Studio Code pour développer mes scripts, qui est un IDE (Environnement de développement) permettant de développer dans de très nombreux langages de programmation. Les premiers jours ont été consacrés à la découverte et à la compréhension de la documentation de l'API. Il fallait en effet retrouver la bonne URL à requêter pour bénéficier des données voulues.



Endpoint Name	Site	Last Logged In User	Group	Domain	Console Visible IP	Agent Version	Last Active	Registered On
[Icon]		N/A	SERVEURS			22.3.2.373	Last 4 minutes	
[Icon]		N/A	SERVEURS			22.3.2.373	Last 4 minutes	
[Icon]		Administrateur	SERVEURS			23.1.1.140	Last 4 minutes	
[Icon]		N/A	SERVEURS			22.3.2.373	Last 4 minutes	
[Icon]			PC-ADMIN			23.1.1.140	Last 4 minutes	
[Icon]		Administrateur	PC			22.3.2.373	11 hours ago	
[Icon]		Administrateur	PC			23.1.1.140	Last 4 minutes	
[Icon]			PC			22.3.2.373	Last 4 minutes	
[Icon]			PC			23.1.1.140	2 days ago	
[Icon]			PC			23.1.1.140	Last 4 minutes	
[Icon]			PC			23.1.1.140	Last 4 minutes	
[Icon]			PC			22.3.2.373	Last 4 minutes	
[Icon]			PC			23.1.1.140	Last 4 minutes	

On retrouve ici une image correspondant à la console SentinelOne contenant l'ensemble des données sur les machines internes et externes.

En seulement quelques jours, j'ai ainsi pu développer les fonctions me permettant de récupérer et stocker les données au format JSON. Parmi celles-ci, on retrouve la fonction `is_connected()` qui permet de vérifier si le script est bien connecté à l'API. On retrouve aussi la fonction `get_data()` qui a pour but d'envoyer des requêtes à l'API pour récupérer les données concernant les machines. Il y a également `modify_json()` qui est utilisé pour modifier les valeurs d'un fichier JSON. Enfin, on va retrouver la fonction `main_function()` qui appelle toutes les fonctions précédentes et qui

permet donc de récupérer et stocker toutes les données concernant les machines.

Cette première semaine m'a également permis de développer la page d'accueil de l'application, que l'on appellera index. Cet index a été développé grâce à des technologies Web telles que HTML, CSS, Javascript et la librairie Bootstrap afin de faciliter la création du style de la page. Cette page est composée d'une entête comportant un lien et un logo du groupe VFLIT. Dans le corps de l'index, on retrouve un tableau dans lequel sont affichées les informations des machines déconnectées. Au pied de la page, on peut voir le délai de rafraichissement de la page ainsi qu'un bouton (à droite) permettant d'accéder à une page de paramètres (créée ultérieurement).

Hostname	État	Dernière activité	Client
PC-STAGIAIRE	<span style="color: red;">●</span> disconnected	01/06/2023 14:12	VFLIT

Rendu de l'index

Pour ce qui est de l'affichage des données, nous avons décidé au départ d'utiliser du JavaScript, ce qui permettait d'aller lire les fichiers contenant les données dans le but d'ajouter des lignes dans le tableau si une machine était déconnectée.



