

# CYBERYS

PROTECTYS · CYBERSECURITY PLATFORM

**Penser attaque. Raisonner défense.**

**P R O T E C T Y S**

**Le bouclier thermique de votre infrastructure.**

Cyberys audite. Protectys protège.

CYBERYS est une technologie locale-first, interopérable par conception.

Protectys V1.0 · document produit · 5 novembre 2026 · PME · TPE · Hôpitaux · Collectivités

# Plateforme d'audit et de supervision sécurité, locale

Cyberys **audite, cartographie, corrèle, prouve et transmet**. Données chez le client, interopérable, fonctionne en réseau fermé.

## Audit & investigation

- **Audit externe** : OSINT, DNS, sous-domaines, certificats, ports, services, TLS, corrélation CVE.
- **Pentest contrôlé** : Black Box / Grey Box / White Box, mandat signé, kill-switch, journal horodaté.
- **Preuves & rapports** : findings qualifiés, horodatés, PDF avec remédiation et check-list.
- **Surveillance planifiée** : chaque lundi, chaque jour ou à la demande, mandat vérifié.

## Réseau & journaux

- **Cartographie** : hôtes, IP, services, flux, empreinte instantanée.
- **Syslog** : UDP, WARNING/ERR/DENY, connexions et volumes, replay, comparaison passé/présent.
- **Graphe d'investigation** : entités, relations, CVE, IOC, preuves, identités.

## Exploitation

- **Terminal intégré** : vrai shell local (zsh/bash/cmd), 1 à 4 terminaux.
- **Clients, mandats, consentements** signés ; facturation et licence.
- **IA locale** (Ollama) ou cloud : priorise les correctifs, sans exécuter d'action.
- **Import scanners** : Nessus, OpenVAS, Qualys. **Exports** : JSON, STIX 2.1, CEF, LEEF.
- **Démo complète** : 3 clients, 3 audits, 115 machines Syslog (IP/MAC/rôles).
- **Multi-OS** : app macOS native ; serveur Windows/Linux + navigateur.

## Sécurité

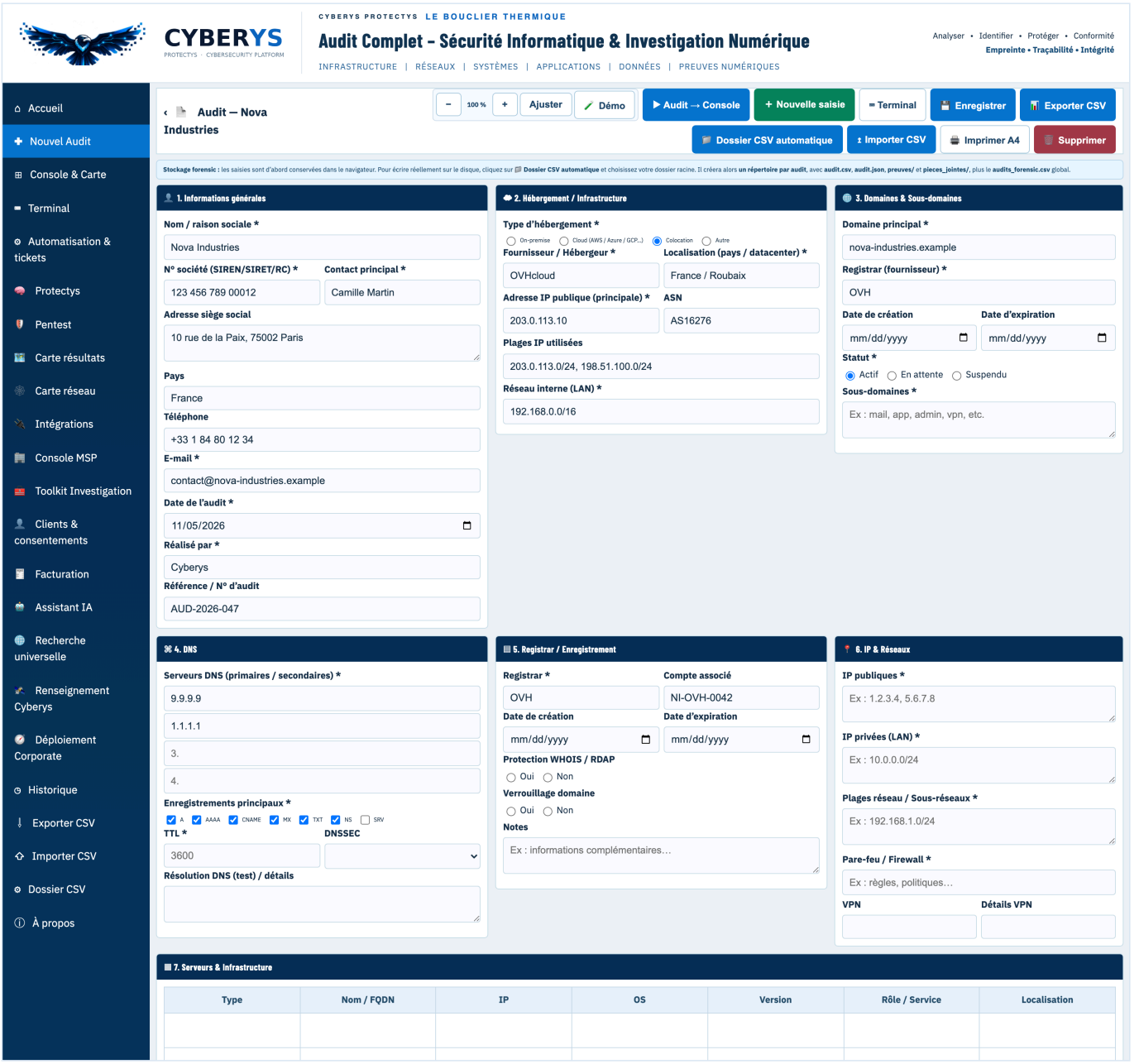
- Coffre **AES-256-GCM**, mot de passe maître PBKDF2-SHA256, clés API en 600.
- Session effacée à chaque lancement ; login obligatoire.
- Consentement signé avant tout test, tests non destructifs, kill-switch.
- Journal d'audit horodaté (qui, quoi, quand, cible, résultat).

