CYBERYS

CYBERYS ENTERPRISE

La configuration complète, prête pour votre DSI.

Un logiciel client qui s'installe sur **macOS**, se déploie sur **Windows ou Linux**, et s'ouvre aussi via une **URL locale**. Paiement unique par carte via Stripe, téléchargement immédiat, déploiement par votre DSI ou administrateur système.

1. Ce que vous installez

Cyberys Enterprise est un logiciel client local : application macOS native, ou serveur local (Windows/Linux) accessible par l'URL locale. Il embarque le moteur d'audit, l'interface web, le graphe réseau, le module de consentement client, les rapports PDF, la facturation, l'agent IA et les connecteurs (Threat Intelligence Cyberys, DNS, Shodan, Censys, HIBP).

- **Appliance** : Ubuntu 22.04/24.04 LTS minimal, service systemd, reverse proxy Caddy (TLS automatique).
- **Interface web** : accessible aux administrateurs et DSI via HTTPS.
- **Agent IA** : Ollama local (souverain) ou OpenAI / Anthropic / compatible OpenAI.
- **Données** : stockage local chiffré (coffre AES-256-GCM, clés API en 600).

2. Prérequis

Élément	Minimum	Recommandé
CPU	4 vCPU	8 vCPU
RAM	8 Go	16 Go (32 Go si LLM local)
Disque	100 Go SSD	250 Go SSD
OS serveur	Ubuntu 22.04 LTS	Ubuntu 24.04 LTS
Client	macOS 13+ / navigateur	App macOS / URL locale Windows-Linux
Réseau	1 IP publique, 80/443	+ enregistrement DNS dédié

DNS / TLS : crée un enregistrement `A` (ex. `cyberys.client.tld`) vers l'IP de l'appliance. Caddy obtient le certificat automatiquement.

Ports : 22 ou 4000 (administration), 80/443 (web). Le port interne 8766 n'est jamais exposé directement.

3. Installation

macOS : ouvrez `CYBERYS.app`. **Windows / Linux :** lancez le serveur local puis ouvrez `http://127.0.0.1:8766` dans le navigateur. Le serveur reste sur la machine ; aucune donnée d'audit n'est envoyée au cloud.

3.1 Paquets système

```
sudo apt update
sudo apt install -y python3 python3-venv python3-pip caddy \
  libpango-1.0-0 libpangoft2-1.0-0 libcairo2 libgdk-pixbuf-2.0-0 \
  libffi8 shared-mime-info fonts-dejavu-core
```

3.2 Compte et fichiers

```
sudo useradd -r -s /usr/sbin/nologin -d /var/lib/cyberys cyberys
sudo mkdir -p /opt/cyberys /var/lib/cyberys
# copier le bundle Cyberys dans /opt/cyberys
sudo cp -R /chemin/vers/CYBERYS/* /opt/cyberys/
sudo chown -R cyberys:cyberys /opt/cyberys /var/lib/cyberys
```

3.3 Environnement Python

```
cd /opt/cyberys
sudo -u cyberys python3 -m venv .venv
sudo -u cyberys .venv/bin/pip install --upgrade pip
sudo -u cyberys .venv/bin/pip install aiohttp cryptography certifi weasyprint
```

3.4 Service systemd

```
sudo tee /etc/systemd/system/cyberys.service >/dev/null <<'EOF'
[Unit]
Description=Cyberys Enterprise
After=network.target

[Service]
User=cyberys
WorkingDirectory=/opt/cyberys
Environment=HOME=/var/lib/cyberys
Environment=CYBERYS_NO_BROWSER=1
ExecStart=/opt/cyberys/.venv/bin/python /opt/cyberys/cyberys_server.py
Restart=always
RestartSec=5

[Install]
WantedBy=multi-user.target
EOF
sudo systemctl daemon-reload
sudo systemctl enable --now cyberys
sudo systemctl status cyberys --no-pager
```

3.5 Reverse proxy TLS (Caddy)

```
sudo tee /etc/caddy/Caddyfile >/dev/null <<'EOF'
cyberys.client.tld {
  encode gzip
  reverse_proxy 127.0.0.1:8766
}
EOF
sudo systemctl reload caddy
```

> **Important :** ne jamais exposer 8766 sur Internet. Caddy assure HTTPS, HSTS et le reverse proxy. Les terminaux intégrés (workspace) restent locaux à l'appliance ; les administrateurs distants utilisent l'interface web, le graphe, l'IA et les rapports.

