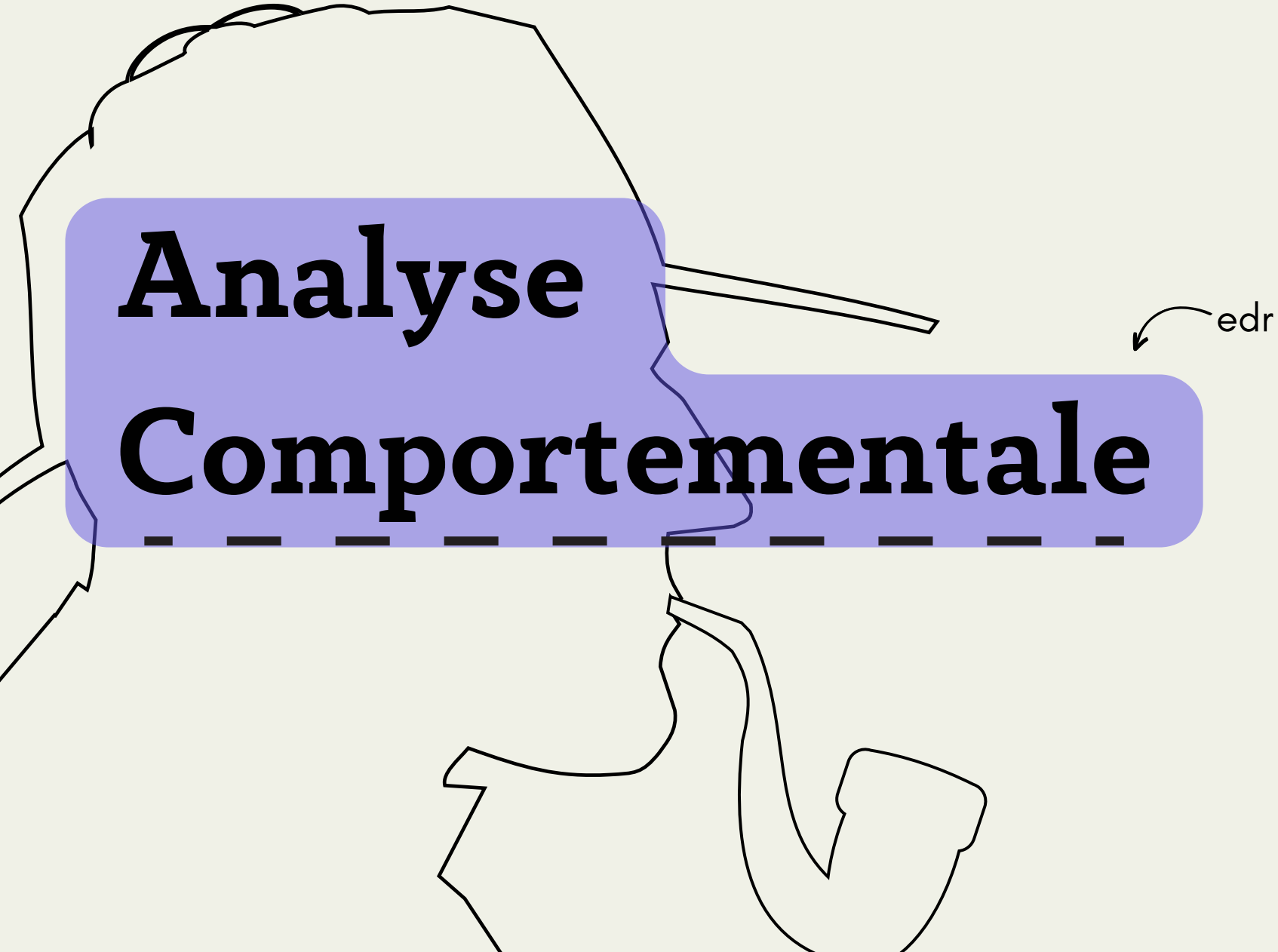
Hi.bouddhaWrite

Killian 'bouddha' PRIN-ABEIL

# Analyse Comportementale

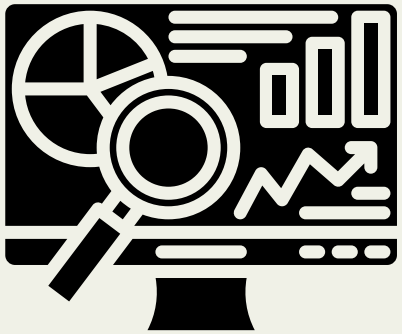


Killian 'bouddha' PRIN-ABEIL

# Analyse comportementale

**Qu'est ce que l'analyse comportemantale ?**

L'analyse comportementale est une approche novatrice visant à détecter les menaces ainsi que les activités malveillantes sur un réseau informatique. Elle se concentre particulièrement sur les comportements et les utilisations anormales pouvant être réalisés par un pirate informatique, dans le but de le bloquer.