## OSINT & investigation

Toolkit Investigation : 435 outils Bellingcat intégrés, 15 catégories · images, réseaux sociaux, personnes, cartes & satellites, transport, DNS/IP, finance, archivage.

- Images : FotoForensics, InVID-WeVerify, ExifPurge, Google Lens, Amazon Rekognition.
- Réseaux & personnes : Amnesty YouTube Dataviewer, Bellingcat TikTok, Botometer, Epieos, Have I Been Pwned.
- Cartes, transport & web : Google Earth Pro, Copernicus, Sentinel Hub, Flightradar24, ADS-B Exchange, Shodan.

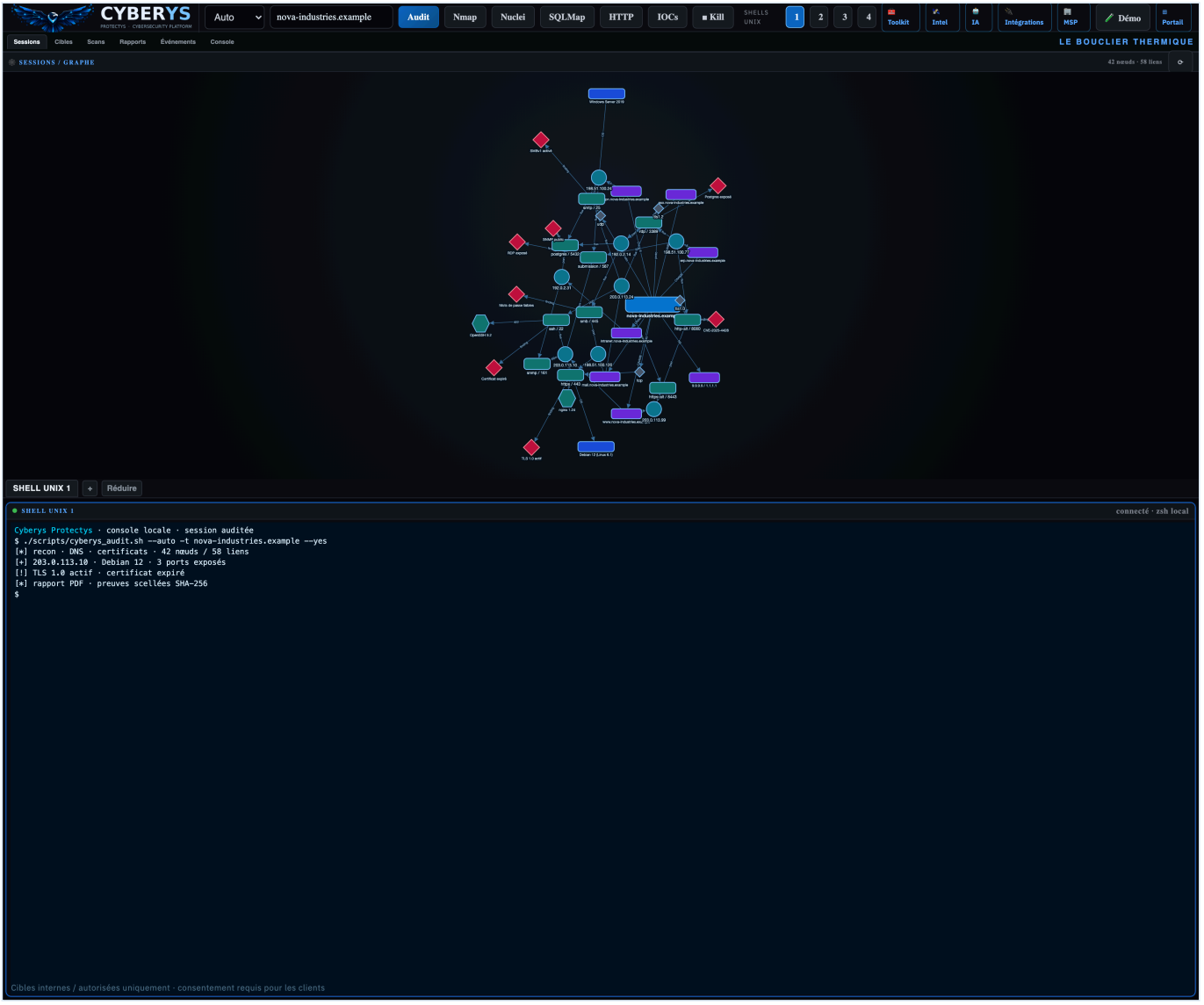
# Audit · formulaire complet (cible, infrastructure, DNS, preuves)




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- Saisie client complète : société, contact, adresse, IP, plages IP, DNS, registrar.
- Champs cible / hébergement / domaines / preuves, export CSV et impression A4.
- Navigation 13 modules : Audit, Console, Pentest, Cartes, Intégrations, MSP, IA.