4. Première configuration

1. Ouvre `https://cyberys.client.tld`.
2. Crée le **mot de passe maître** (PBKDF2 10 M itérations, coffre AES-256-GCM).
3. Renseigne la société dans **Facturation** (SIRET, TVA, IBAN, mentions légales).
4. Ajoute les cibles dans `scripts/pentest_targets.conf` ou via l'interface.
5. Configure les **clients, mandats et consentements** avant tout audit.

5. Comptes et rôles

Version 1 : l'appliance est livrée en **mode opérateur unique** (mot de passe maître + 2FA Cyberys pour le compte lié). Le module **multi-utilisateurs / RBAC** (SuperAdmin, RSSI, Auditeur, Lecteur, Client) et SSO/LDAP est planifié en phase 2.

Recommandation : un accès nominatif par administrateur, MFA sur le VPN/SSO, et journalisation des connexions.

6. Agent IA

Dans **Assistant IA**, choisis un fournisseur :

- **Ollama local** (souverain, recommandé) : installe Ollama, puis `ollama pull llama3.1`, base URL `http://127.0.0.1:11434`.
- **OpenAI / Anthropic / compatible** : renseigne la clé API et le modèle.

Garde-fous : l'IA conseille, elle n'exécute pas d'action. Les données d'audit peuvent être envoyées au fournisseur choisi : utilise Ollama local pour garantir la souveraineté. Une validation humaine est requise avant toute remédiation.

7. Connecteurs

Connecteur	Usage	Configuration
Threat Intelligence Cyberys	Surface, dark web, typosquatting, exposition	Clé API dans le panneau Renseignement
DNS / Certificate Transparency	Reconnaissance, sous-domaines, certificats	Natif
Shodan / Censys	Services exposés, bannières	Clé API (optionnel)
Have I Been Pwned	Fuites d'emails	Clé API (optionnel)

8. Sécurité et conformité

- HTTPS obligatoire, HSTS, cookies HttpOnly/SameSite.
- Pare-feu : n'autoriser que 22/4000 (admin) et 80/443 (web).
- fail2ban sur SSH et reverse proxy.
- Secrets hors du code, fichiers `chmod 600`.
- Consentement client signé avant tout audit ; tests non destructifs et plafonnés.
- Journal d'audit : qui, quoi, quand, cible, résultat.
- RGPD : minimisation, durée de conservation, droit à l'effacement.

9. Sauvegarde et restauration

```
# sauvegarde (à planifier quotidiennement)
sudo tar -czf /backup/cyberys-$(date +%F).tgz /opt/cyberys /var/lib/cyberys

# restauration testée
sudo systemctl stop cyberys
sudo tar -xzf /backup/cyberys-2026-11-05.tgz -C /
sudo systemctl start cyberys
```

Conserver au moins 3 copies (locale, disque externe, hors site) et tester la restauration trimestriellement.

10. Check-list de mise en service

Contrôle	Attendu
Service actif	`systemctl is-active cyberys` → active
HTTPS	`curl -I https://cyberys.client.tld` → 200
Coffre	Mot de passe maître créé, connexion OK
IA	Test de connexion OK (Ollama ou cloud)
Connecteur Threat Intelligence Cyberys	Recherche d'un domaine → organisation/entités
Client + mandat	Consentement signé et importé
Audit	Un audit complet génère un rapport PDF
Sauvegarde	Archive créée et restauration testée

11. Support

Pour toute installation ou vérification : contact@cyberys.fr.

© 2026 Cyberys. Tous droits réservés. Document confidentiel — à remettre au client pour l'installation de son appliance. Mentions légales.