Killian 'bouddha' PRIN-ABEIL

# EDR

**Qu'est-ce que l'EDR ?**

EDR, ou Endpoint Detection and Response, est une approche de sécurité visant à détecter et à répondre aux menaces au niveau des endpoints (terminaux).

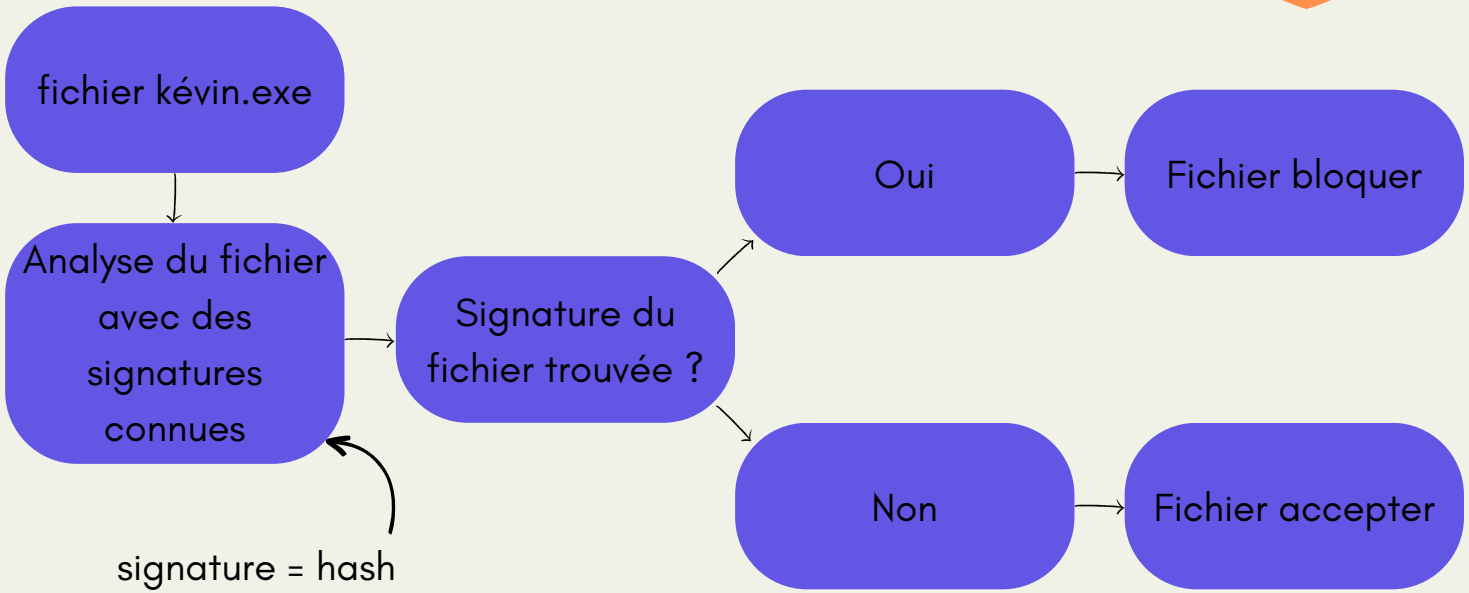
**Mais quel est le lien entre l'EDR et l'analyse comportementale ?**

Eh bien, l'EDR utilise l'analyse comportementale afin de détecter des activités suspectes sur les endpoints. Les informations recueillies par l'EDR, telles que les connexions réseau, les modifications de fichiers, etc., peuvent être analysées à l'aide de modèles comportementaux pour détecter les signes d'une intrusion ou d'une attaque en cours.

