SysDream
Cybersécurité Hub One

Rapport d'analyse de mots de passe

9/12/2025, 7:45:50 PM

Résumé

Un audit de la politique de mot de passe en place a été mené. À cette fin, des attaques par recherche exhaustive ont été conduites sur les condensats recueillis afin de fournir des statistiques précises. L'analyse des résultats a mis en évidence plusieurs lacunes par rapport à l'état de l'art.

Suite à cet audit, le risque lié à la politique de mot de passe en place a été évalué à **Elevé**.

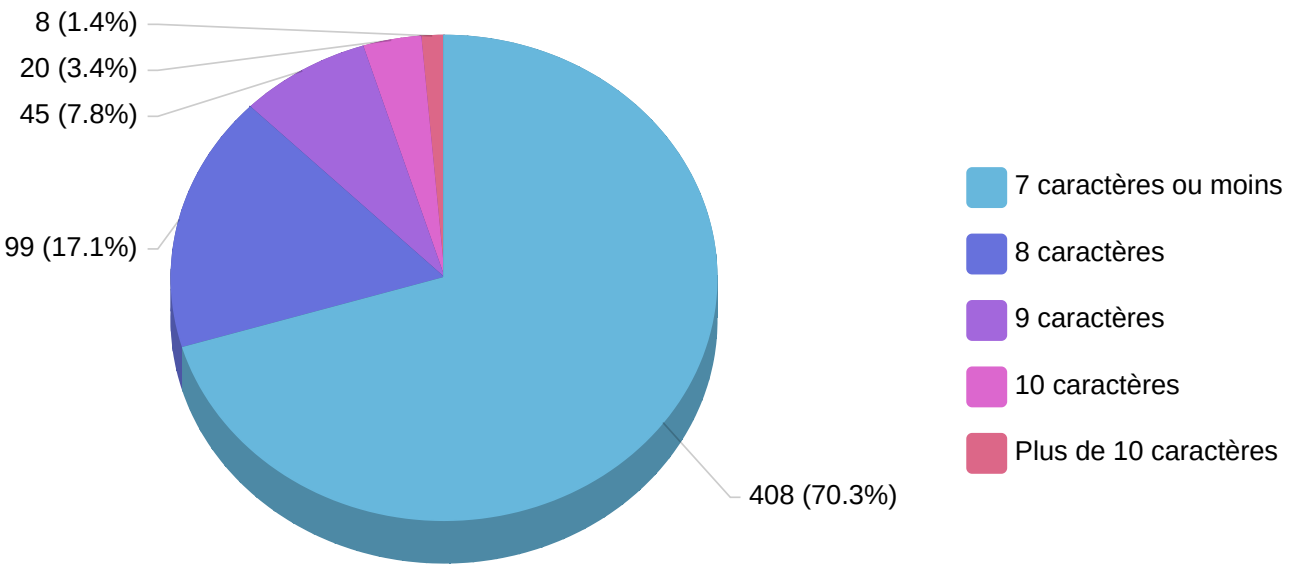
- Au total, **580** des **1000** condensats utilisateurs soit **58%** ont été cassés au cours de la prestation.
- L'utilisation de l'algorithme **LAN MANAGER** a été constatée sur **230** condensats de mot de passe, ce dernier est obsolète et vulnérable.
- Il a également été constaté que la réutilisation des mots de passe concernait **30.2%** des comptes.
- De plus, **84.3%** des mots de passe cassés ne respectent pas le niveau de complexité requis et **98.6%** la longueur recommandée.
- Enfin, **5** comptes utilisent un mot de passe égal au nom d'utilisateur, ce qui représente un risque de compromission immédiate.

Il est fortement recommandé de mettre en œuvre les remédiations décrites dans ce rapport afin d'implémenter une politique de mot de passe robuste conforme à l'état de l'art, et de veiller à son application par des moyens techniques à tous les niveaux.