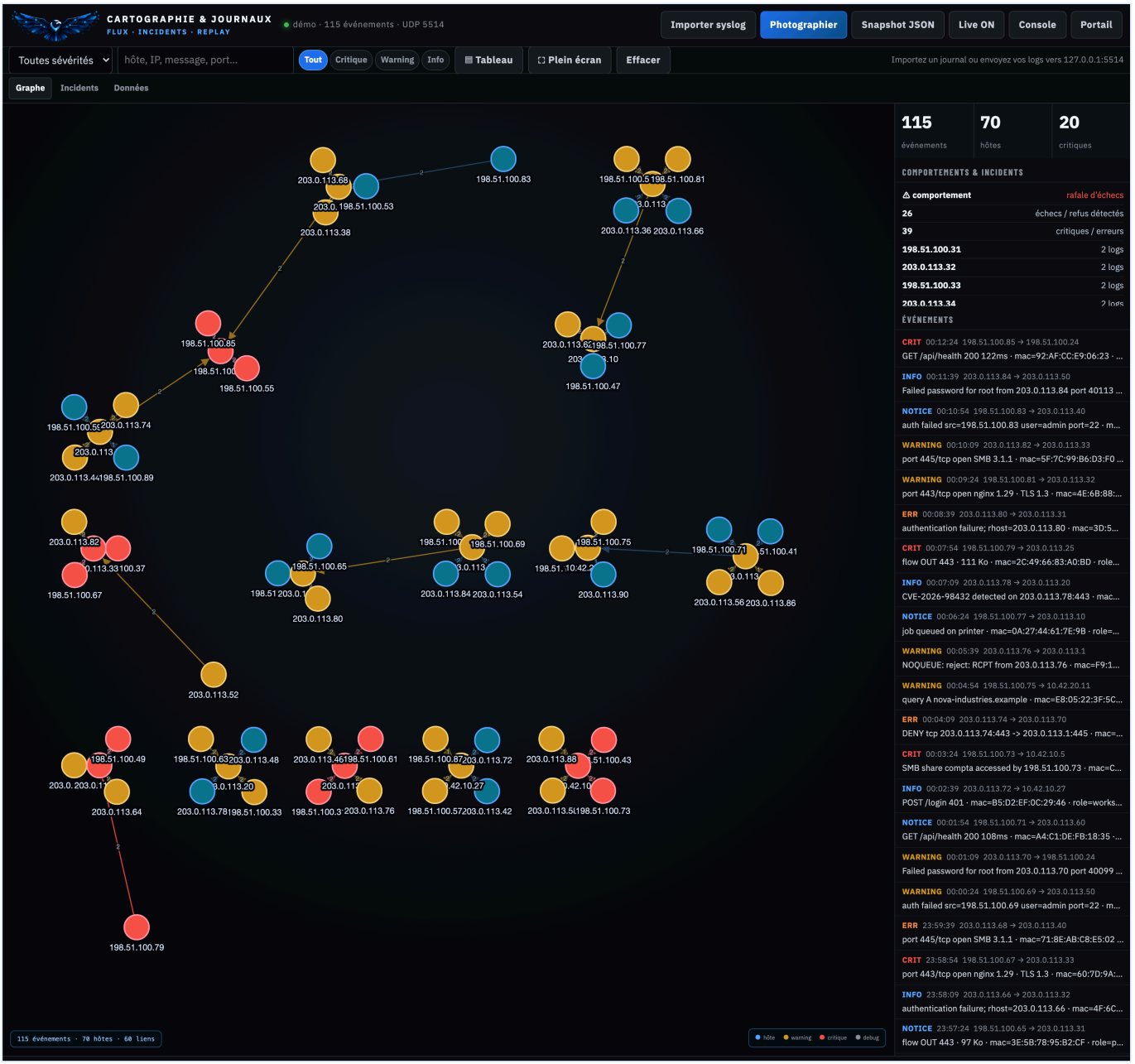
# Console · graphe d'investigation, cibles et terminaux




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- Graphe 42 n·uds / 58 liens issu des 3 audits de démonstration.
- Onglets Sessions, Cibles, Scans, Rapports, Événements, Console.
- Terminaux locaux 1 à 4 et cible active nova-industries.example.

