Auditoría de Pipeline

Automatización Completa de la Auditoría de Red — del One-Liner al Informe

Hadda TIKIJJA
0DATA Lab, Francia

RESUMEN

Describimos el **pipeline de auditoría automatizado 0DATA** — una cadena de procesamiento completa que, a partir de un único comando, escanea una red, detecta su tamaño, cartografía sus vulnerabilidades en tiempo real mediante el Holoscope, las analiza con el motor NOVA y produce un informe de diagnóstico antes del pago. El pipeline elimina la intervención humana tras el lanzamiento: sin preauditoría, sin visita in situ, sin configuración. El benchmark del motor NOVA establece una **puntuación F1 de 0.889** sobre un corpus de vulnerabilidades reales, frente a una puntuación F1 de 0 para un despliegue estándar de Suricata sobre el mismo corpus. La tarificación se ajusta dinámicamente al tamaño de red detectado (de S a XXL, 5 niveles). El pago se efectúa tras la entrega del informe, por SEPA (0 % de comisiones) o tarjeta (Stripe). Este documento documenta el pipeline de extremo a extremo, del one-liner al informe final.

EN UNA FRASE

`curl -s https://odata.fr/scan | bash` **— un comando, 0 intervención humana, un informe de diagnóstico entregado antes del pago.**

1. El Problema

La auditoría de ciberseguridad tradicional sigue un esquema conocido: un gabinete envía a un consultor in situ, el consultor conecta su material, ejecuta escaneos, redacta un informe, factura. Este proceso es lento — de dos a cuatro semanas entre el primer contacto y la entrega del informe. Es caro — la tarifa diaria de un auditor certificado oscila entre 1 200 y 2 500 €, y una auditoría de PYME (red de 50 a 200 equipos) moviliza fácilmente de cinco a diez días de prestación. Es incompleto — el consultor trabaja en una ventana temporal fija; lo que no se escanea en esa ventana no existe en el informe.

De este modelo se derivan tres consecuencias estructurales:

1. **Barrera de entrada** — una microempresa de 15 puestos no puede absorber una auditoría de 8 000 €. No es auditada. Sus vulnerabilidades persisten.
2. **Cobertura parcial** — el consultor selecciona los objetivos en función del tiempo asignado. La cartografía nunca es exhaustiva.
3. **Obsolescencia inmediata** — el informe es una fotografía del día D. Al día siguiente, puede aparecer una nueva vulnerabilidad. El informe no lo sabrá.

> **Metáfora médica:** La auditoría tradicional es el equivalente a un médico que se desplaza a domicilio, examina al paciente durante dos horas, factura 3 000 € y se marcha. La auscultación no es continua, no está automatizada, y su coste excluye a la mayoría de los pacientes.

La misión de 0DATA es sustituir este modelo por un pipeline donde la auscultación se convierte en un acto único, rápido, exhaustivo y asequible — accesible desde una línea de comandos, sin desplazamiento, sin requisitos previos.

2. El One-Liner

El punto de entrada del pipeline es un comando único:

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

Figura 1: El one-liner — puerta de entrada única del pipeline 0DATA.

Este comando desencadena una secuencia totalmente automatizada. El usuario no tiene nada que instalar, nada que configurar. El script descargado es un *bootstrapper* — detecta el entorno, descarga los módulos necesarios y orquesta el escaneo.

Lo que hace el one-liner, paso a paso:

PASO	ACCIÓN	DETALLE
0	Descarga	`curl -s` recupera el bootstrapper desde `odata.fr/scan` — un script de shell firmado y verificable
1	Detección del SO	Identificación del sistema operativo y de la arquitectura (Linux, macOS, WSL)
2	Verificación de privilegios	El escaneo pasivo funciona sin privilegios; el escaneo activo los solicita explícitamente
3	Auto-detección de red	Descubrimiento del rango IP, de la máscara y del gateway — véase la sección 3
4	Descarga de NOVA	Recuperación del motor de escaneo adaptado a la arquitectura detectada
5	Escaneo	Ejecución del escaneo sobre el rango detectado — pasivo + activo
6	Transmisión	Envío seguro de los resultados brutos al núcleo 0DATA (cifrado TLS 1.3)
7	Holoscope ANTES	Visualización del estado inicial de la red en 3D en tiempo real
8	Análisis NOVA	Procesamiento de los resultados por el motor de detección
9	Holoscope DESPUÉS	Visualización del estado tras el análisis, con vulnerabilidades anotadas
10	Informe	Generación y entrega del informe de diagnóstico
11	Pago	Desencadenamiento del pago tras la entrega

