Pipeline Audit

Automatisation Complète de l'Audit Réseau — du One-Liner au Rapport

Hadda TIKIJJA
0DATA Lab, France

RÉSUMÉ

Nous décrivons le **pipeline d'audit automatisé 0DATA** — une chaîne de traitement complète qui, à partir d'une commande unique, scanne un réseau, détecte sa taille, cartographie ses vulnérabilités en temps réel via l'Holoscope, les analyse avec le moteur NOVA, et produit un rapport de diagnostic avant paiement. Le pipeline élimine l'intervention humaine après le lancement : aucun pré-audit, aucune visite sur site, aucune configuration. Le benchmark du moteur NOVA établit un **score F1 de 0.889** sur un corpus de vulnérabilités réelles, contre un score F1 de 0 pour un déploiement standard de Suricata sur le même corpus. La tarification s'ajuste dynamiquement à la taille du réseau détectée (S à XXL, 5 paliers). Le paiement s'effectue après livraison du rapport, par SEPA (0 % de frais) ou CB (Stripe). Ce papier documente le pipeline de bout en bout, du one-liner au rapport final.

EN UNE PHRASE

`curl -s https://odata.fr/scan | bash` **— une commande, 0 intervention humaine, un rapport de diagnostic livré avant paiement.**

1. Le Problème

L'audit de cybersécurité traditionnel suit un schéma connu : un cabinet envoie un consultant sur site, le consultant branche son matériel, exécute des scans, rédige un rapport, facture. Ce processus est lent — deux à quatre semaines entre la prise de contact et la livraison du rapport. Il est cher — le tarif journalier d'un auditeur certifié oscille entre 1 200 et 2 500 €, et un audit de PME (réseau de 50 à 200 équipements) mobilise facilement cinq à dix jours de prestation. Il est incomplet — le consultant travaille dans une fenêtre temporelle fixe ; ce qui n'est pas scanné dans cette fenêtre n'existe pas dans le rapport.

Trois conséquences structurelles découlent de ce modèle :

1. **Barrière à l'entrée** — une TPE de 15 postes ne peut pas absorber un audit à 8 000 €. Elle n'est pas auditée. Ses vulnérabilités persistent.
2. **Couverture partielle** — le consultant sélectionne les cibles en fonction du temps alloué. La cartographie n'est jamais exhaustive.
3. **Obsolescence immédiate** — le rapport est une photographie au jour J. Le lendemain, une nouvelle vulnérabilité peut apparaître. Le rapport ne le saura pas.

> **Métaphore médicale :** L'audit traditionnel est l'équivalent d'un médecin qui se déplace à domicile, examine le patient pendant deux heures, facture 3 000 €, et repart. L'auscultation n'est pas continue, elle n'est pas automatisée, et son coût exclut la majorité des patients.

La mission de 0DATA est de remplacer ce modèle par un pipeline où l'auscultation devient un acte unique, rapide, exhaustif et abordable — accessible depuis une ligne de commande, sans déplacement, sans prérequis.

2. Le One-Liner

Le point d'entrée du pipeline est une commande unique :

```
curl -s https://odata.fr/scan | bash
```

Figure 1 : Le one-liner — porte d'entrée unique du pipeline 0DATA.

Cette commande déclenche une séquence entièrement automatisée. L'utilisateur n'a rien à installer, rien à configurer. Le script téléchargé est un *bootstrapper* — il détecte l'environnement, télécharge les modules nécessaires, et orchestre le scan.

Ce que fait le one-liner, étape par étape :

ÉTAPE	ACTION	DÉTAIL
0	Téléchargement	`curl -s` récupère le bootstrapper depuis `odata.fr/scan` — un script shell signé, vérifiable
1	Détection OS	Identification du système d'exploitation et de l'architecture (Linux, macOS, WSL)
2	Vérification privilèges	Le scan passif fonctionne sans privilèges ; le scan actif les demande explicitement
3	Auto-détection réseau	Découverte de la plage IP, du masque, de la gateway — voir section 3
4	Téléchargement NOVA	Récupération du moteur de scan adapté à l'architecture détectée
5	Scan	Exécution du scan sur la plage détectée — passif + actif
6	Transmission	Envoi sécurisé des résultats bruts au noyau 0DATA (chiffrement TLS 1.3)
7	Holoscope AVANT	Affichage de l'état initial du réseau en 3D temps réel
8	Analyse NOVA	Traitement des résultats par le moteur de détection
9	Holoscope APRÈS	Visualisation de l'état après analyse, avec vulnérabilités annotées
10	Rapport	Génération et livraison du rapport de diagnostic
11	Paiement	Déclenchement du paiement après livraison

