9.SEÑALES DE VIDA (O ALGO PEOR) EN LA RED

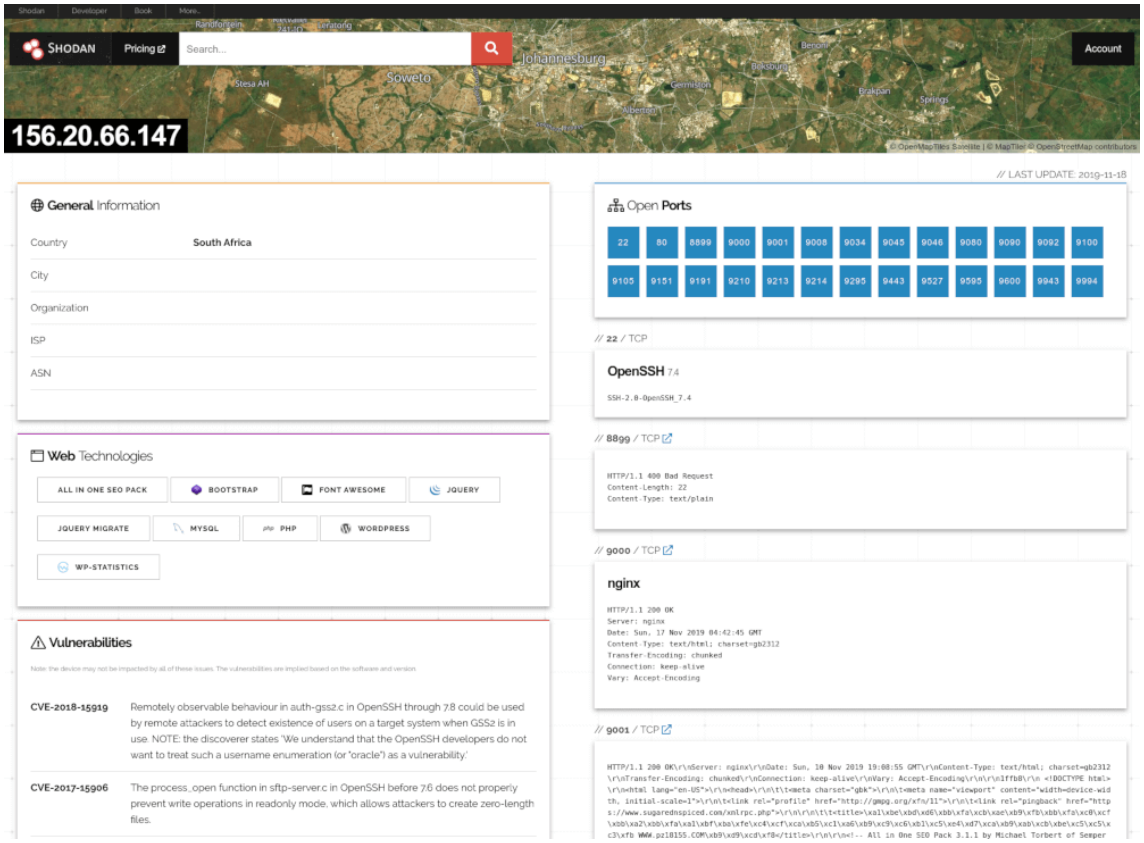
Practica [OSINT]- SEÑALES DE VIDA (O ALGO PEOR) EN LA RED

La nave **USCSS Nostromo** ha recibido una transmisión automática desde un sistema remoto. No se sabe si es una llamada de socorro... o una advertencia.
La compañía ha encomendado al **Equipo de Investigación (tus alumnos)** usar *Shodan* para rastrear:

1. **Señales de dispositivos expuestos**
2. **Orígenes de la transmisión**
3. **Infraestructura del sistema remoto**
4. **Posibles vectores de intrusión**

La misión: **analizar patrones, encontrar conexiones y trazar el mapa de un "nido" digital escondido.**

La actividad se divide en **3 fases**, cada una con un objetivo claro y un filtro de Shodan.



FASE 1 — Localizar señales: “Ping de movimiento”

Objetivo: practicar filtros por tipo de dispositivo + país/ciudad.

El sensor de movimiento de la Nostromo detecta *actividad anómala* en una zona del sistema. Necesitamos saber qué dispositivos expuestos hay allí.