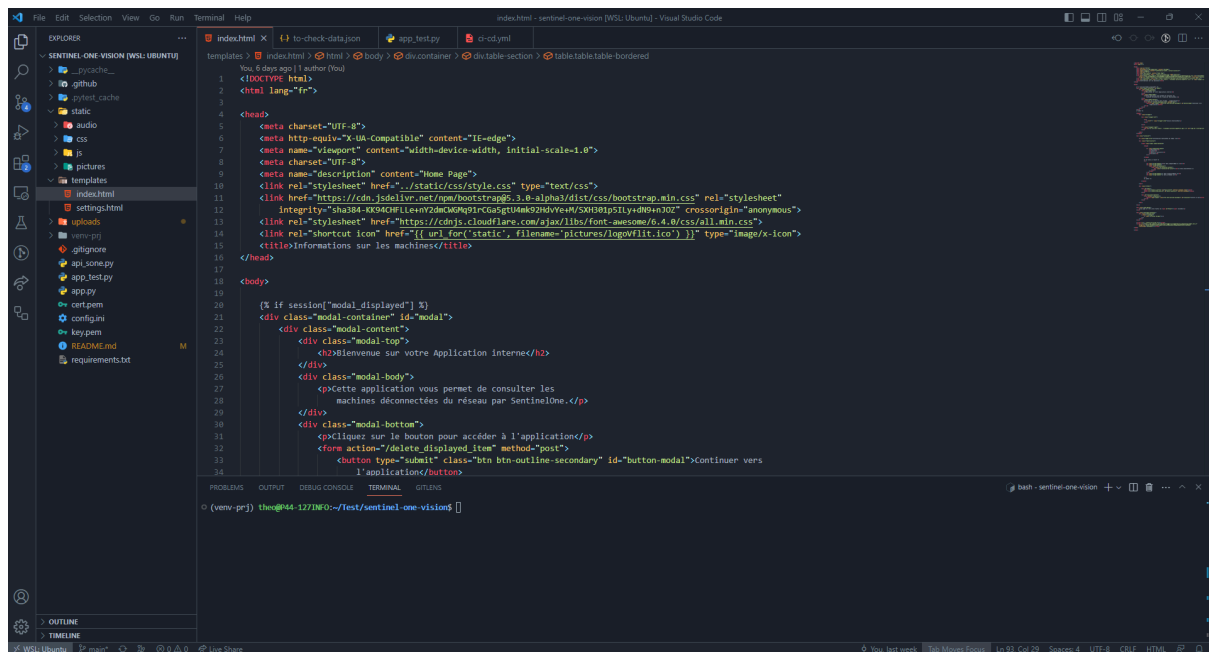
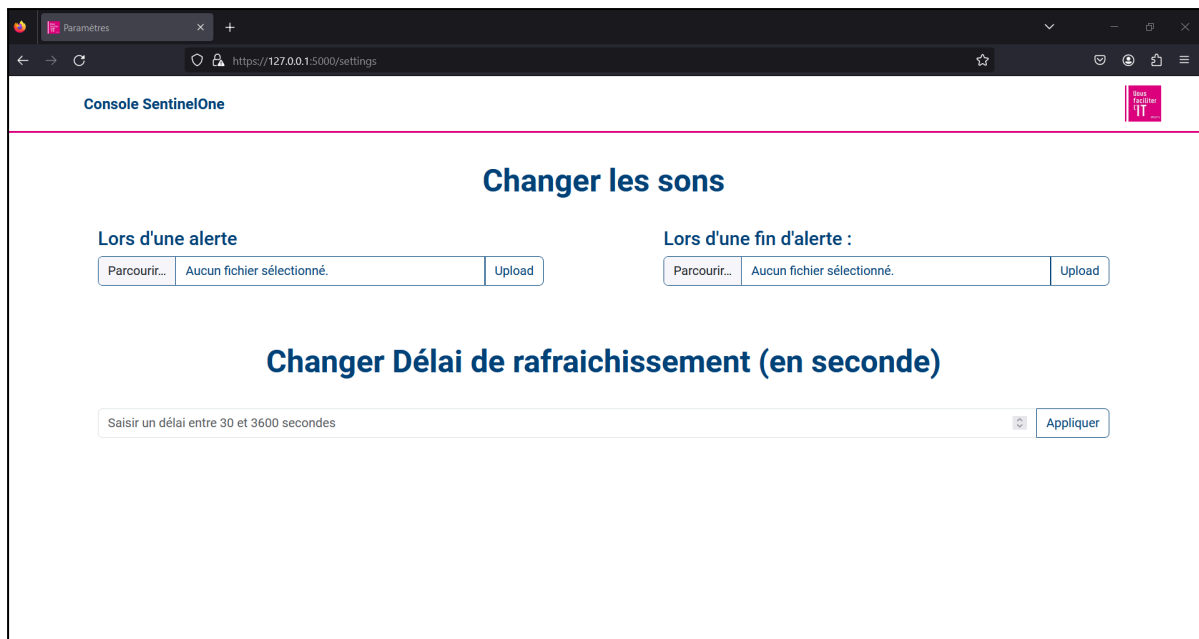


Image représentant l'interface de Visual Studio Code.

La semaine suivante, de nouveaux besoins m'ont été communiqués. En plus d'avoir les alertes, l'application devait déclencher des sons s'il y avait une nouvelle alerte ou une alerte en moins. On devait faire en sorte de pouvoir changer le délai de rafraichissement de l'index. Pour ce faire, on a donc dû revoir la structure du projet, en y intégrant un nouveau module Python, Flask<sup>4</sup>. Ce changement a donc complètement changé le fonctionnement de l'appli, car il fallait maintenant créer des routes<sup>5</sup> pour pouvoir relier les fichiers HTML permettant l'affichage avec les fichiers Python utilisés pour requêter l'API SentinelOne. Ces routes permettent également de créer des liens vers les autres types de fichiers (son, JSON...).

Afin d'intégrer les sons et un nouveau délai, on a dû créer une nouvelle page dans l'application. Cette page contient trois formulaires dont deux permettant d'intégrer un son et un pour changer le délai.



Aperçu de la page settings.html


Cette semaine a aussi été marquée par un changement important dans mon environnement de travail. J'ai installé WSL<sup>6</sup> sur mon poste. Le but de WSL est de pouvoir mettre en place un environnement Linux sur Windows sans avoir à passer par une machine virtuelle. Cela permet notamment de faciliter l'installation et la gestion des dépendances nécessaires, mais aussi de faciliter les fixations de bug sur l'application. Ce changement implique de travailler dans un système Linux et cela m'a permis notamment de découvrir les commandes de base pour créer et déployer une application.