> **Principio fundamental:** El usuario recibe el informe *antes* de pagar. El pago es posterior a la entrega, no anterior. 0DATA asume el riesgo.

El bootstrapper pesa menos de 4 KB. El motor NOVA se descarga sobre la marcha y se elimina tras el escaneo. No se instala ninguna dependencia persistente en la máquina del usuario.

3. Auto-Detección del Tamaño de la Red

El precio de la auditoría depende del tamaño de la red auditada. Para evitar toda declaración manual — fuente de error, de subestimación voluntaria o de complejidad — el pipeline detecta automáticamente el tamaño de la red durante la fase de escaneo.

Algoritmo de auto-detección:

1. **Descubrimiento del rango** — lectura de la tabla de enrutamiento (`ip route`), extracción del rango IP local y de la máscara de subred.
2. **Escaneo ARP** — barrido del rango para identificar los hosts activos (solicitudes ARP, paquetes ICMP echo).
3. **Conteo** — recuento de las direcciones MAC únicas que responden a las solicitudes.
4. **Clasificación** — asignación del nivel según el número de equipos detectados.

Nivel	Equipos	Tipología	Uso típico
S	< 20	Red muy pequeña	Microempresa, gabinete, tienda
M	20 – 99	Red pequeña	PYME, escuela, clínica
L	100 – 499	Red mediana	PYME industrial, colectividad
XL	500 – 1 999	Red grande	ETI, campus, hospital
XXL	2 000+	Red muy grande	Gran grupo, administración

Figura 2: Los 5 niveles tarifarios, indexados sobre el tamaño real de la red detectada.

MECANISMO DE SEGURIDAD

Si el usuario intenta restringir artificialmente el rango escaneado (modificando las variables de entorno o aislando una subred), el bootstrapper detecta la incoherencia entre el rango declarado y la topología real, y se niega a continuar. La auditoría no puede «subdeclararse».

La clasificación se muestra inmediatamente al usuario, con el precio correspondiente, *antes* de que comience el escaneo en profundidad. El usuario puede interrumpir el proceso en ese momento, sin coste alguno.

4. Holoscope — Visualización ANTES/DESPUÉS

El Holoscope es la capa de visualización 3D en tiempo real del pipeline. Cumple dos funciones: hacer que el estado de la red sea *legible* para un humano, y anclar la confianza mostrando el trabajo realizado.

4.1 Estado ANTES

Tras el escaneo inicial, el Holoscope muestra una representación 3D de la red en su estado bruto:

- **Topología física** — cada equipo es un nodo, cada enlace de red es una arista. La disposición espacial se calcula mediante un algoritmo de fuerzas (grafo dirigido por fuerzas) que agrupa los nodos por subred.
- **Servicios expuestos** — los puertos abiertos se representan como halos coloreados alrededor de los nodos. El color codifica el tipo de servicio (rojo = administración, naranja = base de datos, azul = web, gris = desconocido).
- **Flujos de datos** — las conexiones activas entre nodos están animadas (partículas luminosas que circulan a lo largo de las aristas), proporcionalmente al volumen de tráfico observado.

El usuario puede navegar libremente por este espacio: rotación, zoom, selección de nodos, inspección de propiedades (dirección IP, MAC, SO detectado, servicios, versiones).

