CYBERYS PROTECTYS · MANUEL

Cartographie & Syslog

Importer · live UDP · photographie · incidents · replay

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

1. Importer un journal

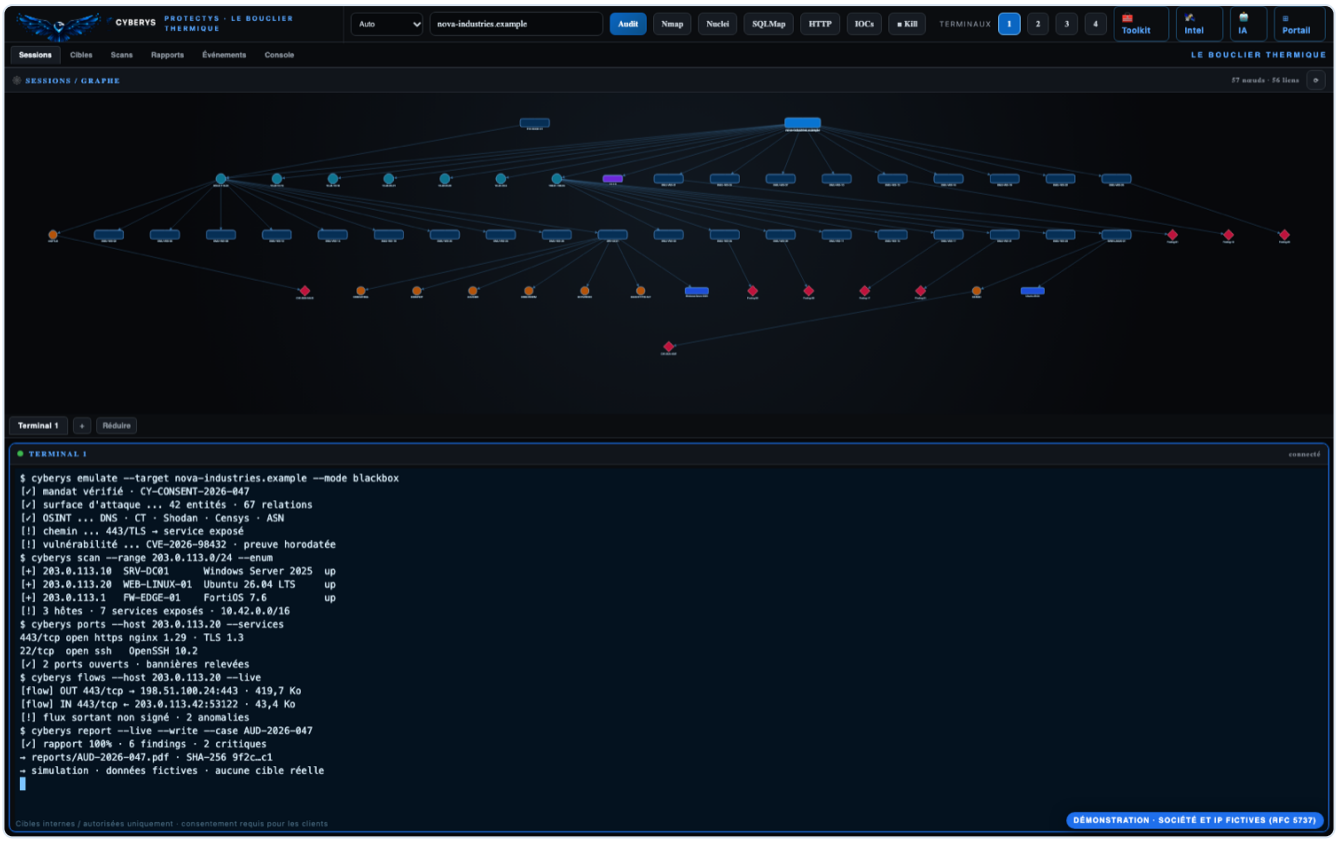
Ouvrir `/netmap` puis « Importer syslog ». Formats acceptés : `.log`, `.txt`, `.json` (snapshot).

```
logger -n 127.0.0.1 -P 5514 "auth failed src=203.0.113.42 user=admin"
```

Le collecteur écoute en UDP sur `127.0.0.1:5514` et écrit dans `~/CyberysLogs/syslog.jsonl`.

2. Lire la carte

Chaque hôte et IP devient un nœud ; les échanges de logs deviennent des liens. La sévérité colore les nœuds et les liens : critique rouge, warning orange, info bleu.



3. Comportements et incidents

- Détection des rafales d'échecs / refus.
- Top sources, top destinations, ports observés.
- Événements critiques et erreurs.
- Clic sur un événement : focus sur l'hôte dans la carte.

4. Replay temporel

Le curseur temporel permet de revoir l'incident image par image. « Rejouer » anime la chronologie ; le filtre sévérité et la recherche permettent d'isoler un hôte, une IP ou un message.

5. Photographier et conserver

« Photographier » exporte la carte en PNG. « Snapshot JSON » exporte les événements pour relecture ultérieure. Le snapshot est réimportable dans l'interface.

> Cas d'usage PME : brancher les logs du pare-feu, du NAS et des serveurs, puis relire l'incident et prouver la chronologie.