Pour ce qui est des sons, nous avons opté, dans un premier temps, pour utiliser Javascript. Cependant, cette manière de faire a généré des problèmes. Il était indispensable que les sons se jouent indéfiniment jusqu'à ce que quelqu'un utilise le bouton d'accusé de l'alerte pour l'arrêter. Or, avec le JavaScript, le son ne se jouait qu'une seule fois ou alors il se répétait pendant une minute, jusqu'au rafraîchissement suivant de la page. C'est pourquoi nous avons décidé de créer de nouvelles routes Flask permettant de jouer les sons et de pouvoir gérer l'affichage du bouton d'accusé. Pour savoir s'il y avait une nouvelle alerte ou une fin d'alerte, on a créé un nouveau fichier JSON qui allait contenir le nombre actuel de

machines déconnectées, et celui à l'occurrence précédente (une minute avant). Ensuite, pour comparer ces valeurs, nous avons utilisé tout de même du JavaScript pour créer des redirections en fonction de ces dernières.

Les sons nous ont causé beaucoup de problèmes pour diverses raisons. Premièrement, il fallait trouver un moyen de rediriger l'utilisateur en fonction des données récoltées, ce qui entraînait au début des redirections infinies et qui a été corrigé par la suite. Deuxièmement, sachant que le son devait se déclencher automatiquement, nous avons été confrontés aux politiques de l'autoplay des navigateurs, qui empêchent les sons de se jouer seul (voir politique de l'autoplay dans la photo ci-dessous).

Chrome's autoplay policies are simple:

- Muted autoplay is always allowed.
  - Autoplay with sound is allowed if:
    - The user has interacted with the domain (click, tap, etc.).
    - On desktop, the user's [Media Engagement Index](#) threshold has been crossed, meaning the user has previously played video with sound.
    - The user has [added the site to their home screen](#) on mobile or [installed the PWA](#) on desktop.
  - Top frames can [delegate autoplay permission](#) to their iframes to allow autoplay with sound.
- 

Politique de l'autoplay pour Chrome (Source : [developer.chrome.com](https://developer.chrome.com/en/docs/autoplay/))

On arrive désormais à la troisième semaine de stage avec ce problème majeur. Pour le régler, nous avons choisi d'utiliser le second point de la capture d'écran précédente, qui consiste à demander à un utilisateur d'effectuer une action avec l'application (un clic sur un bouton par exemple). Nous avons créé un modal comprenant un bouton pour accéder à l'interface. Cependant, nous devons maintenant gérer l'apparition de cette dernière. Nous voulions que le modal ne s'affiche uniquement lorsque l'on arrive sur la page, et non à chaque rafraichissement de page.

C'est pourquoi nous avons utilisé les sessions avec Flask pour créer un cookie permettant de savoir si l'utilisateur est déjà sur la page ou pas.

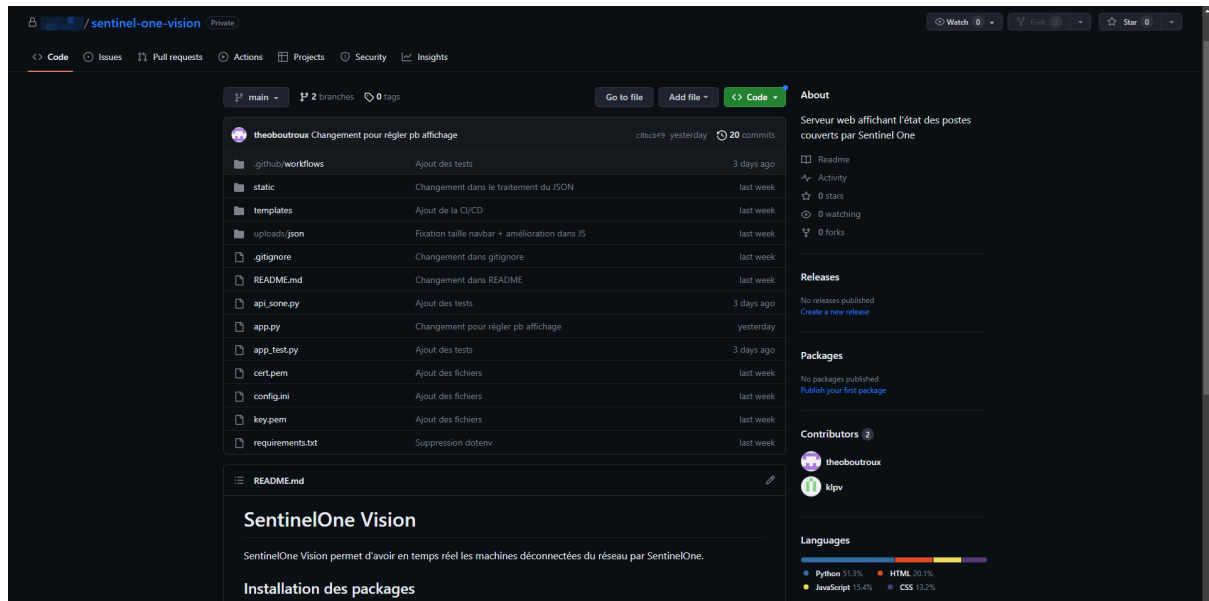
Durant cette semaine, nous avons également opéré un changement dans le tableau de la page index. Dans un souci de performance, nous avons utilisé une structure Jinja<sup>7</sup> dans le fichier HTML pour gérer dynamiquement ce dernier. Nous avons également essayé de tester Socketio, un module Python permettant de gérer dynamiquement les éléments d'une page Web. Cependant, ce test n'ayant pas marché, nous sommes restés sur la solution précédente, qui fonctionnait très bien.