Longueurs de mots de passe

Le graphique ci-dessous présente la répartition des mots de passe utilisateurs selon leur longueur. L'analyse de ces résultats montre que **572** des mots de passe cassés soit **98.6%** font **10 caractères ou moins**.
Les mots de passe courts sont beaucoup plus vulnérables aux attaques par force brute et au devinement, car ils permettent aux attaquants de tester rapidement toutes les combinaisons possibles.

Les principaux standards de sécurité recommandent d'utiliser des mots de passe d'au moins 12 caractères, en combinant lettres majuscules et minuscules, chiffres et symboles spéciaux lorsque cela est possible.



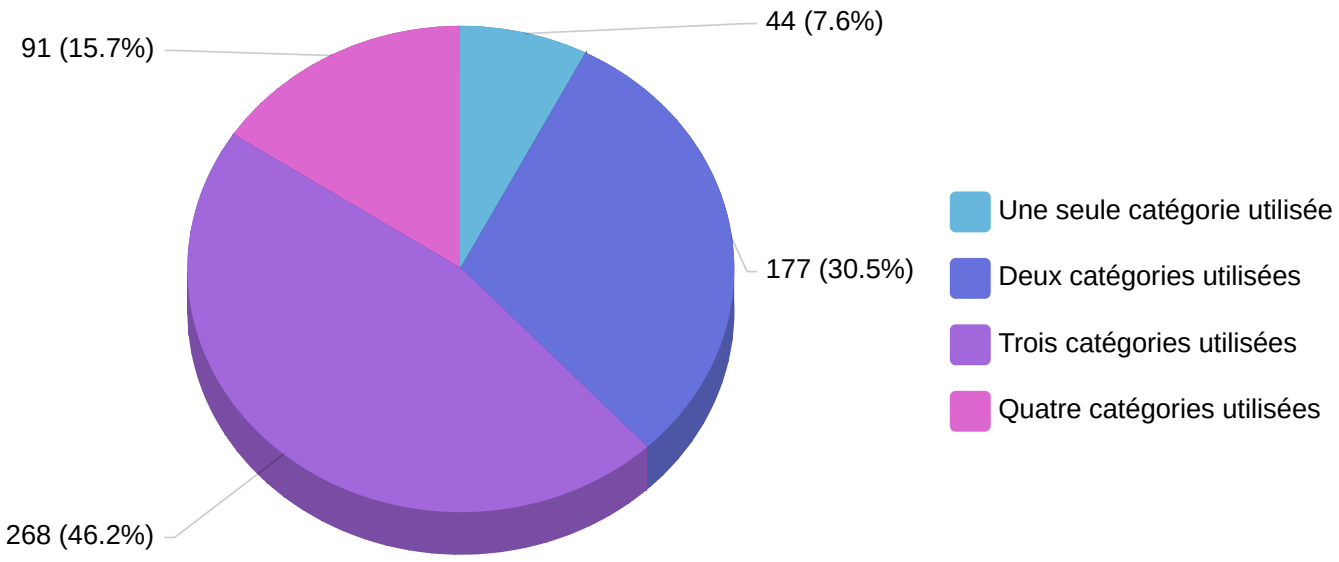
Complexité des mots de passe

Le niveau de complexité des mots de passe peut être évalué par le nombre de catégories utilisées :

- Lettres minuscules;
- Lettres majuscules;
- Chiffres;
- Caractères spéciaux.

Le graphique ci-dessous présente la complexité des mots de passe utilisateurs. L'analyse montre que **489** des mots de passe soit **84.3%** n'utilisent que **3 catégories de caractères ou moins**.

