CYBERYS PROTECTYS · MANUEL

Audit & Terminal

Cibles · consentement · modules · terminaux internes · preuves

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

1. Cible universelle

Domaine, URL, IP, email, pseudonyme, réseau social, téléphone, hash/IOC. Sources : Internet temps réel, base locale, serveur Cyberys ou chemin local autorisé.

2. Garde-fous

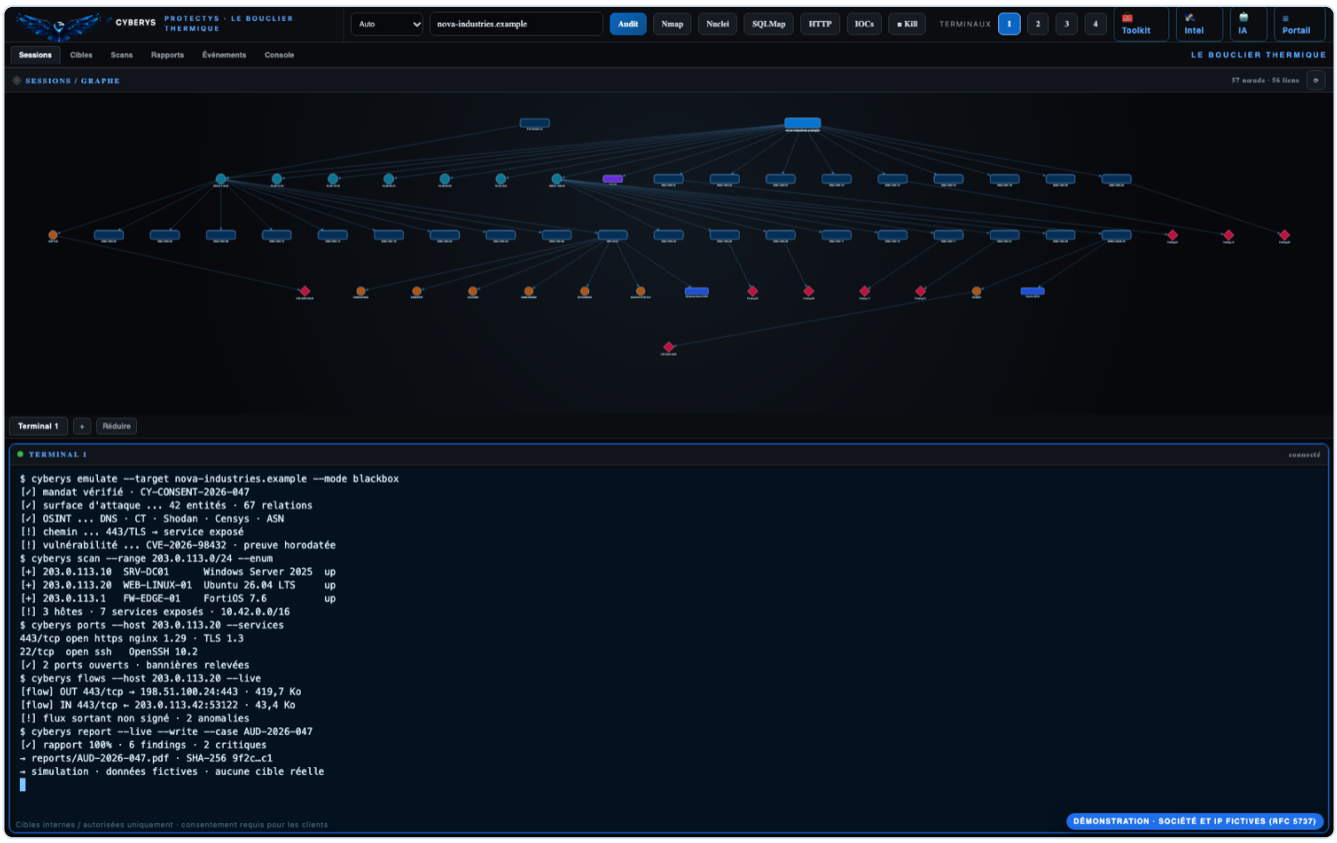
- Mandat signé obligatoire pour tout scan actif.
- Validation de la cible et filtrage des métacaractères.
- Kill-switch sur tous les terminaux.
- Journal horodaté et export d'évidence JSON avec SHA-256.

3. Modules

- AD, Cloud, Kubernetes, certificats, DNS, SMB, flux, CVE, fuites.
- Nmap, Nuclei, testssl, ZAP : orchestration dans le terminal.
- Chaque module produit une ligne de résultat et une preuve.

4. Terminaux

1 à 4 terminaux internes en onglets, réductibles. Tout reste dans la fenêtre Cyberys. Les volumes de flux sont affichés de l'octet au pétaoctet.



5. Rapport et preuves

Les findings sont triés et qualifiés avant publication : faux positifs écartés ou documentés, preuve, contexte, remédiation. Le rapport PDF est prêt pour la revue.