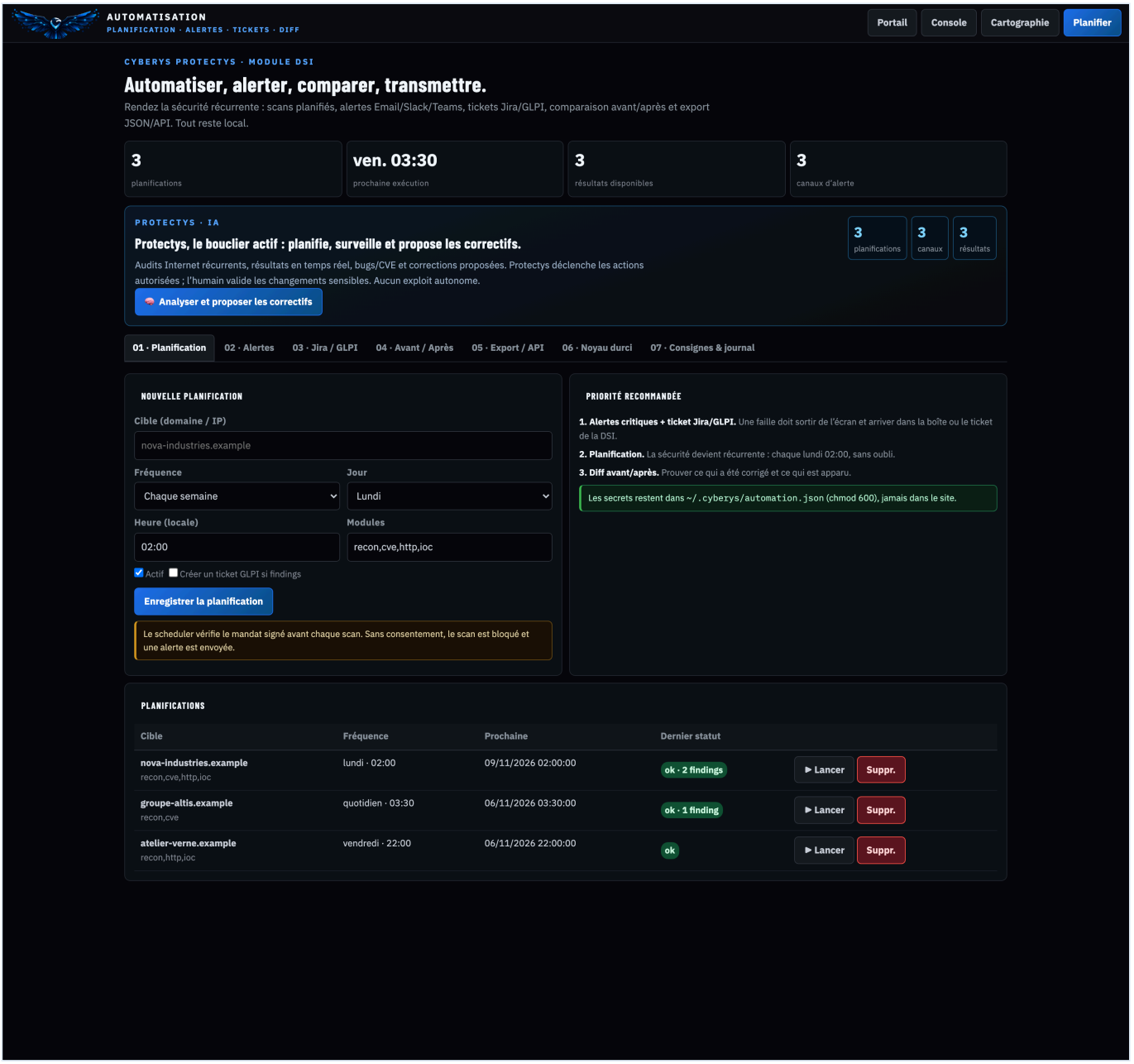
# Cartographie & journaux · 115 événements, 70 hôtes, IP/MAC/rôles




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- 115 événements, 70 hôtes, 60 liens, 20 critiques.
- IP et MAC affichées avec le rôle : firewall, DC, web, mail, imprimantes, NAS, ERP, VPN, SQL, DNS, bastion, caméra.
- Filtres sévérité, tableau, plein écran, replay et export JSON.

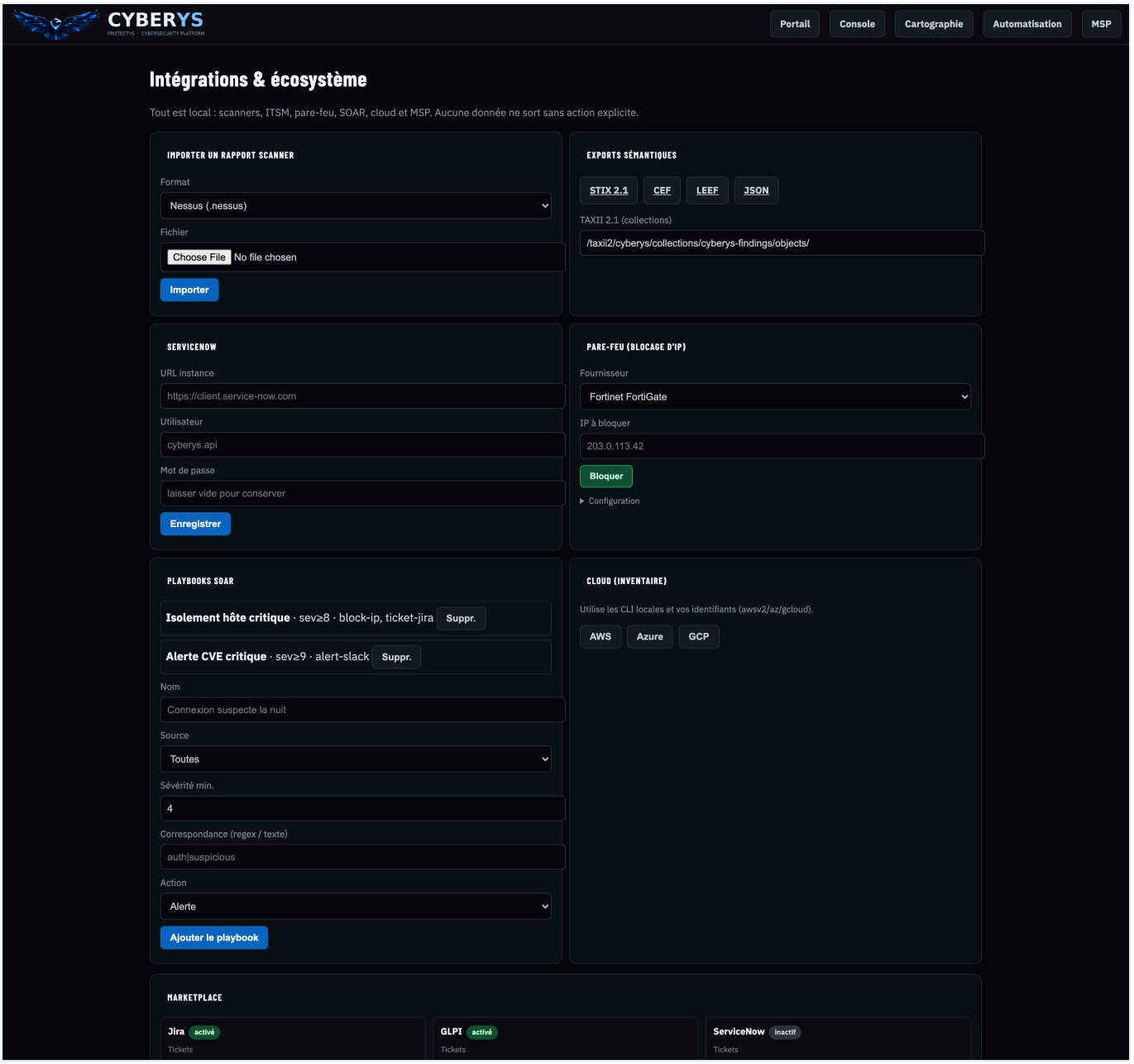
# Automatisation · planifications, alertes, tickets, diff