Pour conclure la troisième semaine, nous nous sommes penchés plus particulièrement sur la sécurité de l'application, afin de s'assurer de son bon fonctionnement et de la protéger contre toute vulnérabilité. Les éléments à sécuriser étaient surtout contenus dans la page settings. Cela impliquait les 3 champs de saisie. Pour ce faire, nous avons réalisé des tests dans le back-end de l'application (Python), dans lequel on a inclus des conditions, pour vérifier si les données correspondaient à celles attendues (bon format de fichier, type de valeur...).

Les dernières semaines étaient consacrées aux derniers ajustements à réaliser pour avoir une application fonctionnelle. Nous avons commencé par réaliser quelques tests unitaires en Python avec le module pytest. Cela permettait de tester certaines fonctions essentielles au bon fonctionnement de l'application. Parmi celles-ci, on retrouve notamment les fonctions permettant de tester la connexion à l'API SentinelOne ainsi que celles pour récupérer les données.

Nous avons également décidé d'utiliser Git<sup>8</sup> afin de pouvoir facilement déployer l'application, mais aussi pour faciliter les changements potentiels dans cette dernière. C'est un outil utilisé par bon nombre de développeurs pour versionner les applications grâce à des commandes Linux comme "git push", "git commit", ou encore "git clone".

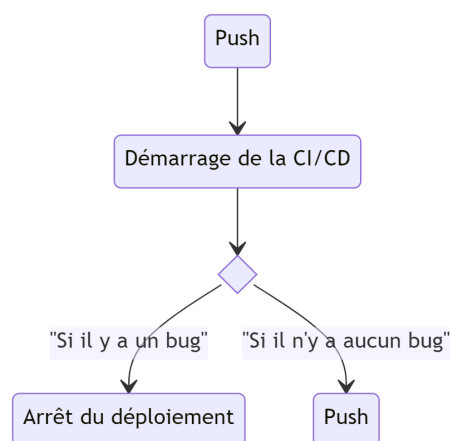
Dans notre cas, nous l'avons utilisé pour stocker notre code sur un dossier Github.



Dossier Github incluant le code source de l'application

Ensuite, nous avons décidé de créer ce qui s'appelle une CI/CD (Continuous Integration / Continuous Deployment) et qui permet d'automatiser le processus de déploiement d'une application. Dans notre cas, elle est déclenchée à chaque fois que quelqu'un réalise un "git push". Elle permet de tester l'installation de Python et de ses dépendances, avant de créer un environnement virtuel Python (venv) et d'exécuter le fichier contenant les tests à passer.

Voici le schéma de fonctionnement de notre CI/CD :



Enfin, à la fin du stage, nous avons pu déployer notre application sur une machine physique présente dans le service. Nous avons utilisé différentes commandes Linux pour récupérer le code stocké sur Github avec Git, mais aussi pour mettre le nouveau dossier au bon endroit sur la machine. Afin de pouvoir reproduire ces manipulations, nous avons également créé une documentation de déploiement (Cf. Annexe 1).

## **Difficultés rencontrées**

Pendant cette mission, j'ai été confronté à de nombreux bugs ou problèmes, tous résolus par la suite. Premièrement, en ce qui concerne l'utilisation d'une API, ce stage en est ma première expérience. J'ai donc dû comprendre comment trouver les bonnes données grâce aux bonnes URL. J'ai également eu par moment quelques problèmes de compréhension dans la documentation de l'API SentinelOne car tout était uniquement écrit en anglais. Deuxièmement, l'utilisation de Flask et des routes était un concept nouveau pour moi, ce qui m'a valu plusieurs jours avant de bien comprendre le fonctionnement de ce module Python. Ensuite, au cours du développement de l'application, le plus gros problème que nous ayons rencontré était les restrictions au niveau des navigateurs pour l'autoplay des sons. Ces dernières ne sont pas les mêmes entre les navigateurs (nous avons testé sur Chrome et Firefox) et donc cela a engendré des problèmes de compatibilité. Puis, j'ai sollicité mes collègues lorsque j'ai dû utiliser des sessions et des cookies pour gérer l'apparition de la modal. Le dernier point sur lequel j'ai rencontré quelques difficultés est la réalisation des tests unitaires avec pytest. J'ai eu du mal à comprendre son fonctionnement, ce qui fait qu'il n'y a que quelques tests dans ce fichier.