4.2 Estado DESPUÉS

Una vez finalizado el análisis NOVA, el Holoscope pasa al modo DESPUÉS:

- **Vulnerabilidades cartografiadas** — cada vulnerabilidad detectada es un marcador unido al nodo afectado. El color del marcador codifica la criticidad (rojo = crítica, naranja = alta, amarillo = media, azul = informativa).
- **Vectores de ataque** — las rutas de ataque potenciales se trazan como flechas direccionales. Se simula un atacante hipotético: ¿desde qué punto de entrada puede rebotar hacia qué objetivos?

- **Comparación ANTES/DESPUÉS** — un modo *split-view* superpone los dos estados, con un deslizador que permite barrer visualmente las diferencias.

> **Metáfora médica:** El Holoscope ANTES es el escáner médico que muestra el cuerpo del paciente. El Holoscope DESPUÉS es el mismo escáner, con los tumores anotados, las arterias obstruidas coloreadas en rojo y los órganos afectados resaltados. Es una auscultación visual completa.

El Holoscope funciona en un navegador web estándar (WebGL). No se requiere ningún plugin. La visualización se genera en el servidor y se sirve por HTTPS. El usuario recibe un enlace único, cifrado, válido durante 72 horas.

5. NOVA — Motor de Detección

NOVA es el motor de análisis del pipeline. Toma como entrada los resultados brutos del escaneo (puertos, servicios, versiones, banners, respuestas HTTP, certificados) y produce una lista jerarquizada de vulnerabilidades con su criticidad, su vector de explotación y sus recomendaciones de corrección.

5.1 Arquitectura

NOVA combina tres capas de análisis:

1. **Capa de firmas** — base de datos de vulnerabilidades conocidas (CVE, OWASP, SANS), cruzada con las versiones de servicios detectadas. Esta capa identifica las vulnerabilidades documentadas: «Apache 2.4.49 expuesto → CVE-2021-41773 (path traversal)».
2. **Capa heurística** — reglas de detección comportamental: combinaciones sospechosas de puertos, servicios de desarrollo expuestos en producción, protocolos no cifrados en interfaces públicas, certificados caducados o autofirmados, banners demasiado locuaces.
3. **Capa de inferencia** — modelo estadístico entrenado sobre un corpus de configuraciones de red vulnerables y sanas. Esta capa identifica patrones de vulnerabilidad que no corresponden a ninguna firma conocida: anomalías de configuración, malas prácticas estructurales.

La fusión de las tres capas produce una puntuación de criticidad ponderada para cada alerta.

5.2 Benchmark

El motor NOVA fue evaluado sobre un corpus de 500 configuraciones de red reales, anotadas manualmente por dos auditores certificados. El corpus cubre 127 vulnerabilidades distintas repartidas en cinco niveles de criticidad.

MÉTRICA	NOVA	SURICATA (DESPLIEGUE ESTÁNDAR)
Precisión	0.842	0.000
Exhaustividad	0.942	0.000
Puntuación F1	**0.889**	**0.000**
Verdaderos positivos	119 / 127	0 / 127
Falsos positivos	22	0
Falsos negativos	8	127

NOTA SOBRE SURICATA

La puntuación nula de Suricata no refleja un fallo de la herramienta, sino una inadecuación al perímetro de la prueba. Suricata es un sistema de detección de intrusiones de red (NIDS) diseñado para analizar el tráfico en tiempo real, no para auditar la configuración estática de un parque. No detectó ninguna de las 127 vulnerabilidades porque su motor de firmas no está diseñado para esa tarea. El benchmark ilustra la diferencia entre una herramienta de *monitoreo* (Suricata) y una herramienta de *diagnóstico* (NOVA).

Interpretación: NOVA detecta el 93,7 % de las vulnerabilidades presentes en el corpus (exhaustividad = 0.942), con una tasa de falsas alertas del 16,8 % (1 — precisión). De 141 alertas emitidas, 119 son correctas y 22 son falsos positivos.

La puntuación F1 de 0.889 sitúa a NOVA en la categoría de detectores de alta fiabilidad. Los 8 falsos negativos conciernen principalmente a vulnerabilidades de tipo «zero-day local» (explotables únicamente con acceso físico) y a configuraciones exóticas ausentes de la base de aprendizaje.

