AYI NEDJIMI Consultants

Shadow IT & OT 2026 : Détection Wireshark

15 février 2026 • Mis à jour le 17 mai 2026 • 50 min de lecture • 768 mo

Guide terrain 2026 : Wireshark pour détecter Shadow IT/OT — capture pas
protocoles industriels Modbus/EtherNet-IP.

À RETENIR

À retenir — Détection Shadow IT/OT Wireshark

Capture 100% passive : Wireshark n'émet aucun paquet — adapté aux env
où un scan Nmap peut faire crasher un automate.

Buffer + rotation : sans configuration ring buffer 1000+ Mo, vous perdez le
fichier pcapng par 30 min).

Filtres signature : ARP gratuit, mDNS, SSDP, Modbus, EtherNet/IP — chaq
trahit sa présence dès le démarrage.

Mirror port vs TAP : SPAN suffit en bureautiq gatoire en
fonctionne sans alimentation).

> **IT/OT sans VLAN** : un seul point de capture sur le switch core suffit à voir t
> configuration idéale pour audit éclair.

La détection du **Shadow IT et Shadow OT** via **Wireshark** est devenue en 2026 une
équipes audit cybersécurité. Contrairement aux scans actifs qui peuvent provoque
d'un capteur industriel sensible, la capture réseau passive permet d'inventorier un
perturbation. Ce guide terrain — testé sur des environnements industriels réels et
configuration des buffers, la rotation des fichiers, les filtres avancés et l'analyse d
(Modbus, EtherNet/IP, PROFINET) pour identifier équipements non déclarés, dériv
inconnus.

Introduction : le Shadow IT tue plus vite en OT qu'en IT

Définitions — ce qu'on chasse vraiment

Le **Shadow IT** désigne tout équipement, application ou service connecté au réseau
validation formelle de la DSI ou du responsable sécurité. Ce n'est pas forcément m
employé qui branche son NAS personnel pour "aller plus vite", un prestataire qui in
sans en parler, ou un responsable commercial qui connecte son iPhone en partage
Wi-Fi est lent".

Le **Shadow OT** est la variante industrielle : un automate ajouté à la ligne de produc
schéma réseau, un écran HMI connecté directement sur le réseau corporate pour
routeur 4G installé dans une armoire électrique par un intégrateur pressé, un capt
sur le réseau SCADA parce qu'il "offrait des statistiq

Réponse sous 24h

Devis gratuit →