## V – Conclusion

Ces cinq semaines de stage chez OMR Infogérance ont été pour moi l'occasion de pouvoir découvrir le monde professionnel, et plus particulièrement dans une entreprise spécialisée dans l'IT. Ce stage m'a également permis de pouvoir découvrir le fonctionnement interne d'une entreprise ainsi que ses process internes. Grâce au projet que j'ai réalisé, j'ai pu participer aux différentes étapes de production d'une application, allant de la réunion initiale avec le client (ici le RSSI) au déploiement final, en passant par le développement et les phases de tests.

### Bilan personnel :

Cette expérience professionnelle a été pour moi l'occasion de confirmer mon intérêt pour le développement full-stack et m'a motivée pour réaliser de nombreux autres projets, qu'ils soient personnels ou professionnels.

D'un point de vue personnel, j'ai pu apprendre un nombre incalculable de choses, ce qui m'a permis de confirmer et développer mon intérêt dans le développement. Le stage a été également pour moi l'occasion d'en découvrir davantage sur la cybersécurité, que ce soit dans son aspect défensif qu'offensif. Cela m'a également permis de découvrir les différentes méthodes utilisées par l'entreprise pour tester la sécurité des systèmes informatiques des clients. Grâce au projet que j'ai réalisé durant les cinq semaines, j'ai pu avoir l'occasion de découvrir de nombreux outils qui vont me permettre de me professionnaliser lors du développement de mes projets futurs.

Enfin, ce stage chez OMR a été l'occasion de me rendre compte de l'importance du rôle de développeur. En effet, après avoir été confronté à des tests d'intrusion et à de réels cas de cyberattaques, j'ai pu réaliser à quel point la sécurité d'une application est primordiale lors du

développement d'une application pour assurer la protection des données de ses clients.

Voici la liste des compétences que j'ai pu acquérir ou développer :

- HTML : langage utilisé pour créer la structure d'une page Web
- CSS : Langage utilisé pour styliser une page Web
- JavaScript : Utilisé pour dynamiser une page Web
- Python : Langage côté serveur permettant de créer des fonctions et méthodes dans le but de créer des applications
- Git : Système de versionning du code source
- Linux : Système d'exploitation
- CI / CD : Outil permettant l'intégration continu d'une application

## **Bilan professionnel :**

D'un point de vue professionnel, ce stage a été pour moi l'occasion de rencontrer des personnes spécialisées dans l'IT, qui ont pu me partager leurs compétences et expériences. Cela a été également l'occasion pour moi de pouvoir me familiariser avec le monde professionnel. J'ai aussi pu améliorer mes soft skills, éléments clés à avoir en entreprise. Parmi ceux-ci, j'ai pu notamment développer mes compétences en matière de communication et de coopération avec les autres. J'ai eu la chance d'avoir des personnes passionnées dans le service cybersécurité, qui ont pu m'aider lorsque je rencontrais des difficultés. De plus, j'ai également pu développer ma capacité d'écoute, notamment en écoutant les besoins et les conseils qu'on a pu me transmettre lors de mon stage. Ce stage m'a appris à être plus persévérant pour pouvoir atteindre les objectifs donnés malgré les difficultés rencontrées.



## VI – Bibliographie

**Flask<sup>4</sup>** : Flask est un micro-framework Python utilisé pour le développement rapide d'applications web. Il offre les fonctionnalités essentielles pour créer des applications web légères et flexibles, tout en laissant aux développeurs la liberté de choisir les bibliothèques et les outils qu'ils souhaitent utiliser.

**Route<sup>5</sup>** : Une route Flask est une fonction dans une application Flask qui est associée à une URL spécifique. Elle permet de définir les actions à effectuer lorsque cette URL est appelée par un client, comme afficher une page HTML, traiter des données ou retourner une réponse JSON.

**WSL<sup>6</sup>** : C'est un environnement de compatibilité intégré à Windows 10 et aux versions ultérieures, permettant d'exécuter des applications et des commandes Linux directement sur un système d'exploitation Windows. Il fournit une couche de compatibilité qui traduit les appels système Linux en appels Windows, ce qui permet aux utilisateurs d'accéder à une grande variété d'outils et de logiciels disponibles sur les distributions Linux populaires, tels que Ubuntu, Debian et Fedora, sans avoir besoin d'installer un système d'exploitation Linux séparé.

**Jinja<sup>7</sup>** : Jinja est un moteur de template pour le langage de programmation Python. Il permet de générer des documents dynamiques en combinant des modèles HTML, XML, YAML, JSON ou tout autre format de données avec du code Python. Jinja utilise une syntaxe simple et expressive, basée sur des balises et des variables, pour décrire comment les données doivent être affichées ou manipulées dans le document final. Il offre des fonctionnalités avancées telles que l'héritage de modèles, les filtres, les boucles et les conditions, ce qui facilite la création de templates réutilisables et flexibles. Jinja est largement utilisé dans les frameworks web Python tels que Flask et Django pour générer des pages web dynamiques et personnalisées.