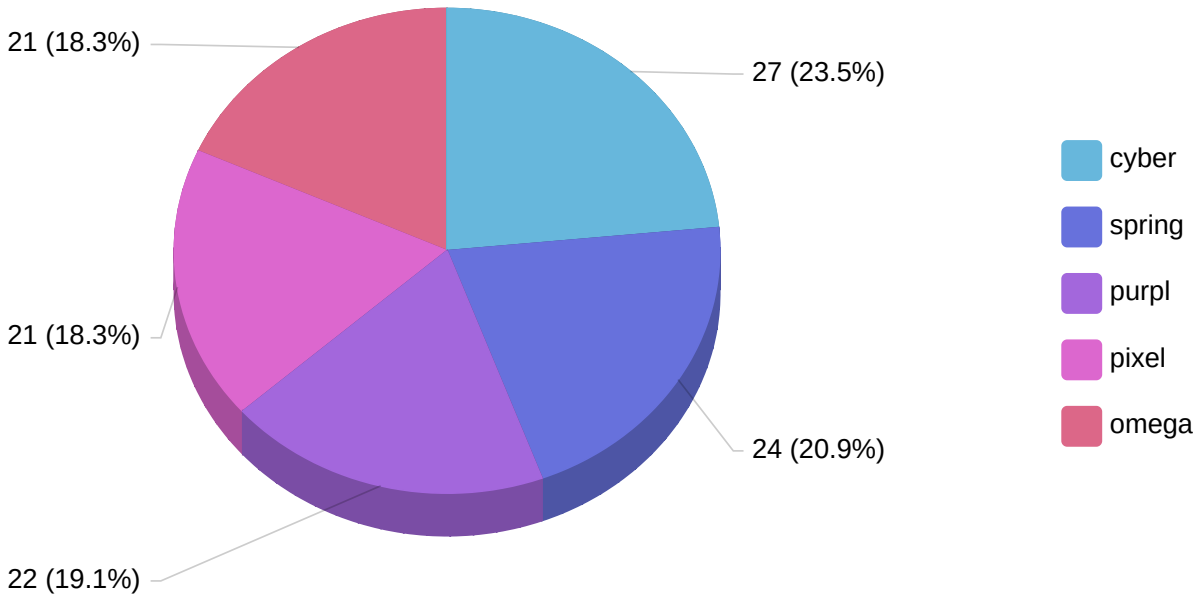
Les mots de passe combinant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux sont bien plus résistants aux attaques par recherche exhaustive. Les recommandations de sécurité préconisent l'utilisation de mots de passe contenant quatre catégories de caractères différentes pour renforcer la sécurité globale et réduire le risque de compromission.



Mots-clés les plus utilisés

Le graphique ci-dessous recense les mots-clés les plus fréquents dans le jeu de données analysé. Les mots **cyber** et **spring** apparaissent respectivement dans **4.7%** et **4.1% des mots cassés**.

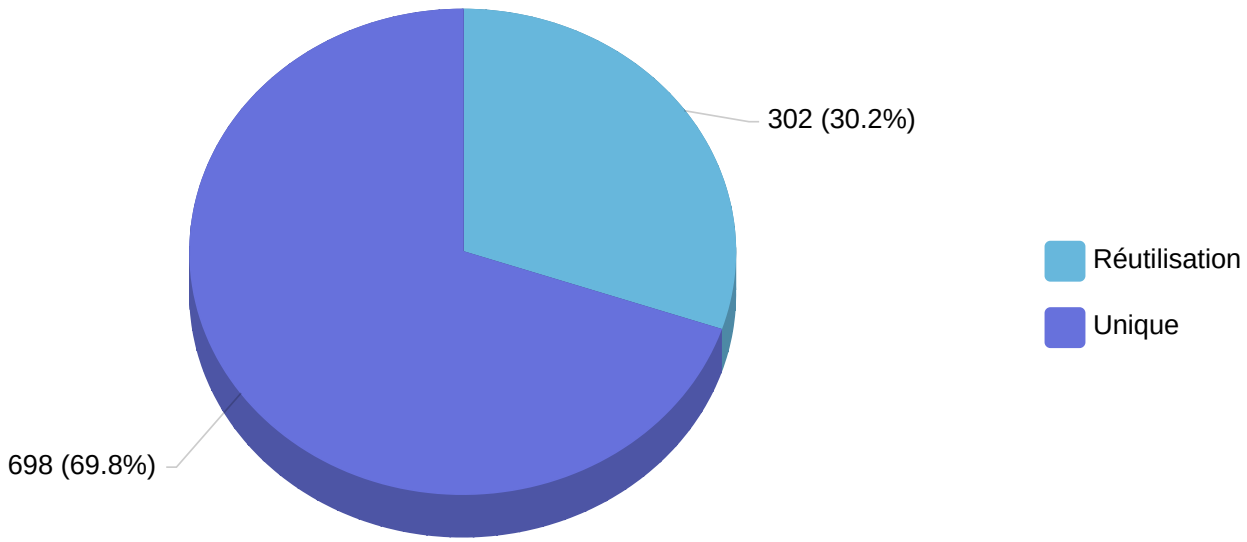
Ces mots de passe sont généralement faibles et largement répandus, ce qui en fait des cibles privilégiées pour les attaquants. L'analyse montre qu'une part importante des comptes compromis utilisaient des mots de passe fréquemment choisis par les utilisateurs.