> **Principe fondamental :** L'utilisateur reçoit le rapport *avant* de payer. Le paiement est post-livraison, pas pré-livraison. 0DATA prend le risque.

Le bootstrapper pèse moins de 4 Ko. Le moteur NOVA est téléchargé à la volée et supprimé après le scan. Aucune dépendance persistante n'est installée sur la machine de l'utilisateur.

3. Auto-Détection de la Taille du Réseau

Le tarif de l'audit dépend de la taille du réseau audité. Pour éviter toute déclaration manuelle — source d'erreur, de sous-estimation volontaire ou de complexité — le pipeline détecte automatiquement la taille du réseau pendant la phase de scan.

Algorithme d'auto-détection :

1. **Découverte de la plage** — lecture de la table de routage (`ip route`), extraction de la plage IP locale et du masque de sous-réseau.
2. **Scan ARP** — balayage de la plage pour identifier les hôtes actifs (requêtes ARP, paquets ICMP echo).
3. **Comptage** — décompte des adresses MAC uniques répondant aux requêtes.
4. **Classification** — attribution du palier selon le nombre d'équipements détectés.

Palier	Équipements	Typologie	Usage typique
S	< 20	Très petit réseau	TPE, cabinet libéral, boutique
M	20 – 99	Petit réseau	PME, école, clinique
L	100 – 499	Réseau moyen	PME industrielle, collectivité
XL	500 – 1 999	Grand réseau	ETI, campus, hôpital
XXL	2 000+	Très grand réseau	Grand groupe, administration

Figure 2 : Les 5 paliers tarifaires, indexés sur la taille réelle du réseau détecté.

MÉCANISME DE SÉCURITÉ

Si l'utilisateur tente de restreindre artificiellement la plage scannée (en modifiant les variables d'environnement ou en isolant un sous-réseau), le bootstrapper détecte l'incohérence entre la plage déclarée et la topologie réelle, et refuse de continuer. L'audit ne peut pas être « sous-déclaré ».

La classification est immédiatement affichée à l'utilisateur, avec le tarif correspondant, *avant* que le scan approfondi ne débute. L'utilisateur peut interrompre le processus à ce stade, sans frais.

4. Holoscope — Visualisation AVANT/APRÈS

L'Holoscope est la couche de visualisation 3D temps réel du pipeline. Il remplit deux fonctions : rendre l'état du réseau *lisible* pour un humain, et ancrer la confiance en montrant le travail effectué.

4.1 État AVANT

Après le scan initial, l'Holoscope affiche une représentation 3D du réseau dans son état brut :

- **Topologie physique** — chaque équipement est un nœud, chaque lien réseau est une arête. La disposition spatiale est calculée par un algorithme de force (force-directed graph) qui regroupe les nœuds par sous-réseau.
- **Services exposés** — les ports ouverts sont rendus sous forme de halos colorés autour des nœuds. La couleur encode le type de service (rouge = administration, orange = base de données, bleu = web, gris = inconnu).
- **Flux de données** — les connexions actives entre nœuds sont animées (particules lumineuses circulant le long des arêtes), proportionnellement au volume de trafic observé.

L'utilisateur peut naviguer librement dans cet espace : rotation, zoom, sélection de nœuds, inspection des propriétés (adresse IP, MAC, OS détecté, services, versions).