Tareas:

1. **Buscar un tipo concreto de dispositivo** (puerta automatizada, cámara IP, sistema industrial, etc.) Ejemplos:

a. Cámaras IP:

`product:GoAhead`

`product:"Hikvision"`

`port:554 has_screenshot:true`

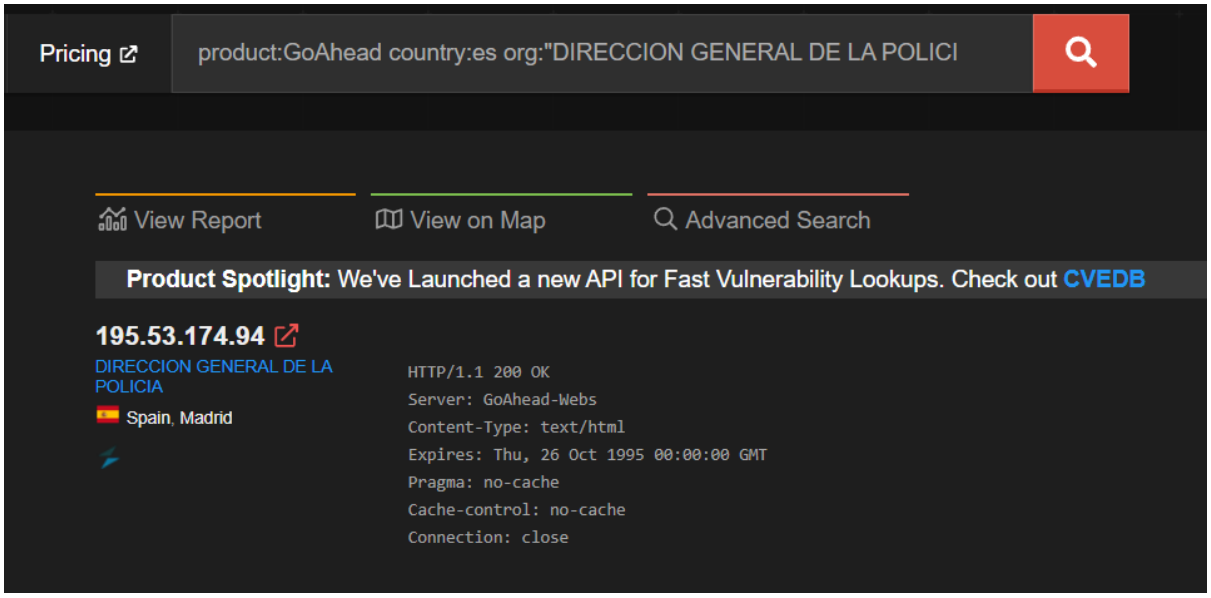
b. Paneles web expuestos:

