

# VEILLE CYBERSÉCURITÉ

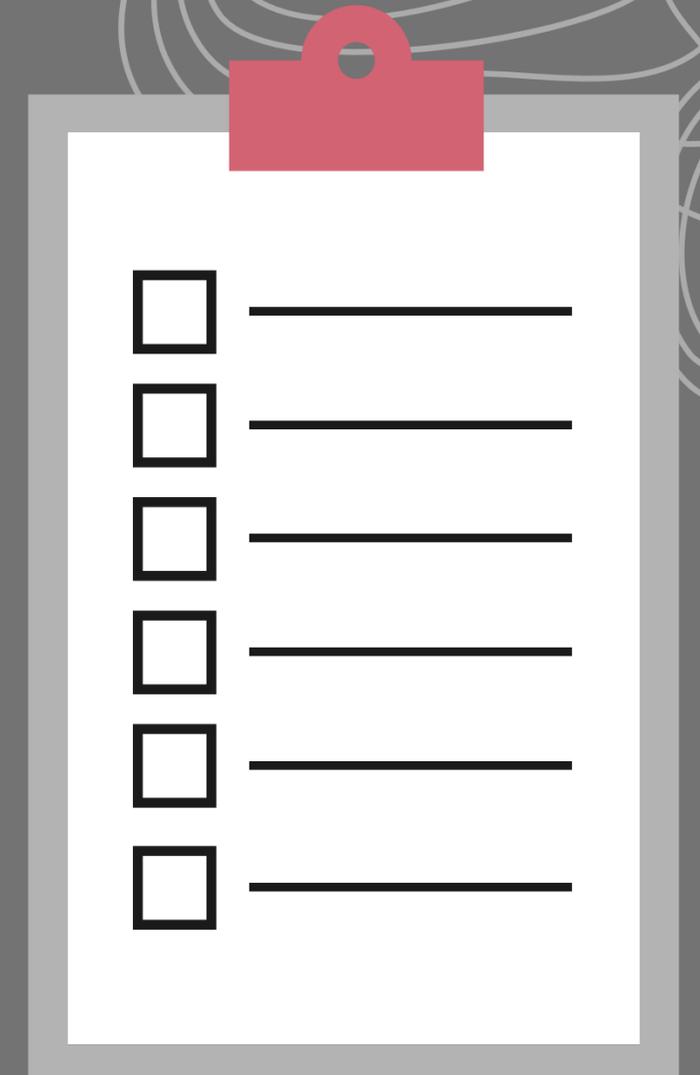
## WHITE HAT HACKERS



ARKI CLÉMENT

# SOMMAIRE

1. Introduction
2. Qu'est-ce qu'un White Hat Hackers ?
3. Rôle économique et impact utilisateur
4. Avantages et inconvénients
5. Les compétences, les qualités et l'éthique d'un White Hat Hacker
6. Responsabilités envers la société
7. L'évolution du rôle
8. Exemples d'actions de White Hat Hackers
9. Mon option personnelle



# 1. INTRODUCTION

- L'intérêt est d'en apprendre un peu plus sur le sujet des hackers éthiques, notamment des White Hat Hackers.
- Comprendre les enjeux liés à la sécurité informatique.