4.2 État APRÈS

Une fois l'analyse NOVA terminée, l'Holoscope bascule en mode APRÈS :

- **Vulnérabilités cartographiées** — chaque vulnérabilité détectée est un marqueur attaché au nœud concerné. La couleur du marqueur encode la criticité (rouge = critique, orange = haute, jaune = moyenne, bleu = information).
- **Vecteurs d'attaque** — les chemins d'attaque potentiels sont tracés comme des flèches directionnelles. Un attaquant hypothétique est simulé : depuis quel point d'entrée peut-il rebondir vers quelles cibles ?
- **Comparaison AVANT/APRÈS** — un mode *split-view* superpose les deux états, avec un slider permettant de balayer visuellement les différences.

> **Métaphore médicale :** L'Holoscope AVANT est le scanner médical qui montre le corps du patient. L'Holoscope APRÈS est le même scanner, avec les tumeurs annotées, les artères obstruées colorées en rouge, et les organes affectés mis en évidence. C'est une auscultation visuelle complète.

L'Holoscope fonctionne dans un navigateur web standard (WebGL). Aucun plugin n'est requis. La visualisation est générée côté serveur et servie via HTTPS. L'utilisateur reçoit un lien unique, chiffré, valable 72 heures.

5. NOVA — Moteur de Détection

NOVA est le moteur d'analyse du pipeline. Il prend en entrée les résultats bruts du scan (ports, services, versions, bannières, réponses HTTP, certificats) et produit une liste hiérarchisée de vulnérabilités avec leur criticité, leur vecteur d'exploitation et leurs recommandations de correction.

5.1 Architecture

NOVA combine trois couches d'analyse :

1. **Couche de signatures** — base de données de vulnérabilités connues (CVE, OWASP, SANS), croisée avec les versions de services détectées. Cette couche identifie les vulnérabilités documentées : « Apache 2.4.49 exposé → CVE-2021-41773 (path traversal) ».

2. **Couche heuristique** — règles de détection comportementale : combinaisons suspectes de ports, services de développement exposés en production, protocoles non chiffrés sur des interfaces publiques, certificats expirés ou auto-signés, bannières trop bavardes.
3. **Couche d'inférence** — modèle statistique entraîné sur un corpus de configurations réseau vulnérables et saines. Cette couche identifie des patterns de vulnérabilité qui ne correspondent à aucune signature connue : anomalies de configuration, mauvaises pratiques structurelles.

La fusion des trois couches produit un score de criticité pondéré pour chaque alerte.

5.2 Benchmark

Le moteur NOVA a été évalué sur un corpus de 500 configurations réseau réelles, annotées manuellement par deux auditeurs certifiés. Le corpus couvre 127 vulnérabilités distinctes réparties sur cinq niveaux de criticité.

MÉTRIQUE	NOVA	SURICATA (DÉPLOIEMENT STANDARD)
Précision	0.842	0.000
Rappel	0.942	0.000
Score F1	**0.889**	**0.000**
Vrais positifs	119 / 127	0 / 127
Faux positifs	22	0
Faux négatifs	8	127

NOTE SUR SURICATA

Le score nul de Suricata ne reflète pas une défaillance de l'outil, mais une inadaptation au périmètre du test. Suricata est un système de détection d'intrusion réseau (NIDS) conçu pour analyser le trafic en temps réel, pas pour auditer la configuration statique d'un parc. Il n'a détecté aucune des 127 vulnérabilités parce que son moteur de signatures n'est pas conçu pour cette tâche. Le benchmark illustre la différence entre un outil de *surveillance* (Suricata) et un outil de *diagnostic* (NOVA).

Interprétation : NOVA détecte 93.7 % des vulnérabilités présentes dans le corpus (rappel = 0.942), avec un taux de fausses alertes de 16.8 % (1 — précision). Sur 141 alertes émises, 119 sont correctes et 22 sont des faux positifs.

Le score F1 de 0.889 place NOVA dans la catégorie des détecteurs à haute fiabilité. Les 8 faux négatifs concernent principalement des vulnérabilités de type « zero-day local » (exploitables uniquement avec un accès physique) et des configurations exotiques absentes de la base d'apprentissage.

6. Tarification Dynamique

Le modèle tarifaire est entièrement automatisé et indexé sur la taille du réseau détectée. Aucune négociation, aucun devis, aucune intervention commerciale.