**Git<sup>8</sup>** : Git est un système de contrôle de version distribué qui permet de gérer efficacement les modifications apportées à un ensemble de fichiers au fil du temps. Il offre aux développeurs la possibilité de suivre, de sauvegarder et de synchroniser leurs modifications, enregistrant l'historique complet des modifications effectuées sur un projet. Git facilite également la collaboration en permettant à plusieurs personnes de travailler simultanément sur un même projet, de fusionner leurs modifications et de gérer les conflits éventuels. C'est un outil essentiel dans le développement de logiciels et dans d'autres domaines où la gestion des versions est cruciale.

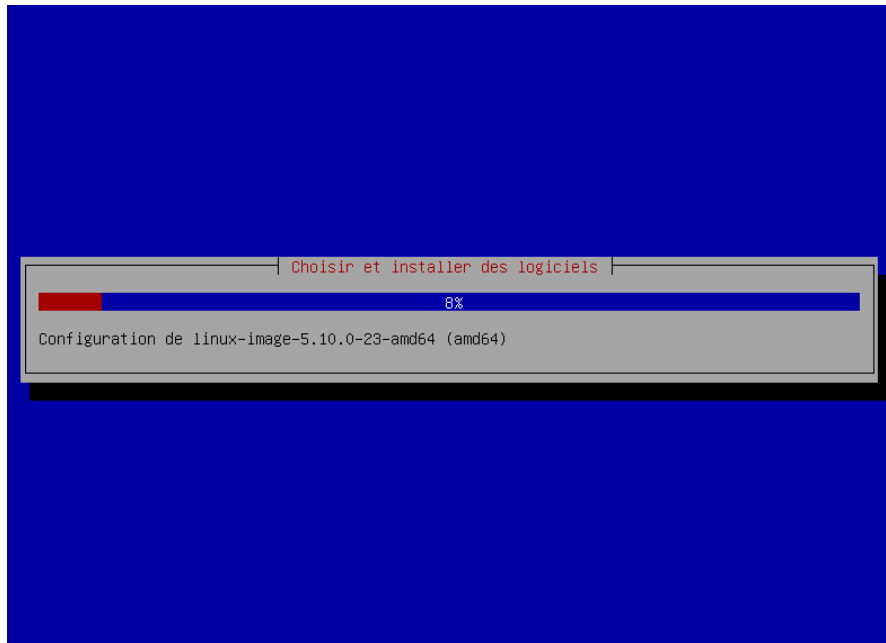
## VII – Annexes

### Annexe 1 : déploiement de supervision SENTINEL-ONE

#### Prérequis systèmes

- OS à jour
- Réseau interne et connexion internet
- Python v 3.10
- Compte Github fonctionnel
- Port 5000/tcp ouvert

1. Création de la VM (machine virtuelle) Debian sous VirtualBox



#### Prérequis de la VM

- 1) Passage en root

```
$ su
```

- 2) Mise à jour de la VM

```
# apt update
```

### 3) Installation de Git

```
# apt install git
```

```
Les NOUVEAUX paquets suivants seront installés :
  git git-man liberror-perl patch
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 7 505 ko dans les archives.
Après cette opération, 38,2 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] 0
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 liberror-perl all 0.17029-1 [31,0 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 git-man all 1:2.30.2-1+deb11u2 [1 828 kB]
Réception de :3 http://deb.debian.org/debian bullseye/main amd64 git amd64 1:2.30.2-1+deb11u2 [5 518 kB]
Réception de :4 http://deb.debian.org/debian bullseye/main amd64 patch amd64 2.7.6-7 [128 kB]
7 505 ko réceptionnés en 1s (5 994 ko/s)
Sélection du paquet liberror-perl précédemment désélectionné.
(Lecture de la base de données... 34259 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../liberror-perl_0.17029-1_all.deb ...
Dépaquetage de liberror-perl (0.17029-1) ...
Sélection du paquet git-man précédemment désélectionné.
Préparation du dépaquetage de .../git-man_1%3a2.30.2-1+deb11u2_all.deb ...
Dépaquetage de git-man (1:2.30.2-1+deb11u2) ...
Sélection du paquet git précédemment désélectionné.
Préparation du dépaquetage de .../git_1%3a2.30.2-1+deb11u2_amd64.deb ...
Dépaquetage de git (1:2.30.2-1+deb11u2) ...
Sélection du paquet patch précédemment désélectionné.
Préparation du dépaquetage de .../patch_2.7.6-7_amd64.deb ...
Dépaquetage de patch (2.7.6-7) ...
Paramétrage de liberror-perl (0.17029-1) ...
Paramétrage de patch (2.7.6-7) ...
Paramétrage de git-man (1:2.30.2-1+deb11u2) ...
Paramétrage de git (1:2.30.2-1+deb11u2) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
root@s1-vision:~#
```

Visuel de la VM après l'installation des paquets

### 4) Configuration de Git

```
# git config -global user.email "<votre adresse mail>"
# git config -global user.name "<Votre nom d'utilisateur>"
```