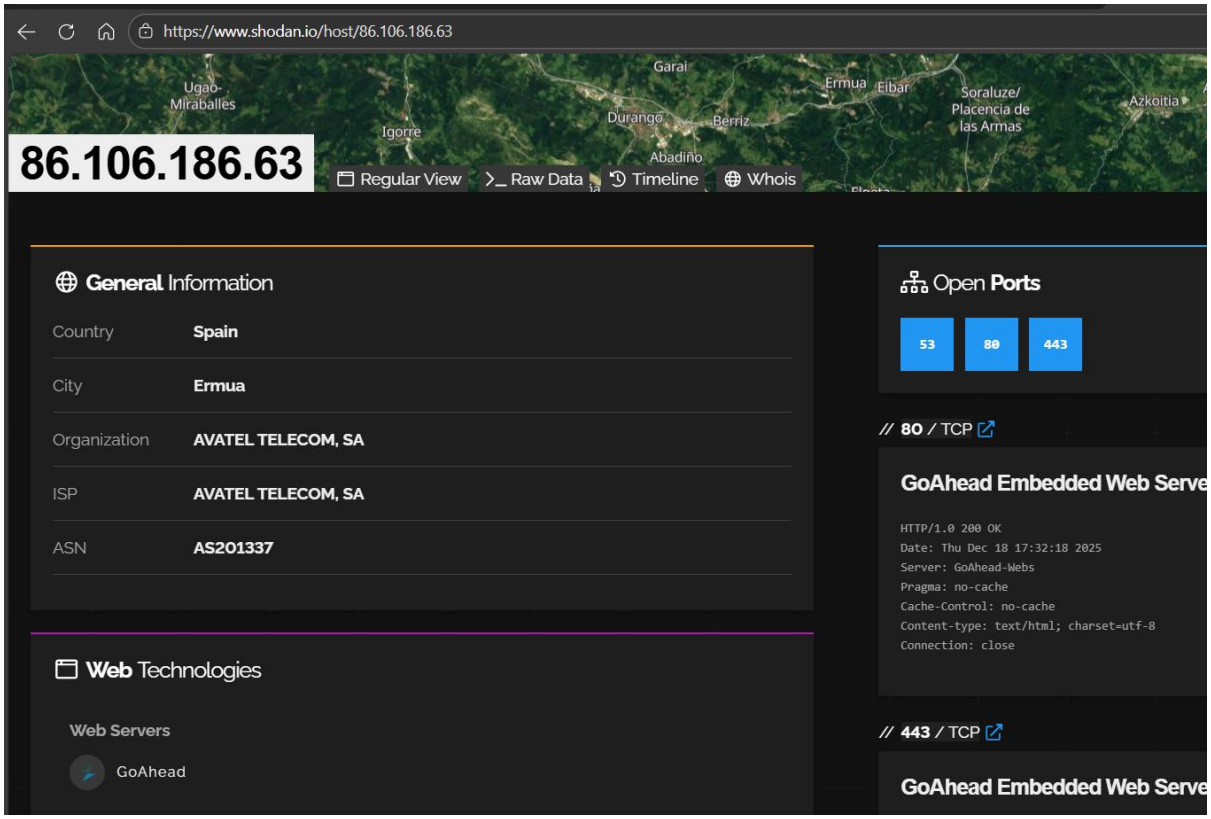
`http.title:"login"`

2. **Añadir filtro de ubicación** (país o ciudad).

   Por ejemplo, España: `country:ES product:GoAhead` O por ciudad: `city:Madrid http.title:login`

3. Apuntar **IP, puerto, captura y versión** como si fueran "señales biológicas".





FASE 2 — Identificar el origen de la transmisión

Objetivo: buscar por **organización o dominio**.

La señal parece provenir de una colonia (una empresa, universidad o dominio). Deben “explorar todas las instalaciones” de ese lugar.

Ejercicios:

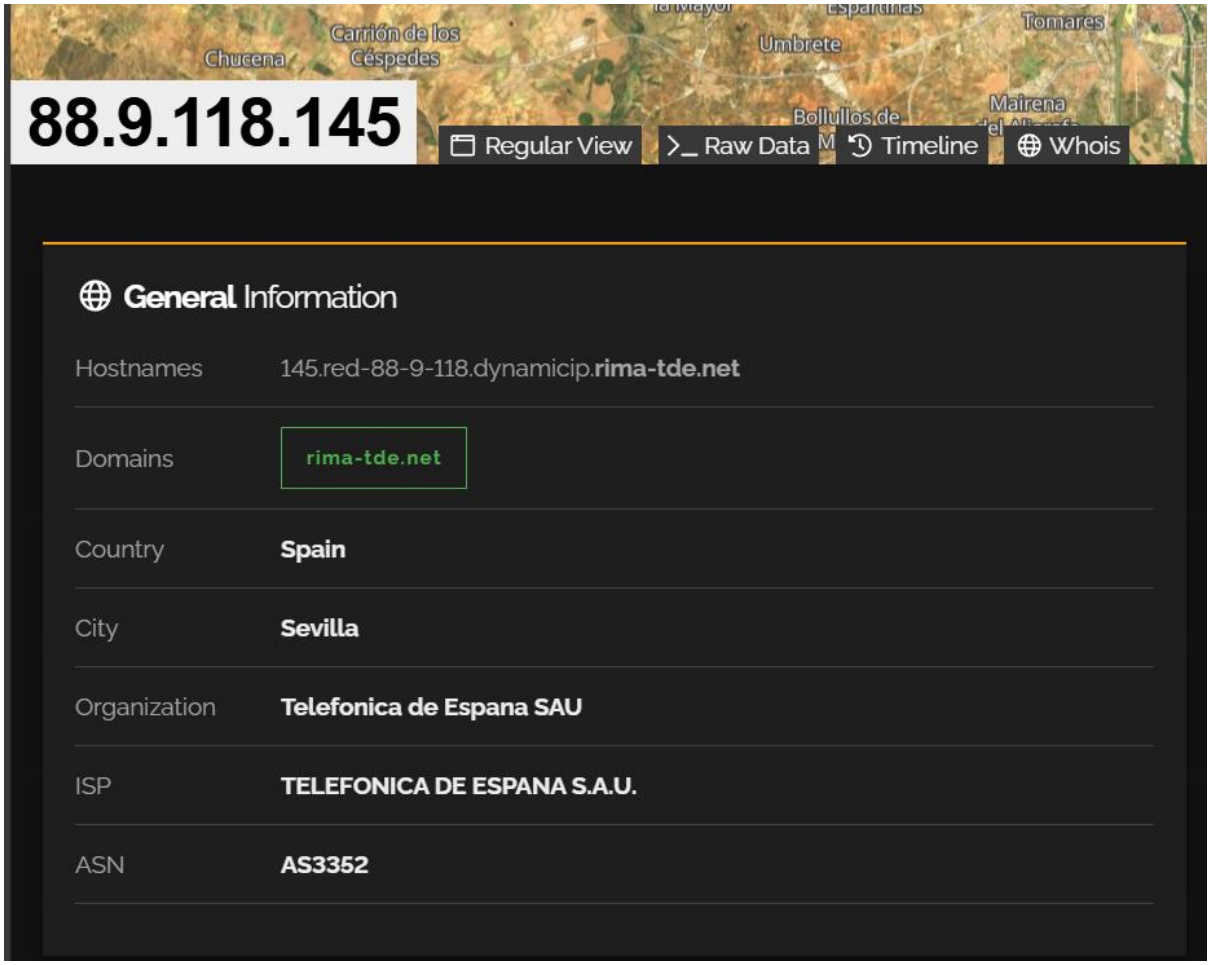
1. Elegir una organización pública o conocida: Ejemplos: `org:"Universidad Complutense"` `org:"Telefonica"`