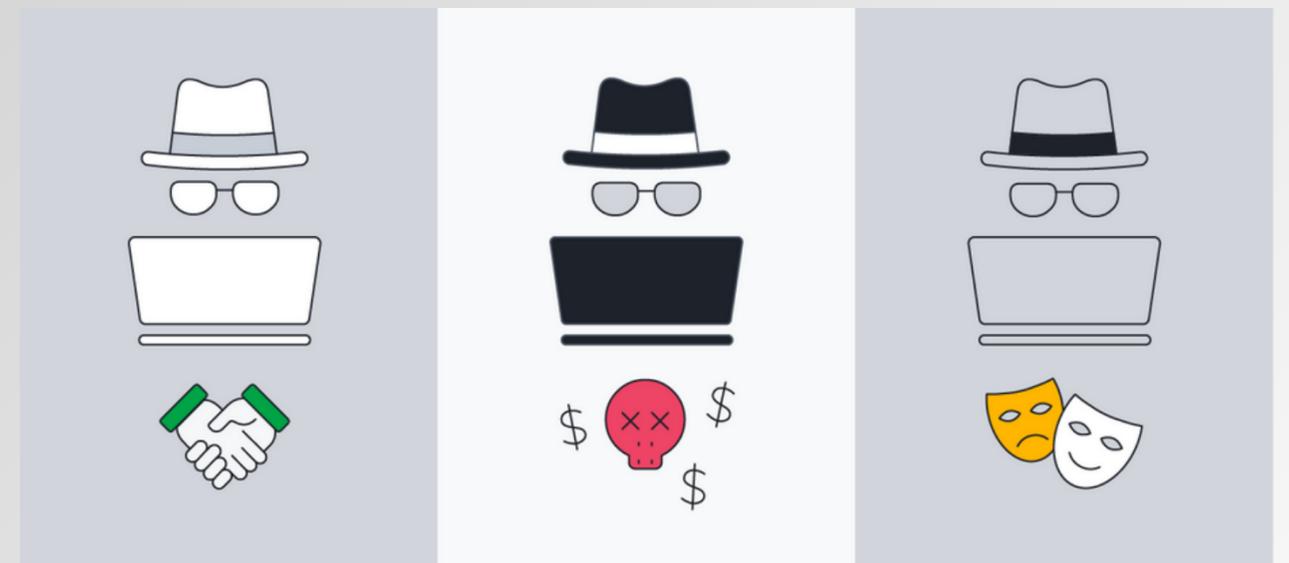
## 2. QU'EST-CE QU'UN WHITE HAT HACKERS ?

- Un White Hat Hacker : personne experte en sécurité informatique qui utilise des compétences de piratage pour identifier les vulnérabilités de sécurité du matériel, des logiciels ou des réseaux (essentiellement dans les entreprises).
- Ils agissent de manière légale et éthique.
- Émergence dans les années 1960 avec le développement des premiers systèmes informatiques
- Popularisé dans les années 1970 et 1980 avec la montée des culture hacker et des groupes de sécurité informatique
- Agissent en respectant les lois et règlements en vigueur en matière de piratage informatique.
- L'inverse des White Hat sont les Black Hat (agissent de manière malveillante)
- Termes origine des films de western : Chapeau blanc le shérif (White Hat) et chapeau noir le bandit (Black Hat)



# 3. RÔLE ÉCONOMIQUE ET IMPACT UTILISATEUR

- Rôle économique des White Hat Hackers :
  - Contribution à la sécurité informatique en identifiant et en corrigeant les vulnérabilités des systèmes informatiques.
  - En détectant des attaques, les hackers éthiques aident les entreprises à renforcer leurs défenses en évitant ainsi des pertes financières et de réputation.
  - En participant à des programmes avec des primes conséquentes pour la découverte de failles.
  - Salaire moyen d'un White Hat : 74 450 € par an.
  - Salaire par mois d'un Hacker éthique débutant : 4000€.
  - Salaire par mois d'un Hacker éthique confirmé : 7500€.
- L'impact des White Hat Hackers sur les utilisateurs :
  - Garantir la sécurité en ligne, ce qui renforce la confiance des utilisateurs dans les plateformes numériques.
  - Protègent des données personnelles lorsqu'ils découvrent des vulnérabilités.
  - Font en sorte de réduire les risques de piratage et de vol de données pour une utilisation plus sûre.



# 4. AVANTAGES ET INCONVÉNIENTS

## AVANTAGES



### Sécurité

Contribuent à la sécurité en ligne en identifiant et en corrigeant les vulnérabilités.



### Protection

Protègent les données personnelles et financières des utilisateurs.



### Confiance

Favorisent la confiance des utilisateurs envers les plateformes numériques.