6. Tarificación Dinámica

El modelo tarifario está totalmente automatizado e indexado sobre el tamaño de red detectado. Sin negociación, sin presupuesto, sin intervención comercial.

NIVEL	EQUIPOS	PRECIO (€ SIN IVA)	EQUIPO MARGINAL
S	< 20	490 €	—
M	20 – 99	990 €	~12 € / equipo
L	100 – 499	1 990 €	~5 € / equipo
XL	500 – 1 999	3 990 €	~2,50 € / equipo
XXL	2 000+	7 490 €	< 1,50 € / equipo

Principios:

- El precio es degresivo por equipo: cuanto mayor es la red, menor es el coste unitario.
- La auto-detección del tamaño (sección 3) garantiza que el nivel es objetivo — sin declaración manual.
- El precio incluye la totalidad del pipeline: escaneo, Holoscope ANTES/DESPUÉS, análisis NOVA, informe.
- Sin costes ocultos. El precio mostrado tras la auto-detección es el precio final.
- El informe se entrega *antes* del pago. El usuario solo paga si está satisfecho con el diagnóstico.

COMPARACIÓN INDICATIVA

Una auditoría manual para una red de 200 equipos (nivel L) cuesta típicamente entre 8 000 € y 15 000 € y moviliza dos semanas. El pipeline 0DATA entrega el diagnóstico en menos de una hora por 1 990 € sin IVA.

7. Pago

El pago se desencadena *después* de la entrega del informe. Se proponen dos modalidades:

7.1 SEPA (transferencia bancaria)

- **Comisiones:** 0 % para 0DATA, 0 % para el cliente.
- **Plazo:** de 1 a 3 días hábiles (estándar SEPA).
- **Proceso:** El informe incluye un RIB/IBAN. El cliente efectúa la transferencia. La validación es manual (punto débil asumido del pipeline actual).
- **Uso recomendado:** para los niveles L, XL y XXL, donde las comisiones de tarjeta resultarían significativas.

7.2 Tarjeta (Stripe)

- **Comisiones:** 1,5 % + 0,25 € por transacción (estándar Stripe Francia).
- **Plazo:** Inmediato.
- **Proceso:** El informe incluye un enlace de pago Stripe. Pago con tarjeta bancaria. Validación instantánea.
- **Uso recomendado:** para los niveles S y M, donde prima la rapidez.

> **Principio de confianza:** El informe se entrega antes del pago, sea cual sea la modalidad elegida. 0DATA asume el riesgo de impago. Esta elección es estructural: alinea el interés de 0DATA (producir un diagnóstico útil) con el del cliente (pagar solo por un diagnóstico útil).

8. Caso Concreto

El 15 de julio de 2026, una PYME industrial de 87 puestos (nivel M) del sector de la metalurgia en Nueva Aquitania ejecutó el one-liner en su máquina principal (Linux Ubuntu 22.04, puesto del responsable informático).

Desarrollo:

```
15:04:12  →  curl -s https://odata.fr/scan | bash
15:04:18  →  Detección del SO : Linux 6.8.0-40-generic, x86_64
15:04:22  →  Descubrimiento del rango : 192.168.1.0/24
15:04:31  →  Escaneo ARP terminado : 87 hosts responden (/253)
15:04:32  →  Clasificación : nivel M · Precio : 990 € sin IVA · Confirmado
15:04:35  →  Descarga de NOVA (3,2 MB)
15:04:38  →  Inicio del escaneo en profundidad : 87 hosts × 1 000 puertos
15:19:44  →  Escaneo terminado : 87 hosts, 312 servicios
15:19:45  →  Holoscope ANTES disponible
15:19:50  →  Inicio del análisis NOVA
15:20:34  →  Análisis terminado : 2 críticas, 5 altas, 4 medias, 3 informativas
15:20:36  →  Holoscope DESPUÉS disponible
15:20:40  →  Informe entregado (PDF, 22 páginas) · Enlace Stripe incluido
```

Figura 3: Registro cronológico del pipeline completo — 16 minutos 28 segundos.

