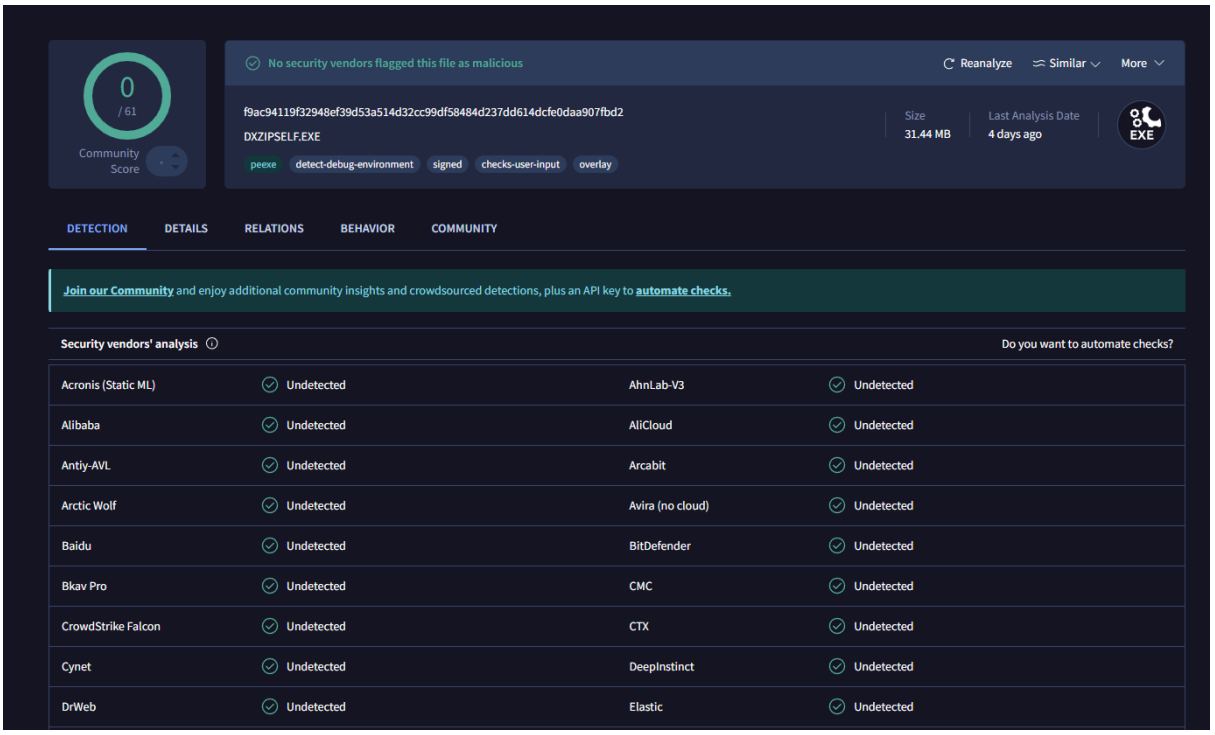
Exemple d’analyse d’un binaire

Lors de mon stage de 3eme année de licence au sein d’un soc j’ai pu analyser plusieurs binaire suspect grâce a l’edr et la sandbox, en voici un exemple.