### Prévention

Préviennent les cyberattaques et réduisent les risques de piratage.



### Sensibilisation

Sensibilisent à l'importance de la cybersécurité.

## INCONVÉNIENTS



### Divulgation

Risque de divulgation d'informations sensibles lors de la découverte de failles.



### Pression

Pression accrue pour résoudre rapidement les failles pour prévenir les attaques.



### Attentes

Attentes élevées de la part des parties prenantes pour éviter les violations de sécurité.



### Complexité

Peuvent être confrontés à des défis techniques complexes pour identifier les failles.



### Réputation

Risque de perte de réputation en cas d'erreur.

# 5. LES COMPÉTENCES, LES QUALITÉS ET L'ÉTHIQUE D'UN WHITE HAT HACKER

## COMPÉTENCES

- Capacité de compréhension des menaces en cybersécurité
- Capacité à exploiter des sources ouvertes de manière sécurisée
- Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
- Détection, qualification et analyse d'informations pertinentes
- Le droit et les réglementations en vigueur en matière de cybersécurité

## QUALITÉS

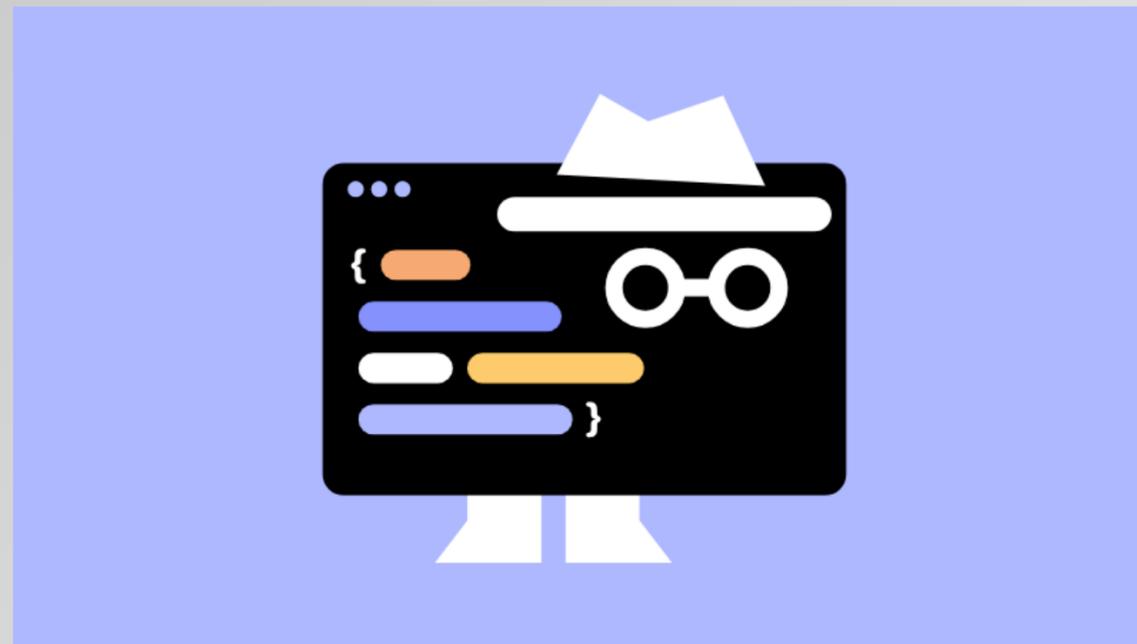
- Avoir un sens de la curiosité
- Être dynamique et réactif
- Savoir faire preuve de créativité
- Pourvoir être disponible
- Avoir un sens de la confidentialité
- Aimer le travail en équipe et le goût du défi

## ÉTHIQUE

- Engagement éthique : essentiel pour la recherche de vulnérabilité et aussi pour la préservation de la sécurité
- Certains agissent de manière illégale sans autorisation en voulant agir pour le bien (garde une éthique)
- Passé ambigu pour certains White Hat Hackers car il était impliqué dans des activités de piratage malveillant.
- Suite à ça, ont évolué vers des pratiques éthiques

