CYBERYS PROTECTYS · MANUEL

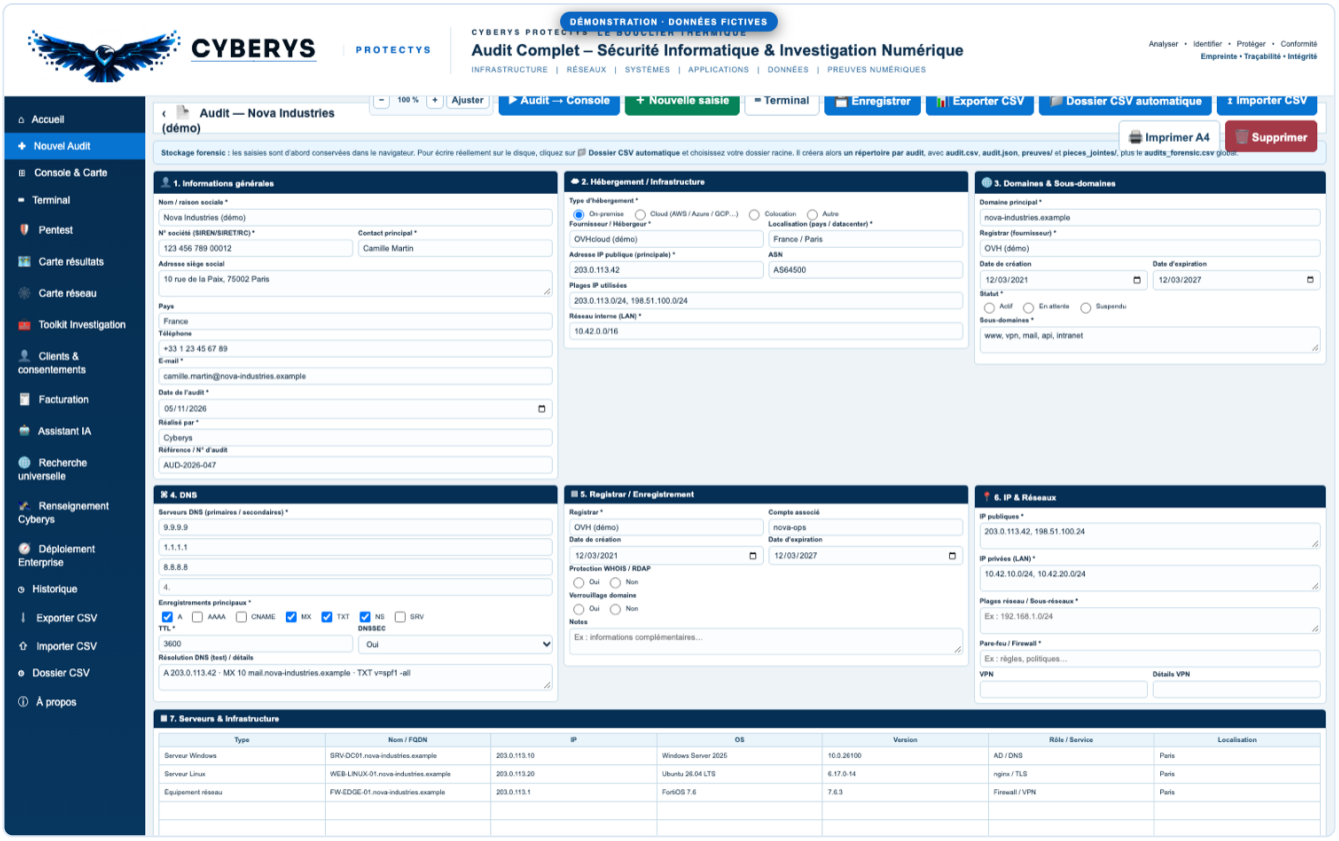
Installation complète

macOS · Windows · Linux · premier lancement · sécurisation

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

1. Ce que vous installez

Cyberys Enterprise est un logiciel client local : application macOS native, ou serveur local Windows/Linux accessible par `http://127.0.0.1:8766`. Le serveur reste sur votre machine ; les données d'audit ne sont pas envoyées au cloud.



2. Prérequis

Élément	Minimum	Recommandé
CPU	4 vCPU	8 vCPU
RAM	8 Go	16 Go
Disque	100 Go SSD	250 Go SSD
OS serveur	Ubuntu 24.04 LTS	Ubuntu 26.04 LTS
Client	macOS 15+ / navigateur	macOS 26 Tahoe / Windows-Linux

> **Ne jamais exposer 8766 sur Internet.** Le port local doit rester sur 127.0.0.1 ; l'accès distant passe par un reverse proxy TLS et une authentification.

3. macOS

1. Dézipper le pack Enterprise.
2. Ouvrir `CYBERYS.app`.
3. Si Gatekeeper bloque : clic droit → Ouvrir, ou Réglages Système → Confidentialité et sécurité → Ouvrir quand même.
4. Créer le coffre et le mot de passe maître au premier lancement.
5. Vérifier que le serveur local répond sur `http://127.0.0.1:8766`.

4. Windows / Linux

```
cd /opt/cyberys
python3 -m venv .venv
```

```
.venv/bin/pip install --upgrade pip
.venv/bin/pip install aiohttp cryptography certifi weasyprint
.venv/bin/python cyberys_server.py
```

Ouvrir ensuite `http://127.0.0.1:8766` dans le navigateur local.

Service systemd (Linux)

```
[Unit]
Description=Cyberys Enterprise
After=network.target

[Service]
User=cyberys
WorkingDirectory=/opt/cyberys
Environment=HOME=/var/lib/cyberys
Environment=CYBERYS_NO_BROWSER=1
Environment=CYBERYS_SYSLOG_HOST=127.0.0.1
Environment=CYBERYS_SYSLOG_PORT=5514
ExecStart=/opt/cyberys/.venv/bin/python /opt/cyberys/cyberys_server.py
Restart=always

[Install]
WantedBy=multi-user.target
```

```
sudo systemctl daemon-reload
sudo systemctl enable --now cyberys
```

5. Premier lancement

1. Créer le mot de passe maître (coffre AES-256-GCM).
2. Activer la 2FA si disponible.
3. Configurer les clés API dans le coffre (Threat Intelligence, IA, etc.).
4. Vérifier les connecteurs DNS, certificats, Threat Intelligence.
5. Tester un audit sur une cible de démonstration autorisée.

6. Sécurité avant mise en production

- 8766 et 8767 liés à 127.0.0.1 uniquement.
- Reverse proxy TLS (Caddy/nginx) si accès distant.
- Pare-feu : n'ouvrir que 443 et l'administration nécessaire.
- Comptes nominatifs, moindre privilège, 2FA.
- Sauvegardes chiffrées et test de restauration.
- Journalisation et supervision des accès.

> **Prêt.** La configuration est terminée ; passez aux manuels Configuration, Audit & Terminal, Cartographie & Syslog, Rapports.