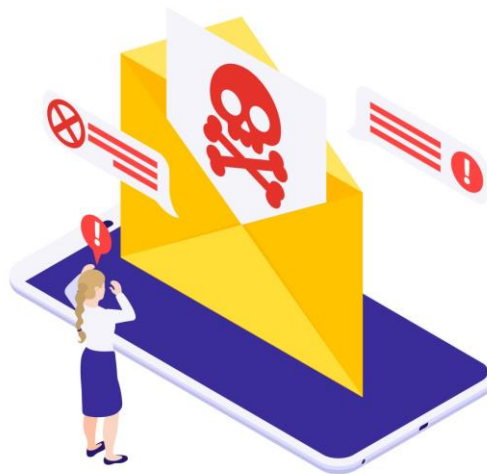


KM-ThreatAnalyzer : Une solution web pour l'analyse automatique des fichiers contre les menaces



Réalisé par : Karim maâli



Présentation :

Dans un contexte où les menaces informatiques deviennent de plus en plus fréquentes et sophistiquées, j'ai décidé de développer un outil simple, rapide et efficace pour aider à identifier les fichiers potentiellement dangereux.

C'est ainsi qu'est né **KM-ThreatAnalyzer**, une application web que j'ai conçue moi-même de A à Z, en utilisant Python (Flask), HTML, CSS et l'API publique de VirusTotal.

J'ai baptisé ce projet **KM-ThreatAnalyzer** en lien avec mes initiales (**KM**) et sa fonction principale : analyser les menaces dans les fichiers.

Ce projet représente non seulement un exercice technique personnel, mais également une solution concrète que toute entreprise ou particulier pourrait exploiter pour renforcer sa cybersécurité.



Fonctionnalités clés :

1. Téléversement simple de fichiers (PDF, EXE, ZIP, etc.).
2. Intégration de l'API VirusTotal pour l'analyse.
3. Interface épurée, responsive et sans dépendances externes.
4. Suppression automatique des fichiers uploadés après traitement.
5. Résultats affichés en temps réel de manière claire et lisible.



Technologies utilisées :

Backend : Python + Flask

Frontend : HTML / CSS / JS (dans un seul fichier)

Analyse : API VirusTotal



Pourquoi ce projet ?

En tant qu'étudiant passionné par la cybersécurité et les systèmes réseaux, je voulais développer un projet utile qui combine **API**, **sécurité**, et **expérience utilisateur fluide**.

KM-ThreatAnalyzer est donc à la fois une preuve de concept, un portfolio personnel, et un outil prêt à être utilisé.



Envie de tester ou de contribuer ?

Je suis ouvert aux feedbacks et à la collaboration. Si vous souhaitez :

- tester le projet en ligne
- contribuer à son évolution
- ou même l'intégrer à votre entreprise...

n'hésitez pas à me contacter via LinkedIn



Interface principale de KM-ThreatAnalyzer – Analyse de fichiers simplifiée

← → ↻ 🏠 ⓘ 127.0.0.1:5000 ☆ 📦 📄 📶 📱

🗄️ | 🌐 | 📺 | 📧 | 📍 | 📁 Tous les favoris

📄 | 🌐 | 📺 | 📧 | 📍 | 📁 Tous les favoris

KM-ThreatAnalyzer

Choisir un fichier Aucun fichier choisi

Analyser le fichier

L'interface est simple et intuitive. Il suffit de choisir le fichier que vous souhaitez analyser, puis de cliquer sur le bouton « Analyser le fichier » pour lancer l'analyse. Cette page représente la porte d'entrée du système de détection des menaces développé pour analyser les fichiers suspects.



Comment faire fonctionner :

Ouvrir le terminal et se placer dans le dossier du projet.

Vérifier que tous les modules nécessaires sont installés (flask, requests, python-dotenv, .).

python app.py

```
C:\KM-ThreatAnalyzer>python app.py
```

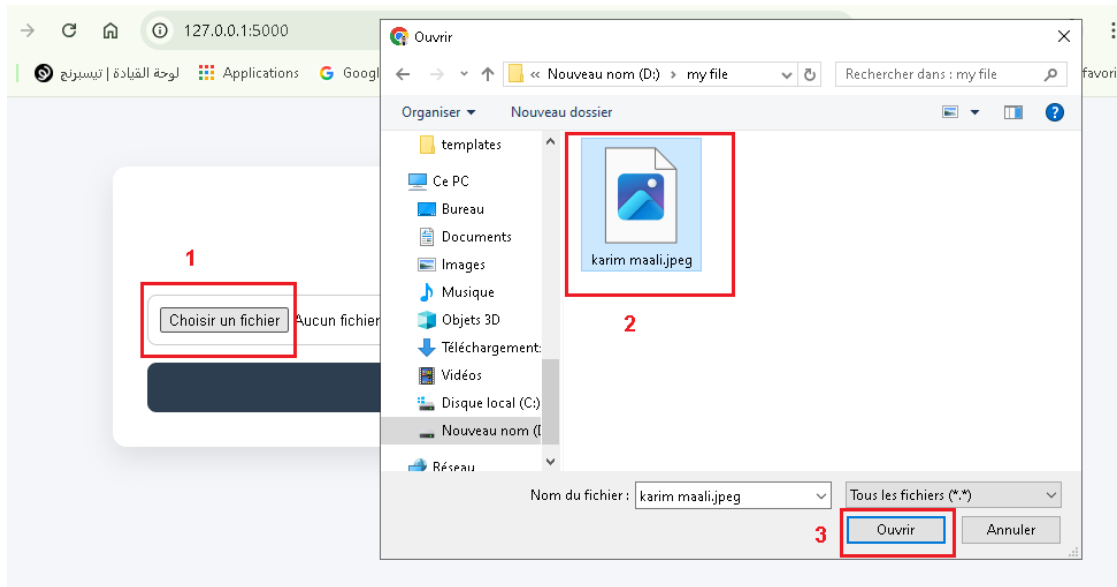
```
C:\KM-ThreatAnalyzer>python app.py
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://192.168.1.8:5000
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 274-554-770
```

Une fois lancée, ouvrir le navigateur et accéder à l'adresse suivante :

<http://127.0.0.1:5000>



Depuis l'interface web, choisir le fichier à analyser, puis cliquer sur « **Analyser le fichier** ».



KM-ThreatAnalyzer

Choisir un fichier karim maali.jpeg

Analyser le fichier

🔍 Le résultat s'affichera après l'analyse

Résultats de l'analyse

Fichier :	karim_maali.jpeg
Malveillant :	0
Suspect :	0
Sain :	0
Non détecté :	61

Revenir à l'accueil

Maintenant, nous allons tester l'analyse avec un fichier malveillant afin de simuler un scénario réel.

KM-ThreatAnalyzer

Choisir un fichier virus.txt

Analyser le fichier

Ce fichier contient un code malveillant détecté lors de l'analyse.

Résultats de l'analyse

Fichier :

virus.txt

Malveillant :

66

Suspect :

0

Sain :

0

Non détecté :

3

[Revenir à l'accueil](#)



Conclusion :

Ce site est une version expérimentale destinée à démontrer les capacités d'analyse automatique des fichiers suspects.

À l'avenir, je prévois d'ajouter de nombreuses fonctionnalités avancées pour améliorer la précision, la rapidité et l'expérience utilisateur.