Les gestionnaires de mots de passe

Partager, stocker vos mots de passe de façon sécurisé.

Présenté par Louis MEDO

Plan.

1. Qu'est-ce qu'un gestionnaire de mots de passe ?
2. Problématique résolu.
3. Pertinence de l’outil.
4. Bitwarden.
5. Passbotl.
6. KeepPass.
7. Matrice comparative.

Qu'est-ce qu'un gestionnaire de mots de passe ?

Un coffre-fort

Stocke tous vos identifiants dans une base de données chiffrée.

Un seul mot de passe

Retenez un seul mot de passe (appelé le mot de passe “maitre”).

Génération automatique

Génération de mots de passe complexes et robustes.

Problématique résolu.

Comment retenir des mots de passe complexe et différent sur plusieurs sites ?

- **Entropie** : nous utilisions des mots de passe faciles à retenir (azerty, 123456, Prenom2024).
- **Réutilisation** : nous utilisions le même mot de passe sur plusieurs services.
- **Mémoire** : difficile à retenir 50 mots de passe uniques.

Pertinence de l’outil.

SISR

Les fonctions :

- Gestion des comptes à privilèges.
- Gestion des clés SSH.
- Partage sécurisé en équipe.

SLAM

Les fonctions :

- Gestion des secrets (API & Tokens)
- Injections des secrets dans des piplines CI/CD[1]

Cas concret :

Vous êtes en AP et votre camarade n’est pas là, vous aurez quand même accès aux mots de passe de vos projets.

[1] : processus informatique de mise en production.

Bitwarden.

bitwarden

Authentification forte

- 2FA et MFA
  - TOTP
  - YubiKey
- Alertes de sécurité (mot de passes faibles ou réutilisés)

Partage sécurisé entre collaborateur

- Gestion des droits :
  - Lecture seule
  - Modification
  - Partage
- Possibilité d'envoyé des messages éphémères.

Auto hébergement

- Installation sur serveur Linux.
- Installation sur Docker.
- Contrôle total sur vos données.

Fonctions avancées

- Interface web.
- Extensions navigateur (Firefox, Chrome...).
- API pour les pipelines CI/CD.

https://bitwarden.com

Passbotl.

passbolt

Gestion des mots de passe

- Organisation par dossiers.
- Notes sécurisées.
- Stockage chiffrés avec GPG/ openPGP.

Partage sécurisé entre collaborateur

- Gestion des droits :
  - Lecture seule
  - Modification
  - Partage

Auto hébergement

- Installation sur serveur Linux
- Contrôle total sur vos données.

Fonctions avancées

- Interface web.
- Extensions navigateur (Firefox, Chrome...).
- API pour les pipelines CI/CD.

https://www.passbolt.com

KeepPass.

Serverless
Sans serveur.

- Base de données sous forme de fichier unique.
- Pas de données hébergées sur des serveurs.

Logiciel de type portable.

- Fonctionne sans aucune installation.
- Peut être utilisé depuis une clé USB.

Modularité
Plugins.

- Ajout de plugins possible.
  - SSH Agent
  - Générateur OTP
  - Synchronisation cloud

https://keepass.info

Matrice comparative.

Critères	Bitwarden	Passbolt	KeePass
Architecture	Auto-hébergement (Docker/Linux)	Auto-hébergement (Linux)	Serverless (Fichier unique local)
Sécurité	2FA, MFA, Yubikey, Audit des mdp	Chiffrement GPG/OpenPGP	Stockage local (Pas de donnée sur serveur)
Collaboration	Partage sécurisé, Droits (Lecture/Modif)	Partage sécurisé, Droits (Lecture/Modif)	Non natif (Utilisation monoposte via fichier)
Interfaces	Web, Extensions navigateur	Web, Extensions navigateur	Logiciel portable (USB), pas d'installation
Intégration Dev	API pour pipelines CI/CD	API pour pipelines CI/CD	Modularité via Plugins (SSH Agent, OTP)

Comment mettre la solution “Bitwarden” en place ?

Tutoriel de mise en place de la solution.

QR code vers le tutoriel pour mettre en place bitwarden en AP.

Ressources de la présentation.

QR code vers le dépôt github qui contient toutes les ressources de la présentation.