# 6. RESPONSABILITÉS ENVERS LA SOCIÉTÉ

- Actuellement 84% des organisations font appel à des hackers éthique pour renforcer leur cybersécurité.
- Avant d'évaluer la sécurité du réseau d'une entreprise, l'hacker éthique sera soumis à une procédure qui sera :
  - Documenter le chemin d'attaque identifié.
  - Signer un accord de confidentialité.
  - Signaler immédiatement toute violation de sécurité.
  - Effacer toutes les traces de tests de vulnérabilités.



# 7. L'ÉVOLUTION DU RÔLE

- **Rôle s'élargie** en incluant :
  - La sensibilisation à la sécurité.
  - La collaboration avec les entreprises.
  - Anticiper les failles.
  - Renforcer les défenses.
  - **En formant de nouveaux experts en cybersécurité.**



- Les causes de ces évolutions :
  - **Menace de cyberattaques beaucoup plus présente aujourd'hui**
  - Besoins liés à l'instauration d'un environnement de travail hybride sécurisé.
- **Dépenses mondiales en logiciels, matériels et service de cybersécurité sera de 300 milliards de dollars d'ici 2026.**

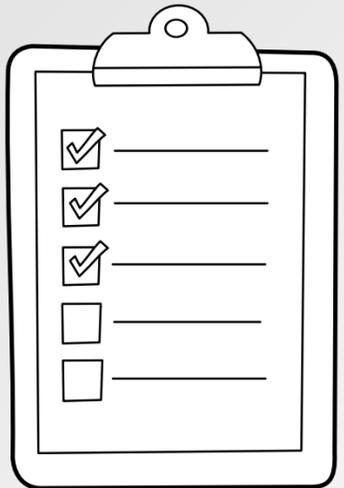
# 8. EXEMPLES D' ACTIONS DE WHITE HAT HACKERS

## **Attaque contre le secteur financier :**

Un "White Hat" a attaqué Ede Finance, provoquant une perte de 580 000 dollars, et exposé une vulnérabilité exploitée par les développeurs pour manipuler les prix. En réponse, l'équipe a pris des mesures correctives, supprimant le contrat problématique et remboursant les pertes des utilisateurs avec leurs propres fonds.

**Test de faille de sécurité chez FranceConnect :** Le gouvernement lance une campagne invitant les meilleurs génies de l'informatique à tester la sécurité du serveur France Connect, promettant une récompense de 20 000 € pour la découverte de failles critiques. La Direction interministérielle du numérique (Dinum) utilise cette initiative pour promouvoir le concept de "hacking éthique".

**Histoire d'un Anonymous (de Black Hat à White Hat) :** Hector Monsegur, ancien membre d'Anonymous et fondateur de LulzSec, a fait la transition du Black Hat au White Hat après avoir été arrêté par le FBI en 2011. En tant qu'informateur, il a aidé à identifier des membres d'Anonymous et de LulzSec. Après une peine de 7 mois de prison et une interdiction d'accès à Internet pendant 2 ans, Monsegur est devenu chercheur indépendant en sécurité, adoptant une approche éthique en tant que White Hat.



# 9. MON OPINION PERSONNELLE



- Je suis **en faveur des White Hat Hackers** car :
  - **Essentiel dans la sécurité informatique.**
  - Détecte les vulnérabilités et les failles au sein des systèmes informatiques : donc contribue contre les cyberattaques.
  - Des **professionnels légaux** sollicités pour évaluer la sécurité d'une organisation.
  - **Parfois dans l'illégalité mais ils gardent une morale (une éthique)** et agissent pour le bien.
- **Face au nouvelle menace : Il doit garantir la sécurité des systèmes et des données informatiques.**  
Ce rôle devient donc de plus en plus important.



**MERCI POUR  
VOTRE ATTENTION**

