

CYBERYS

CYBERYS PROTECTYS · MANUEL

Configuration

Coffre · clés API · connecteurs · IA · consentement · sauvegardes

Version 2.0 · Novembre 2026 · Cyberys Protectys · Document de démonstration

1. Coffre et secrets

Le coffre est chiffré localement (AES-256-GCM). Les clés API ne doivent jamais être dans un fichier public ni dans un dépôt Git. Stockez-les dans le coffre ou dans `~/.cyberys/api_keys.txt` avec `chmod 600`.

Ne jamais coller une clé API dans un écran partagé, un ticket ou un journal.

2. Connecteurs

- **Threat Intelligence** : URL de base, en-tête et clé API dans le coffre.
- **DNS / certificats** : résolveurs et sources publiques.
- **IA** : Ollama local (souverain) ou OpenAI / Anthropic / compatible OpenAI.
- **Syslog** : collecteur UDP local 127.0.0.1:5514.

3. Consentement client

Chaque audit actif exige un mandat signé. Renseignez le client, le domaine, les dates et le périmètre, puis faites signer électroniquement. Le consentement est vérifié avant chaque lancement.

4. Réseau et sécurité

- Le serveur ne doit pas être exposé directement sur Internet.
- Reverse proxy TLS avec HSTS si accès distant.
- Filtrer les accès administratifs par IP ou VPN.
- Activer les sauvegardes et tester la restauration.

Checklist : coffre créé · 2FA · clés API · connecteurs testés · consentement · sauvegarde.