### 5) Génération d'une clé SSH

```
# ssh-keygen
```

Appuyer sur "Entrée" 3 fois

Voilà le rendu après la génération de la clé :

```
ssh-keygen  ssh-keyscan
root@sl-vision:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:GRLIOMpu9QgKaF2nGITP/1V2N8pZyD2QWtPLc50wIc8 root@sl-vision
The key's randomart image is:
+---[RSA 3072]-----+
|  o+ ..      . .+  |
| .o.o. o    +B .  |
|o.+.+ + .    +EO +|
|++ * . . o + + @o|
|= o +   S o o =  |
|.o . o .    +    |
|.      . .      |
|      .        |
|              |
+-----[SHA256]-----+
root@sl-vision:~#
```

6) Récupération de la clé publique pour la mettre dans github

```
# cat /root/.ssh/id_rsa.pub
```

La commande renvoie :

```
# ssh-rsa <Clé SSH>
```

7) Ajout de la clé dans Github

Aller sur Github puis :

→ Settings

→ SSH and GPG keys

→ New SSH key

## Déploiement

1) Aller dans le répertoire /opt

```
# cd /opt
```

2) Clonage du dossier créé auparavant sur Github

```
# git clone git@github.com:<utilisateur>/repository.git
```

```
root@sl-vision:~# cd /opt/  
root@sl-vision:/opt# git clone git@github.com:secufliit/sentinel-one-vision.git  
Clonage dans 'sentinel-one-vision'...  
The authenticity of host 'github.com (140.82.121.3)' can't be established.  
ECDSA key fingerprint is SHA256:p2OAMXNIC1TJYWeIOtrVc98/R1BUFWu3/LiyKgUfQM.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'github.com,140.82.121.3' (ECDSA) to the list of known hosts.  
remote: Enumerating objects: 162, done.  
remote: Counting objects: 100% (162/162), done.  
remote: Compressing objects: 100% (81/81), done.  
remote: Total 162 (delta 59), reused 145 (delta 46), pack-reused 0  
Réception d'objets: 100% (162/162), 3.16 Mio | 1.40 Mio/s, fait.  
Résolution des deltas: 100% (59/59), fait.  
root@sl-vision:/opt#
```

### 3) Installation de Python, de pip et de venv sur la VM

```
# apt install python  
# apt install python3-pip  
# apt-get install python3-venv
```

### 4) Création et démarrage d'un environnement virtuel Python

```
# python3 -m venv venv  
# source venv/bin/activate
```

### 5) Installation des paquets depuis le requirements.txt

⚠ Un requirements.txt est un fichier contenant l'ensemble des dépendances utilisées et leur version dans l'application

```
# pip3 install -r requirements.txt
```

## Visuel de l'installation des paquets


```
Collecting attrs>=23.1.0
  Downloading attrs-23.1.0-py3-none-any.whl (61 kB)
    |████████████████████| 61 kB 1.6 MB/s
Collecting autopep8>=2.0.2
  Downloading autopep8-2.0.2-py2.py3-none-any.whl (45 kB)
    |████████████████████| 45 kB 3.7 MB/s
Collecting bidict>=0.22.1
  Downloading bidict-0.22.1-py3-none-any.whl (35 kB)
Collecting blinker>=1.6.2
  Downloading blinker-1.6.2-py3-none-any.whl (13 kB)
Collecting certifi>=2023.5.7
  Downloading certifi-2023.5.7-py3-none-any.whl (156 kB)
    |████████████████████| 156 kB 4.0 MB/s
Collecting cffi>=1.15.1
  Downloading cffi-1.15.1-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (441 kB)
    |████████████████████| 441 kB 27.6 MB/s
Collecting charset-normalizer>=3.1.0
  Downloading charset_normalizer-3.1.0-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (199 kB)
    |████████████████████| 199 kB 105.2 MB/s
Collecting click>=8.1.3
  Downloading click-8.1.3-py3-none-any.whl (96 kB)
    |████████████████████| 96 kB 8.5 MB/s
Collecting cryptography>=40.0.2
  Downloading cryptography-40.0.2-cp36-abi3-manylinux_2_28_x86_64.whl (3.7 MB)
    |████████████████████| 3.7 MB 92.2 MB/s
Collecting dotenv>=0.0.5
  Downloading dotenv-0.0.5.tar.gz (2.4 kB)
```