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- 3 planifications : lundi 02:00, chaque jour 03:30, vendredi 22:00.
- Alertes Email / Slack / Teams et tickets Jira / GLPI / ServiceNow.
- Diff avant/après, export JSON/API et consignes administrateur.

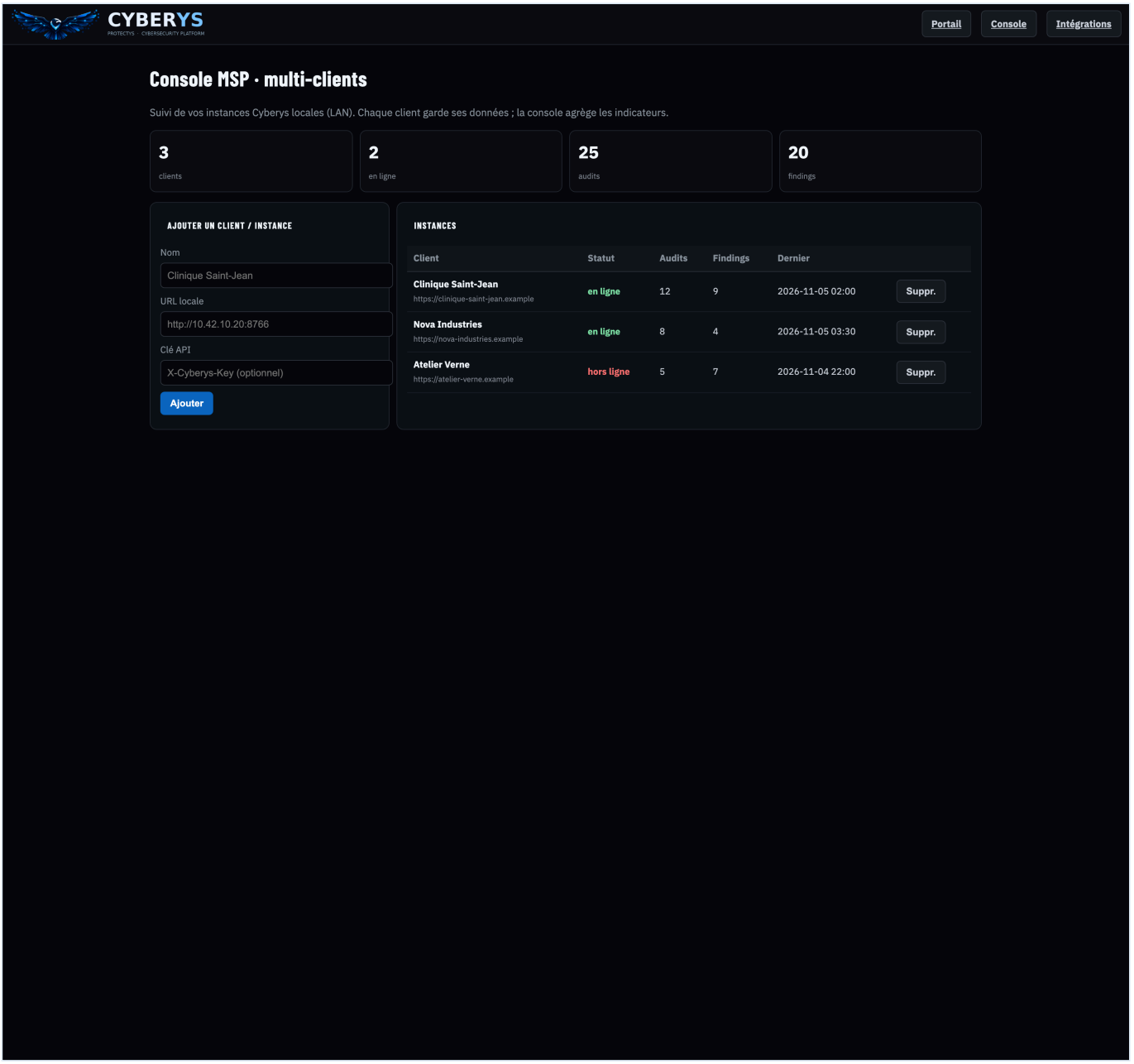
# Intégrations · scanners, ITSM, pare-feu, SOAR, cloud




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- Import Nessus / OpenVAS / Qualys et exports STIX / CEF / LEEF.
- Pare-feu Fortinet / Cisco et playbooks SOAR.
- Marketplace : Jira, GLPI, ServiceNow, Slack, Teams, Zabbix, n8n, cloud, scanners.