Réutilisation des mots de passe

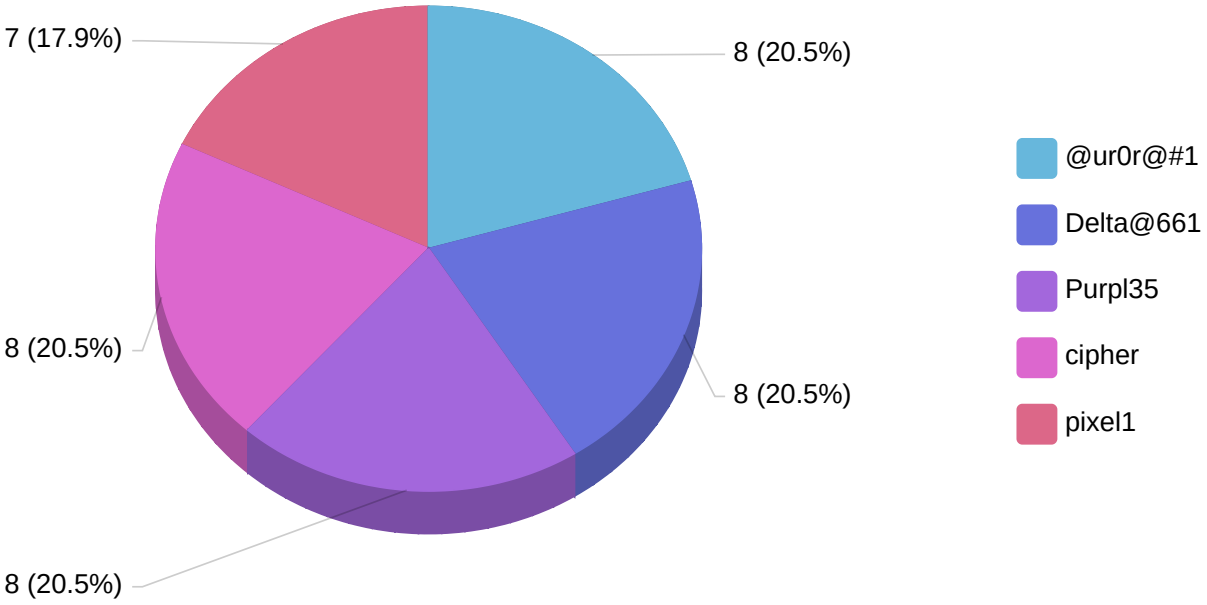
Le graphique ci-dessous met en évidence l'ampleur de la réutilisation des mots de passe parmi les comptes utilisateurs du jeu de données analysé (**la totalité des condensats de mot de passe**).

Les présents résultats montrent un taux de réutilisation de **30.2%** soit **302 comptes**. La réutilisation de mot de passe accroît considérablement la surface d'attaque. En cas de compromission d'un compte, tous les autres comptes utilisant ce même mot de passe deviennent vulnérables.



Mots de passe les plus réutilisé

Le graphique ci-dessous présente les mots de passe les plus réutilisés parmi ceux cassés. Les mots de passe **Delta@661** et **Purpl35** sont réutilisés respectivement dans **1.4%** et **1.4%** des mots cassés.



