

Terminologie de base Cyber

I. Types de hackers

Ils sont rangés par considérations éthiques au regard de la loi et non eu regard de leurs convictions.



Le "**white hat**"

Connu en tant que "**Hacker éthique**", ils sont employés par des sociétés privées ou des gouvernement pour identifier les failles et aider les entreprises et institution à se protéger. Il s'agit d'experts en cybersécurité agissants sous contrat et dans un cadre légal strict.

Ils comprennent entre autres :

- Les auditeurs en cybersécurité
- Les chercheurs en cybersécurité
- Les personnes agréées en OSINT



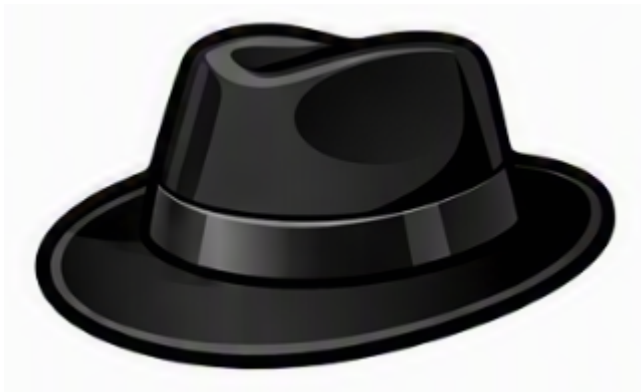
Le "Grey hat"

Bien qu'agissant souvent pour le bien commun ou pour prouver leurs compétences, ils le font à la marge du cadre légal voire en dehors. Il peut s'agir d'experts ou de "**freelance**" et agissent le plus souvent en électron libre. Leurs actions visent à révéler des faiblesses ou des failles dans les infrastructures, ou apporter une preuve de leurs compétences, bien qu'ils ne soient pas mandatés pour le faire.

Certains le font également pour alerter le public en exfiltrant des documents ou informations confidentielles.

Ils comprennent entre autres :

- Les lanceurs d'alertes
- Les "**security enthusiasts**"
- Les "**pentesters**" amateurs
- Les "**Hacktivistes**" (tant qu'ils n'ont pas de comportement destructeurs ou à visée terroriste).



Le "**Black hat**"

Il s'agit de tous les types de pirates malveillant ou agissant de manière destructive. On y retrouve toutes les activités cybercriminelles allant du Ransomware au vol d'information confidentielle. Si la plupart du temps, ils agissent pour l'argent, certains peuvent agir par raison politique.

Ils comprennent entre autre :

- Les cybercriminels (isolés ou en organisation)
- Les organisations terroristes
- Les '**script kiddies**'
- Les "**Hacktivistes**" plus extrémistes

II. Red Team, Blue Team

Revision #2

Created 2026-07-17 22:33:06 UTC by Olivier

Updated 2026-07-25 09:06:28 UTC by Olivier