# Console MSP · suivi multi-clients




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- 3 clients suivis : Clinique Saint-Jean, Nova Industries, Atelier Verne.
- Statut en ligne/hors ligne, audits, findings, dernier passage.
- Ajout d·une instance locale (URL + clé API), aucune donnée centralisée.

# Accès sécurisé · login local, coffre AES-256-GCM




Démonstration intégrée · données fictives (RFC 5737) · Cyberys Protectys V1.0.

- Login + mot de passe maître, coffre AES-256-GCM, PBKDF2-SHA256.
- Compatible Windows, macOS, Linux, Unix, Chrome, Edge.
- Session effacée à chaque lancement de l·application.

# Lire, exporter et piloter

**Cyberys est une technologie locale-first, interopérable par conception.** API REST JSON, clé API, exports standards et webhooks internes.

| Endpoint | Usage | Statut |
|---|---|---|
| `GET /api/results` · `/graph` · `/targets` · `/logs` | Lecture | Disponible |
| `GET /api/export.json` · `/stix` · `/cef` · `/leef` | Exports sémantiques | Disponible |
| `GET /taxii2/…` | Serveur TAXII 2.1 (clé API) | Disponible |
| `POST /api/scan` | Lancer un audit à distance | Disponible |
| `POST /api/import` | Nessus / OpenVAS / Qualys | Disponible |
| `POST /api/firewall/block` | Fortinet / Cisco | Disponible |
| `POST /api/cloud/scan` | AWS / Azure / GCP (CLI locale) | Disponible |
| `POST /api/itsm/zabbix` | Trigger Zabbix + playbooks | Disponible |
| `GET/POST /api/msp/*` | Console multi-clients | Disponible |

## Alertes & ITSM

Email · Slack · Teams · Zabbix (sortant) · Jira · GLPI · ServiceNow. Playbooks SOAR : **SI** source/sévérité/regex **ALORS** alerte, ticket ou blocage IP.

## Exemple d'appel (local)

```
curl -H "X-Cyberys-Key: <clé>" -H "Content-Type: application/json" -d '{"domain":"nova-industries.example"}' http://127.0.0.1:8766/api/scan
```

La clé se récupère dans /api/apikey (session authentifiée). Toutes les réponses sont en JSON, aucune sortie Internet.

## Sécurité API

- Session HttpOnly / SameSite ; clé API locale stockée en 600.
- Webhook ITSM : jeton partagé et/ou accès loopback uniquement.
- Chaque appel est journalisé (journal d'audit local).

## Webhooks sortants

| Canal | Format |
|---|---|
| Slack / Teams | JSON texte |
| Zabbix | JSON (source, sujet, sévérité) |
| Jira / GLPI / ServiceNow | Tickets natifs |

# Technologie locale-first, interopérable par conception

Import scanners, ITSM, pare-feu, SOAR, MSP et cloud — sans dépendance au cloud.

| Intégration | Détail | Statut |
|---|---|---|
| Nessus · OpenVAS · Qualys | Import XML/JSON | Disponible |
| ServiceNow · Jira · GLPI | Tickets | Disponible |
| TAXII 2.1 · STIX · CEF · LEEF | Partage sémantique | Disponible |
| Fortinet · Cisco | Blocage d'IP | Disponible |
| Playbooks SOAR | SI... ALORS... | Disponible |
| Console MSP | Multi-clients (LAN) | Disponible |
| AWS · Azure · GCP | Inventaire via CLI | Disponible |
| Nmap · Nuclei · OpenSSL | Modules natifs | Disponible |

## Modèle

Cyberys reste le cœur local : entrées (webhooks, imports, scanners), sorties (alertes, tickets, exports standards). Aucune centralisation sans action explicite.

## Marketplace

Catalogue local : activez Jira, GLPI, ServiceNow, Slack, Teams, Zabbix, n8n, AWS, Azure, GCP, Nessus, OpenVAS, Qualys, Fortinet, Cisco. Les connecteurs restent sur l'appliance ; aucun téléchargement externe requis.

## Prérequis par connecteur

| Connecteur | Prérequis |
|---|---|
| ServiceNow | URL instance, compte API, mot de passe |
| Fortinet | URL FortiGate, token API |
| Cisco | URL RESTCONF, compte, mot de passe |
| AWS / Azure / GCP | CLI installée et identifiants locaux |
| MSP | URL + clé API de chaque instance Cyberys |

# Conçu pour fonctionner sans Internet

- App macOS native, serveur Windows/Linux, interface locale (127.0.0.1 / LAN).
- Coffre AES-256-GCM, clés API en 600, consentements et journaux locaux.
- Audit réseau, cartographie, Syslog UDP, replay, graphe, rapports PDF.
- Polices, Leaflet, Cytoscape, xterm, démo **hébergés localement**.
- API REST, STIX/CEF/LEEF, TAXII, clé API : tout reste sur le réseau.