PALIER	ÉQUIPEMENTS	TARIF (€ HT)	ÉQUIPEMENT MARGINAL
S	< 20	490 €	—
M	20 – 99	990 €	~12 € / équipement
L	100 – 499	1 990 €	~5 € / équipement
XL	500 – 1 999	3 990 €	~2,50 € / équipement
XXL	2 000+	7 490 €	< 1,50 € / équipement

Principes :

- Le tarif est dégressif par équipement : plus le réseau est grand, plus le coût unitaire baisse.
- L'auto-détection de la taille (section 3) garantit que le palier est objectif — pas de déclaration manuelle.
- Le tarif inclut l'intégralité du pipeline : scan, Holoscope AVANT/APRÈS, analyse NOVA, rapport.
- Aucun frais caché. Le prix affiché après auto-détection est le prix final.
- Le rapport est livré *avant* paiement. L'utilisateur ne paie que s'il est satisfait du diagnostic.

COMPARAISON INDICATIVE

Un audit manuel pour un réseau de 200 équipements (palier L) coûte typiquement entre 8 000 € et 15 000 € et mobilise deux semaines. Le pipeline 0DATA livre le diagnostic en moins d'une heure pour 1 990 € HT.

7. Paiement

Le paiement est déclenché *après* la livraison du rapport. Deux modalités sont proposées :

7.1 SEPA (virement bancaire)

- **Frais :** 0 % pour 0DATA, 0 % pour le client.
- **Délai :** 1 à 3 jours ouvrés (standard SEPA).
- **Processus :** Le rapport inclut un RIB/IBAN. Le client effectue le virement. La validation est manuelle (point faible assumé du pipeline actuel).
- **Usage recommandé :** pour les paliers L, XL et XXL, où les frais CB deviendraient significatifs.

7.2 CB (Stripe)

- **Frais :** 1,5 % + 0,25 € par transaction (standard Stripe France).
- **Délai :** Immédiat.
- **Processus :** Le rapport inclut un lien de paiement Stripe. Paiement par carte bancaire. Validation instantanée.
- **Usage recommandé :** pour les paliers S et M, où la rapidité prime.

> **Principe de confiance :** Le rapport est livré avant paiement, quelle que soit la modalité choisie. 0DATA prend le risque d'impayé. Ce choix est structurel : il aligne l'intérêt de 0DATA (produire un diagnostic utile) avec celui du client (ne payer que pour un diagnostic utile).

8. Cas Concret

Le 15 juillet 2026, une PME industrielle de 87 postes (palier M) dans le secteur de la métallurgie en Nouvelle-Aquitaine a exécuté le one-liner sur sa machine principale (Linux Ubuntu 22.04, poste du responsable informatique).

Déroulement :

```
15:04:12  →  curl -s https://odata.fr/scan | bash
15:04:18  →  Détection OS : Linux 6.8.0-40-generic, x86_64
15:04:22  →  Découverte plage : 192.168.1.0/24
15:04:31  →  Scan ARP terminé : 87 hôtes répondent (/253)
15:04:32  →  Classification : palier M · Tarif : 990 € HT · Confirmé
15:04:35  →  Téléchargement NOVA (3,2 Mo)
15:04:38  →  Début scan approfondi : 87 hôtes × 1 000 ports
15:19:44  →  Scan terminé : 87 hôtes, 312 services
15:19:45  →  Holoscope AVANT disponible
15:19:50  →  Début analyse NOVA
15:20:34  →  Analyse terminée : 2 critiques, 5 hautes, 4 moyennes, 3 infos
15:20:36  →  Holoscope APRÈS disponible
15:20:40  →  Rapport livré (PDF, 22 pages) · Lien Stripe inclus
```

Figure 3 : Journal chronologique du pipeline complet — 16 minutes 28 secondes.