Killian 'bouddha' PRIN-ABEIL

# Fonctionnement

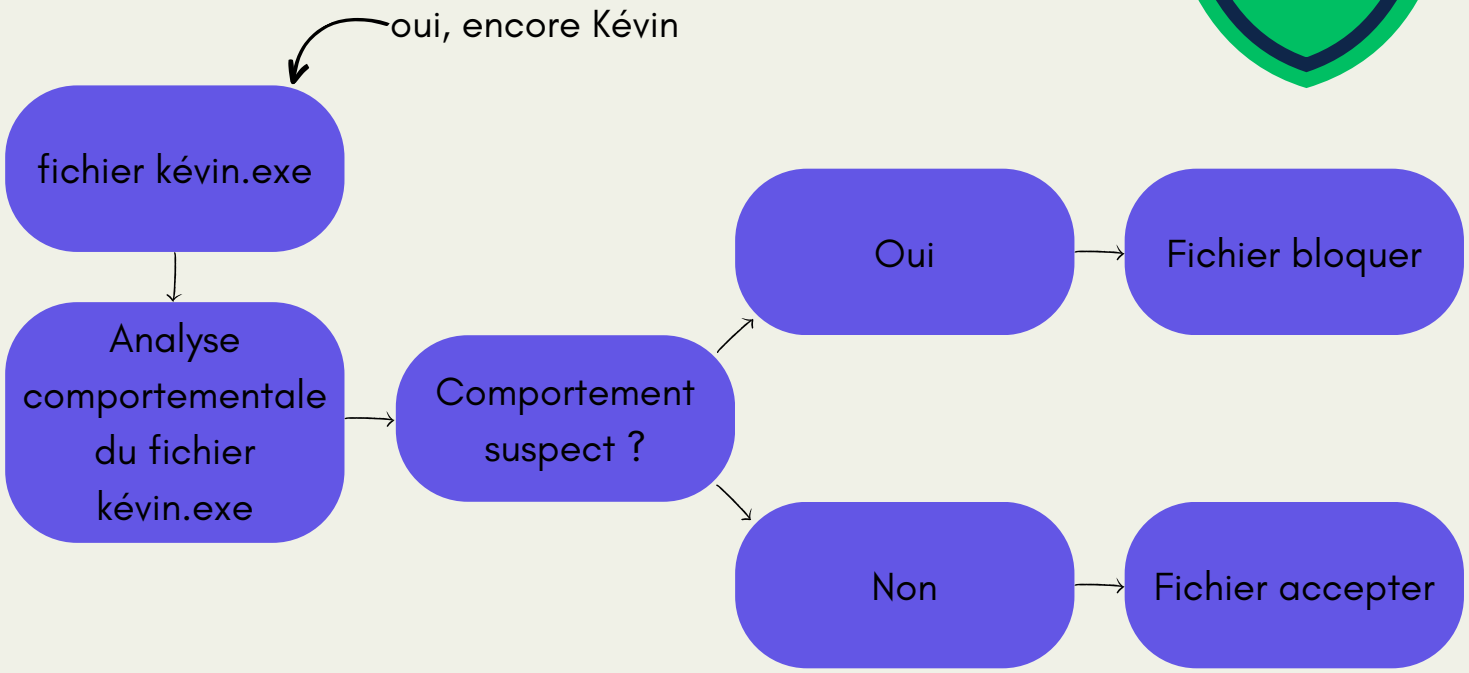
Fonctionnement d'un antivirus :



Killian 'bouddha' PRIN-ABEIL

# Fonctionnement

Fonctionnement de l'edr :



# Conclusion

**En conclusion**, comme vu précédemment, un antivirus analyse la signature d'un fichier pour déterminer s'il est accepté ou non. En revanche, l'EDR analyse le comportement d'un fichier, ne se limitant pas à sa signature ou aux signatures connues. Il observe le comportement du fichier pour détecter les indicateurs de compromission.

# Lien avec ma veille

demande en mariage à prévoir

**Bon, je vais encore parler de CrowdSec.**

Afin de mieux comprendre comment fonctionne CrowdSec, j'ai également dû comprendre le fonctionnement de l'analyse comportementale. CrowdSec parvient à mettre en place l'analyse comportementale grâce à plusieurs points :

- Collecte de données
- Analyse en temps réel des logs
- Mécanisme d'adaptation ou d'apprentissage automatique

Killian 'bouddha' PRIN-ABEIL

# Fin

"*My command lines are absolute.*"