Motifs les plus utilisés

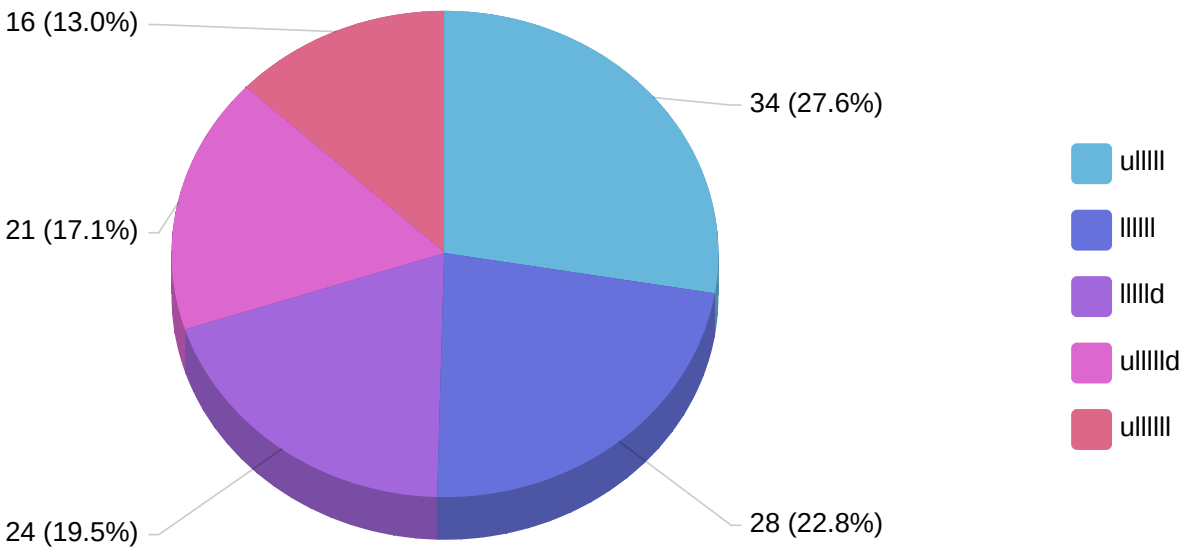
Le motif d'un mot de passe peut être analysé en observant la succession des types de caractères qu'il contient :

- **l** : lettre minuscule
- **u** : lettre majuscule
- **d** : chiffre
- **s** : caractère spécial

Voici quelques exemples de motifs souvent observés:

- **`ullllllldd`** : par exemple *Password21*, qui commence par une majuscule et termine par deux chiffres.
- **`ulllldddds`** : par exemple *Summer2018!*, Commençant par une majuscule et se terminant par quatre chiffres et un caractère spécial.

Cette analyse permet de mieux comprendre les habitudes de création de mots de passe et de cibler les combinaisons les plus prévisibles.



Remédiations

Afin de mettre en œuvre une politique de mots de passe forte, il est recommandé d'appliquer les remédiations suivantes :

- Utiliser des mots de passe uniques et complexes pour chaque compte ou service.
- Interdire l'utilisation de mots de passe courants ou en lien avec l'entreprise.
- Encourager l'utilisation de gestionnaires de mots de passe afin de générer et stocker des mots de passe forts.
- Utiliser des mots de passe d'au moins 12 caractères
- Combiner lettres majuscules, minuscules, chiffres et symboles spéciaux.
- Mettre en place une authentification multifacteur (MFA) pour les accès sensibles.
- Désactiver le stockage des condensats avec l'algorithme LAN Manager (LM).

Références

- [FR] ANSSI - Recommandations relatives à l'authentification multifacteur et aux mots de passe : https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
- [FR] ANSSI - Recommandations sur la sécurité relative à Active Directory : https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf
- [EN] OWASP - Recommandations de sécurité relatives aux mots de passe : https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Implement_Proper_Password_Strength_Controls
- [EN] Microsoft - Network security: Do not store LAN Manager hash value on next password change : https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password