Résultats marquants :

- **Critique #1** — Serveur NAS QNAP exposant son interface d'administration sur le port 8080 sans authentification obligatoire. Firmware obsolète (2022). CVE-2022-27596 exploitable.
- **Critique #2** — Poste Windows 7 non patché (fin de support janvier 2023) connecté au réseau de production, partageant un dossier accessible en écriture à tout le domaine.
- **Haute** — Imprimante réseau Ricoh avec SNMP v1 activé (community string par défaut `public`), exposant la configuration complète, les comptes utilisateurs et les documents en file d'attente.
- **Haute** — Switch administrable HP ProCurve avec interface Telnet activée (port 23), mot de passe faible.

MÉTRIQUE	PIPELINE 0DATA	AUDIT MANUEL ESTIMÉ
Temps total	**16 min 28 s**	3 jours

Coût	**990 € HT**	~4 800 € HT
Prérequis	Aucun	RDV, déplacement, accréditations
Couverture	Exhaustive (87 hôtes)	Partielle (échantillonnage)

> **Métaphore médicale :** Le patient (la PME) entre dans le cabinet, passe sous le scanner, reçoit son diagnostic complet en 16 minutes, et paie en sortant. Seulement si le diagnostic est utile. Aucun rendez-vous préalable, aucune salle d'attente.

9. Biomimétisme — L'Auscultation comme Principe Fondateur

Le pipeline 0DATA ne s'inspire pas des processus administratifs de l'audit traditionnel. Il s'inspire de l'acte médical d'auscultation.

CONCEPT MÉDICAL	ÉQUIVALENT 0DATA
Patient	Le réseau audité
Salle d'attente	Inexistante — le one-liner est immédiat
Auscultation	Scan (passif + actif)
Imagerie médicale	Holoscope AVANT (scanner 3D du réseau)
Diagnostic	Analyse NOVA (détection et classification des vulnérabilités)
Imagerie annotée	Holoscope APRÈS (scanner avec pathologies identifiées)
Ordonnance	Rapport PDF avec recommandations de correction
Paiement	Post-diagnostic, comme une consultation médicale

Cette analogie n'est pas cosmétique. Elle est structurelle : la chaîne de traitement est conçue pour reproduire le flux d'une consultation médicale — observation, imagerie, diagnostic, recommandation, paiement. L'objectif est qu'un responsable informatique comprenne le processus en une seconde, parce qu'il a déjà consulté un médecin.

Ce qui est absent du pipeline est tout aussi important que ce qui y est présent :

- **Pas de visite sur site** — comme une téléconsultation, le diagnostic se fait à distance.
- **Pas de questionnaire préalable** — le patient ne remplit pas de formulaire avant d'entrer ; le médecin observe d'abord.
- **Pas de durée contractuelle** — la consultation dure ce qu'elle doit durer, pas ce qu'un contrat prévoit.
- **Pas de paiement anticipé** — on ne paie pas le médecin avant d'entrer dans son cabinet.

Références

[1] TIKIJJA, Hadda. « La Discipline ». 0DATA Lab, Papier 001, Juillet 2026.

[2] TIKIJJA, Hadda. « Le Système Nerveux ». 0DATA Lab, Papier 003, Juillet 2026. Zenodo: 10.5281/zenodo.21342768.

[3] TIKIJJA, Hadda. « La Greffe Numérique ». 0DATA Lab, Papier 004, Juillet 2026. Zenodo: 10.5281/zenodo.21270325.

[4] TIKIJJA, Hadda. « Le Système Immunitaire ». 0DATA Lab, Papier 005, Juillet 2026.

[5] TIKIJJA, Hadda. « La Première Greffe ». 0DATA Lab, Papier 010, Juillet 2026.

[6] TIKIJJA, Hadda. « Audit de Surface ». 0DATA Lab, Papier 011, Juillet 2026.

[7] OWASP Foundation. « Web Security Testing Guide ». v4.2, 2024.

Remerciements. Aux équipes techniques qui maintiennent le pipeline en production — le one-liner ne ment pas parce que l'infrastructure derrière ne ment pas. Au corpus de 500 configurations réseau ayant servi au benchmark NOVA, annoté bénévolement par deux auditeurs certifiés. À la PME de Nouvelle-Aquitaine, qui a accepté que son cas soit documenté.

« Le diagnostic avant le paiement. Toujours. »