## Optionnel

Flux CVE publics, Threat Intelligence, IA cloud, tuiles de carte, CLI cloud.

**Bonnes pratiques :** Ollama local pour l'IA ; Jira/GLPI/ServiceNow/Zabbix sur le LAN ; miroir CVE interne ; sauvegardes chiffrées hors ligne. Si Internet est absent, les fonctions externes sont ignorées ; le cœur d'audit reste opérationnel.

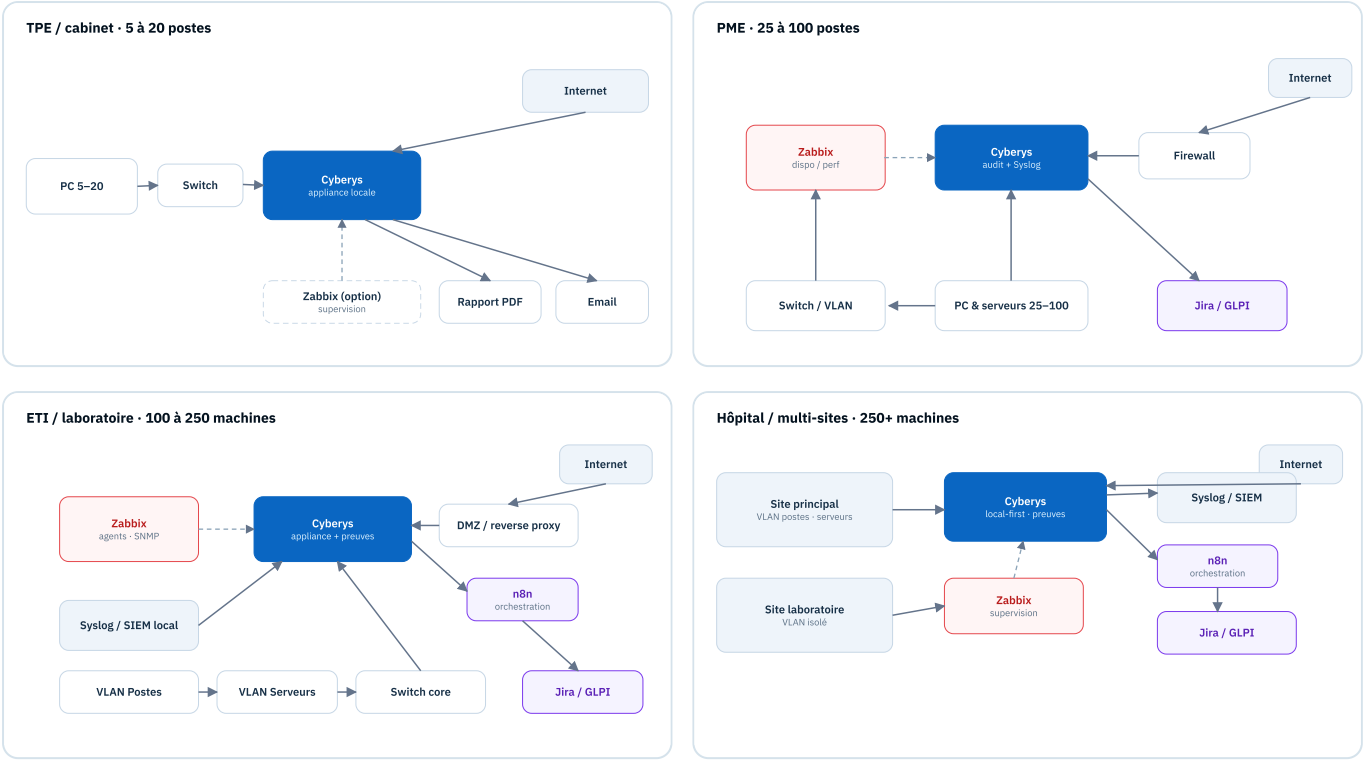
## Matrice rapide

| Besoin | Hors Internet | Internet optionnel |
|---|---|---|
| Audit, cartographie, Syslog, rapports | Oui | — |
| ITSM / tickets (Jira, GLPI, ServiceNow) | Oui (LAN) | — |
| Threat Intelligence, CVE publics | Non | Oui |
| IA | Ollama local | Cloud |
| Cloud AWS/Azure/GCP | Non | CLI + identifiants |