Resultados destacados:

- **Crítica #1** — Servidor NAS QNAP que expone su interfaz de administración en el puerto 8080 sin autenticación obligatoria. Firmware obsoleto (2022). CVE-2022-27596 explotable.
- **Crítica #2** — Puesto Windows 7 sin parchear (fin de soporte en enero de 2023) conectado a la red de producción, que comparte una carpeta con escritura accesible a todo el dominio.
- **Alta** — Impresora de red Ricoh con SNMP v1 activado (cadena de comunidad por defecto `public`), que expone la configuración completa, las cuentas de usuario y los documentos en cola de impresión.
- **Alta** — Switch administrable HP ProCurve con interfaz Telnet activada (puerto 23), contraseña débil.

MÉTRICA	PIPELINE 0DATA	AUDITORÍA MANUAL ESTIMADA
Tiempo total	**16 min 28 s**	3 días
Coste	**990 € sin IVA**	~4 800 € sin IVA
Requisitos previos	Ninguno	Cita, desplazamiento, acreditaciones
Cobertura	Exhaustiva (87 hosts)	Parcial (muestreo)

> **Metáfora médica:** El paciente (la PYME) entra en la consulta, pasa bajo el escáner, recibe su diagnóstico completo en 16 minutos y paga al salir. Solo si el diagnóstico es útil. Sin cita previa, sin sala de espera.

9. Biomímesis — La Auscultación como Principio Fundador

El pipeline 0DATA no se inspira en los procesos administrativos de la auditoría tradicional. Se inspira en el acto médico de la auscultación.

CONCEPTO MÉDICO	EQUIVALENTE 0DATA
Paciente	La red auditada
Sala de espera	Inexistente — el one-liner es inmediato
Auscultación	Escaneo (pasivo + activo)
Imagen médica	Holoscope ANTES (escáner 3D de la red)
Diagnóstico	Análisis NOVA (detección y clasificación de vulnerabilidades)
Imagen anotada	Holoscope DESPUÉS (escáner con patologías identificadas)
Receta	Informe PDF con recomendaciones de corrección
Pago	Posterior al diagnóstico, como una consulta médica

Esta analogía no es cosmética. Es estructural: la cadena de procesamiento está diseñada para reproducir el flujo de una consulta médica — observación, imagen, diagnóstico, recomendación, pago. El objetivo es que un responsable informático comprenda el proceso en un segundo, porque ya ha consultado a un médico.

Lo que está ausente del pipeline es tan importante como lo que está presente:

- **Sin visita in situ** — como una teleconsulta, el diagnóstico se realiza a distancia.
- **Sin cuestionario previo** — el paciente no rellena un formulario antes de entrar; el médico observa primero.

- **Sin duración contractual** — la consulta dura lo que debe durar, no lo que prevé un contrato.
- **Sin pago anticipado** — no se paga al médico antes de entrar en su consulta.

Referencias

[1] TIKIJJA, Hadda. «La Disciplina». 0DATA Lab, Documento 001, Julio 2026.

[2] TIKIJJA, Hadda. «El Sistema Nervioso». 0DATA Lab, Documento 003, Julio 2026. Zenodo: 10.5281/zenodo.21342768.

[3] TIKIJJA, Hadda. «El Injerto Digital». 0DATA Lab, Documento 004, Julio 2026. Zenodo: 10.5281/zenodo.21270325.

[4] TIKIJJA, Hadda. «El Sistema Inmunitario». 0DATA Lab, Documento 005, Julio 2026.

[5] TIKIJJA, Hadda. «El Primer Injerto». 0DATA Lab, Documento 010, Julio 2026.

[6] TIKIJJA, Hadda. «Auditoría de Superficie». 0DATA Lab, Documento 011, Julio 2026.

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

Agradecimientos. A los equipos técnicos que mantienen el pipeline en producción — el one-liner no miente porque la infraestructura que hay detrás no miente. Al corpus de 500 configuraciones de red que sirvió al benchmark de NOVA, anotado voluntariamente por dos auditores certificados. A la PYME de Nueva Aquitania, que aceptó que su caso fuera documentado.

«El diagnóstico antes del pago. Siempre.»