## 6) Démarrage de l'application

```
# python3 app.py
```

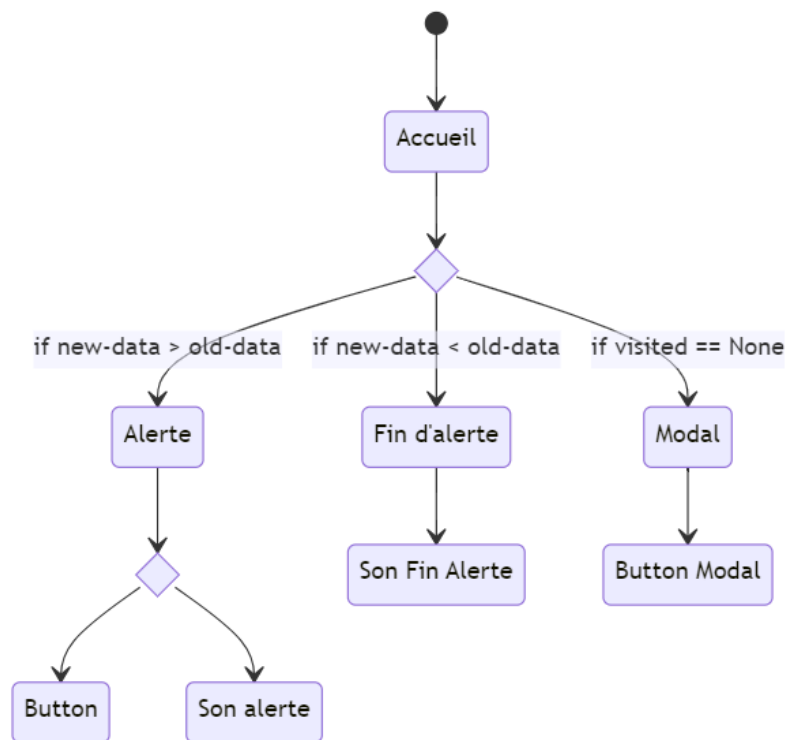
```
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on https://127.0.0.1:5000
* Running on https://192.168.46.73:5000
```

## 7) Aller sur le navigateur à l'adresse https://127.0.0.1:5000

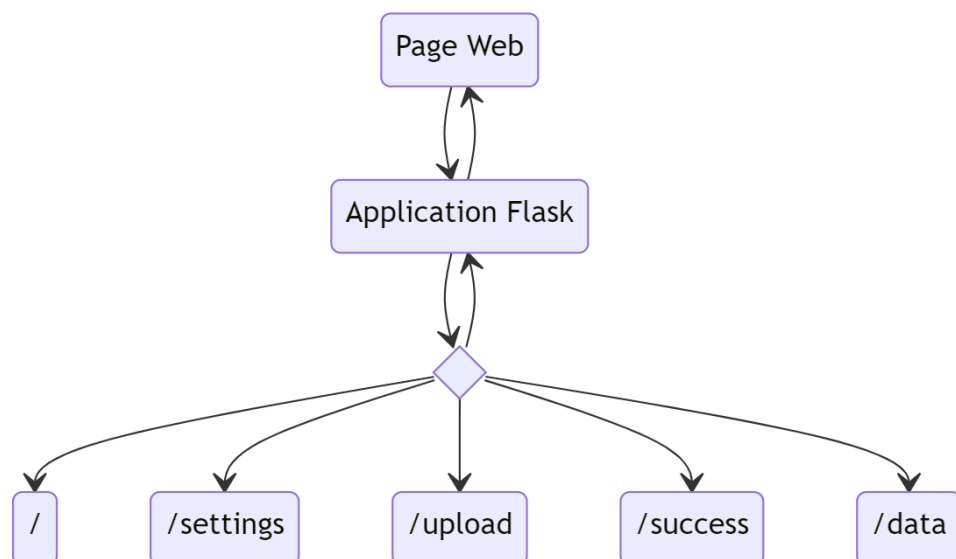
Console SentinelOne				
Informations SentinelOne en temps réel				
Hostname	État	Dernière activité	Client	

## Annexe 2 : Schémas de fonctionnement

Fonctionnement de l'appli



Les routes Flask



## Annexe 3 : Diplômes obtenus lors de cours en ligne sur la cybersécurité et sur les bonnes pratiques





## CERTIFICATION DÉLIVRÉE À

**Théo BOUTROUX**



Nous attestons que le candidat a suivi avec succès le module et obtenu le score suivant à l'évaluation

Module	Date de l'évaluation	Score
<i>Module Phishing</i>	2 mai 2023	19,33

## Annexe 4 : Lettre de recommandation

Nicolas NOEL (n.noel@vflit.fr)

RSSI

OMR Infogérance

21/06/2023

Objet : Lettre de recommandation pour Théo BOUTROUX

Madame, Monsieur,

Théo a récemment effectué un stage au sein de notre service cybersécurité chez OMR Infogérance. En tant que RSSI, j'ai pu superviser son travail pendant son mois de stage et j'ai particulièrement apprécié ses compétences techniques, son attitude professionnelle et sa contribution significative à notre équipe.

Théo s'est joint à nous en tant que stagiaire BTS SIO pour développer un outil de supervision de l'EDR que nous déployons chez nos clients. Il a démontré de l'enthousiasme pour le sujet et a rapidement su monter en compétences pour répondre au besoin.

En plus de ses compétences techniques, Théo est une personne humble et agréable qui a su s'intégrer rapidement au sein de l'équipe, communiquer clairement et obtenir l'aide dont il avait besoin.

Je recommande vivement Théo pour toute opportunité professionnelle future. Son enthousiasme, ses compétences techniques et sa capacité à s'intégrer à une équipe sont de très bons atouts.

Cordialement,

Nicolas NOEL