Execution from Music Folder

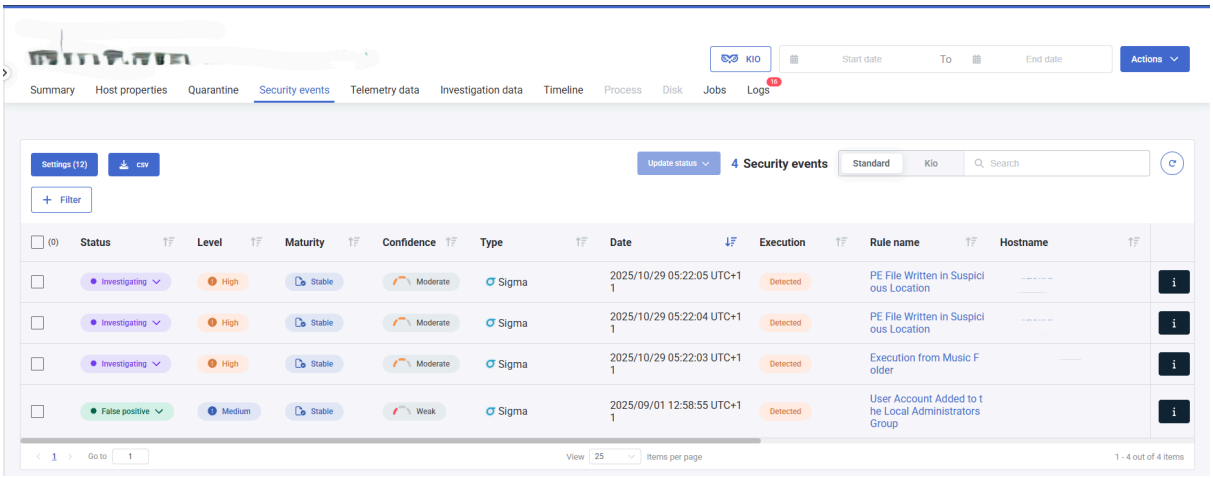
On voit un exécutable qui se nomme Y22B_C1-hostm-210.EXE, l’alerte se déclenche car c’est un exécutable qui a été exécuter depuis le répertoire Music. L’lorsqu’un binaire est lancé depuis un dossier personnel il y a des chances pour qu’il soit malveillant.

virus total :



On voit un score de 0/61, c’est rassurant.

Je check si sur ce poste il y a eu des evenements apres cet executable,



C’est le cas, pas bon signe.

Je vois que je peux télécharger cet exécutable, je vais le mettre dans une sandbox,

après analyse on a ceci :

La partie intéressante se trouve dans la section “Modified Files” .

On y voit beaucoup d’installation dans le répertoire /Temp/gdi, apres une simple recherche on sait que

"Dans `C:\Users\<USER>\AppData\Local\Temp\gdi\` *tu trouves principalement des fichiers temporaires liés aux drivers d’imprimantes, souvent Brother."*

dans toutes ces lignes on y trouve 2 exécutables :

C:\Users\w10cape\AppData\Local\Temp\gdi\dpinstx64.exe
C:\Users\w10cape\AppData\Local\Temp\gdi\dpinstx86.exe

Ce sont **des installateurs de drivers Microsoft**.

- **dpinstx64.exe** → pour Windows **64 bits**
- **dpinstx86.exe** → pour Windows **32 bits**

> *Ils servent à **installer les pilotes PnP** (Plug and Play) proprement, avec signature, copie des .dll, etc.*
>
> *Présents lors :*
>
> - *installation de périphériques (imprimantes, scanners, USB...)*
> - *mises à jour de drivers*
> - *exécutés souvent en arrière-plan ou via un setup principal*
>
> ➡️*Légitimes si associés à un driver connu. Suspicion uniquement si présents dans un contexte louche ou lancés sans raison.*

Donc on va voir si ils sont associé a un drivers connu :

après quelques recherches j'ai trouvé que dans l'installation de driver on a 2 types de fichiers obligatoire :

.inf : Windows le lit pour savoir comment installer un pilote.

.cat : Permet à Windows de vérifier que le driver n'a pas été modifié et qu'il provient d'un éditeur de confiance

On va donc les chercher :

C:\Users\w10cape\AppData\Local\Temp\gdi\BROHL22A.CAT
C:\Users\w10cape\AppData\Local\Temp\gdi\BROHL22A.INF

Très simple :

BROHL22A.INF
→ C'est le fichier de configuration du pilote.
→ Il indique que ce pilote concerne probablement un **périphérique Brother** (imprimante ou scanner).
→ Le nom contient **HL**, qui renvoie généralement à la gamme **Brother HL** (imprimantes laser).

BROHL22A.CAT
→ C'est le fichier de signature du **même pilote**.
→ Il garantit que BROHL22A.INF (et les autres fichiers du driver) n'ont pas été altérés.

Donc :
Ces deux fichiers appartiennent à un **driver Brother HL**, destiné à installer et authentifier le support de cette imprimante.

On peux donc conclure que cette alerte est un faux positif et est donc seulement une installation de driver pour imprimante.