## Sauvegarde & continuité

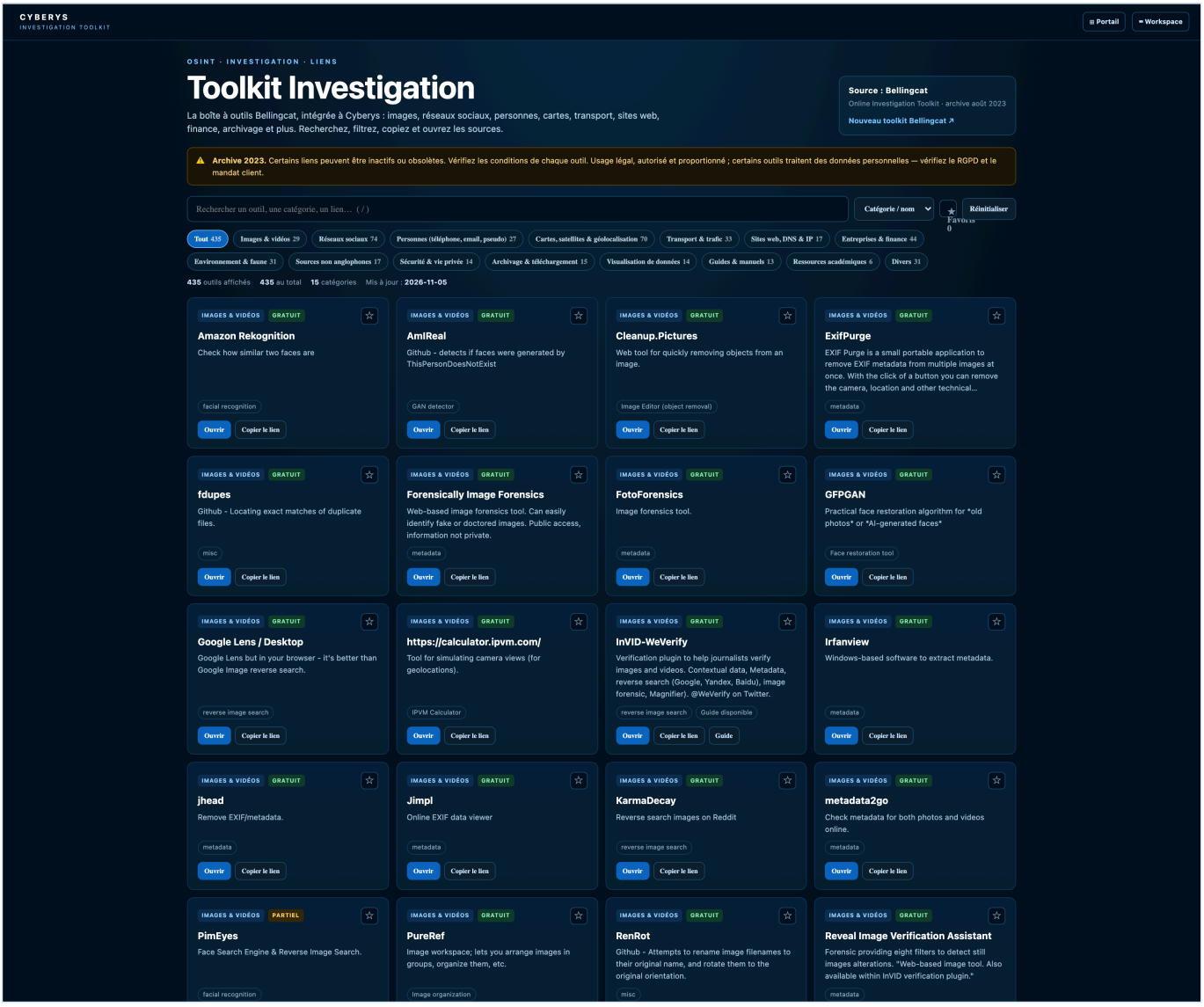
**Sauvegarde chiffrée** de /opt/cyberys et du coffre, hors ligne, testée trimestriellement.
**Mise à jour** par remplacement du pack, sans Internet obligatoire.
**Support** : contact@cyberys.fr · dpo@packdata.io

# Du cabinet de 5 postes à l'hôpital multi-sites




TPE 5–20 · PME 25–100 · ETI/laboratoire 100–250 · Hôpital 250+. Zabbix, Jira/GLPI, n8n, VLAN, DMZ.

# Toolkit Investigation · 435 outils OSINT intégrés




Source : Bellingcat (archive août 2023) · usage légal, autorisé et proportionné · données publiques.

- 435 outils, 15 catégories : images & vidéos, réseaux sociaux, personnes, cartes & satellites, transport, DNS/IP, finance, archivage.
- Images & vidéos : FotoForensics, InVID-WeVerify, ExifPurge, Google Lens, Amazon Rekognition, GFPGAN.
- Réseaux sociaux & personnes : Amnesty YouTube Dataviewer, Bellingcat TikTok, Botometer, Epieos, Have I Been Pwned, Blackbird.
- Cartes & transport : Google Earth Pro, Copernicus, Sentinel Hub, Flightradar24, ADS-B Exchange, MarineTraffic, Global Fishing Watch.
- Web, DNS & finance : Shodan, Passive DNS, DNS History, SpyOnWeb, Companies House, OpenCorporates, Etherscan.

# Une démo complète, sans rien installer

- **3 clients** : Nova Industries, Groupe Altis, Atelier Verne.
- **3 audits** complets avec findings, ports, OS, statut.
- **115 événements Syslog** · 70 hôtes · 60 liens · IP/MAC/rôles (firewall, DC, web, mail, imprimantes, NAS, ERP, VPN, SQL, DNS, bastion, caméra).
- **3 mandats** signés, 3 planifications, exports STIX/CEF/LEEF.

## Contact

contact@cyberys.fr · dpo@packdata.io
PACKDATA LTD · 71-75 Shelton Street, Covent Garden, London WC2H 9JQ

Document confidentiel — à remettre au client. Les données des captures sont fictives (RFC 5737).

## Lancer la démo

1. Ouvrir l'application et se connecter (login + mot de passe maître).
2. La démo est active par défaut quand aucun audit réel n'existe.
3. Bouton 🧪 **Démo** dans le workspace pour basculer démo/réel.
4. Parcourir Audit, Console, Cartographie, Automatisation, Intégrations, MSP.