147.96.0.0

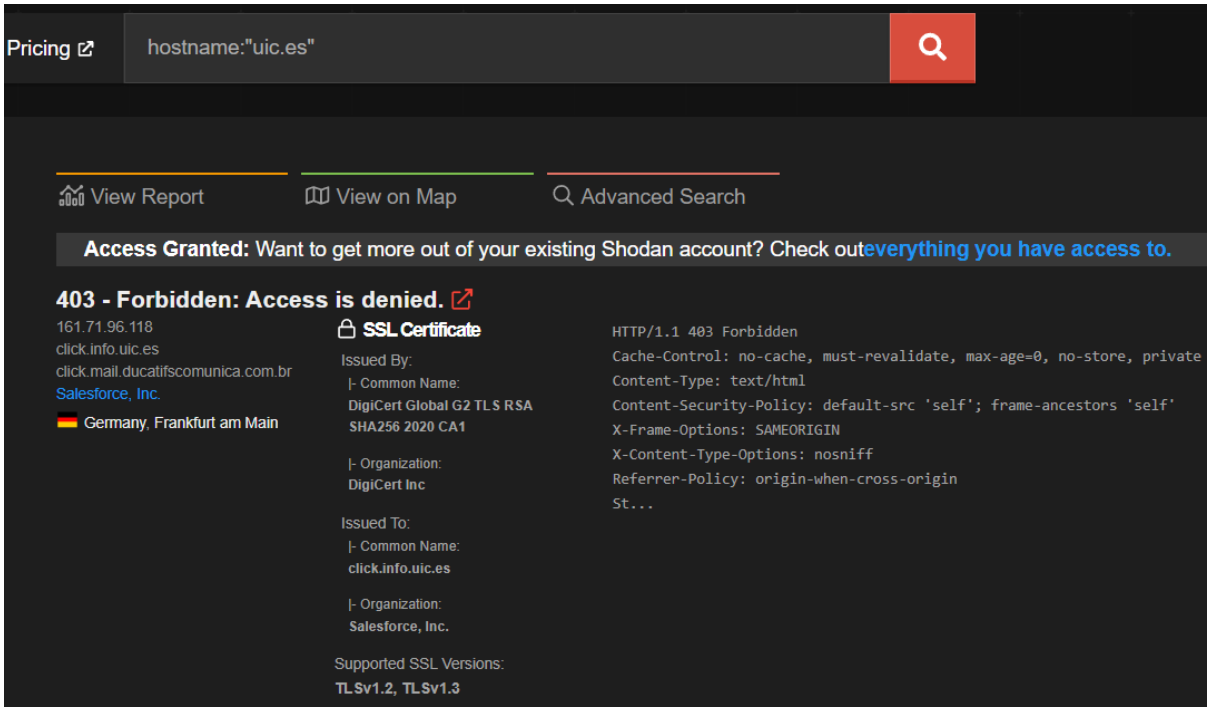
Regular View | Raw Data | Timeline | Whois

General Information

Hostnames	**ucm.es** www.coie.**ucm.es** www.ope.**ucm.es**
Domains	ucm.es
Country	**Spain**
City	**Madrid**
Organization	**Universidad Complutense de Madrid**
ISP	**Entidad Publica Empresarial Red.es**
ASN	**AS766**



2. Buscar *todos los dispositivos de la misma entidad*: `hostname:"uic.es" hostname:"unizar.es"`



FASE 3 — Conexión entre señales: seguir el rastro del xenomorfo

Objetivo: enlazar **un dispositivo concreto → el resto del ecosistema**.

Han encontrado una máquina sospechosa que transmite paquetes extraños. La misión es identificar **todo el entorno que la rodea**.

Cómo hacerlo:

1. Selecciona un dispositivo que hayas encontrado en Fase 1.
2. Observan:
    a. dominio
    b. ASN
    c. organización
    d. versión del servicio
3. Construyen una nueva búsqueda:

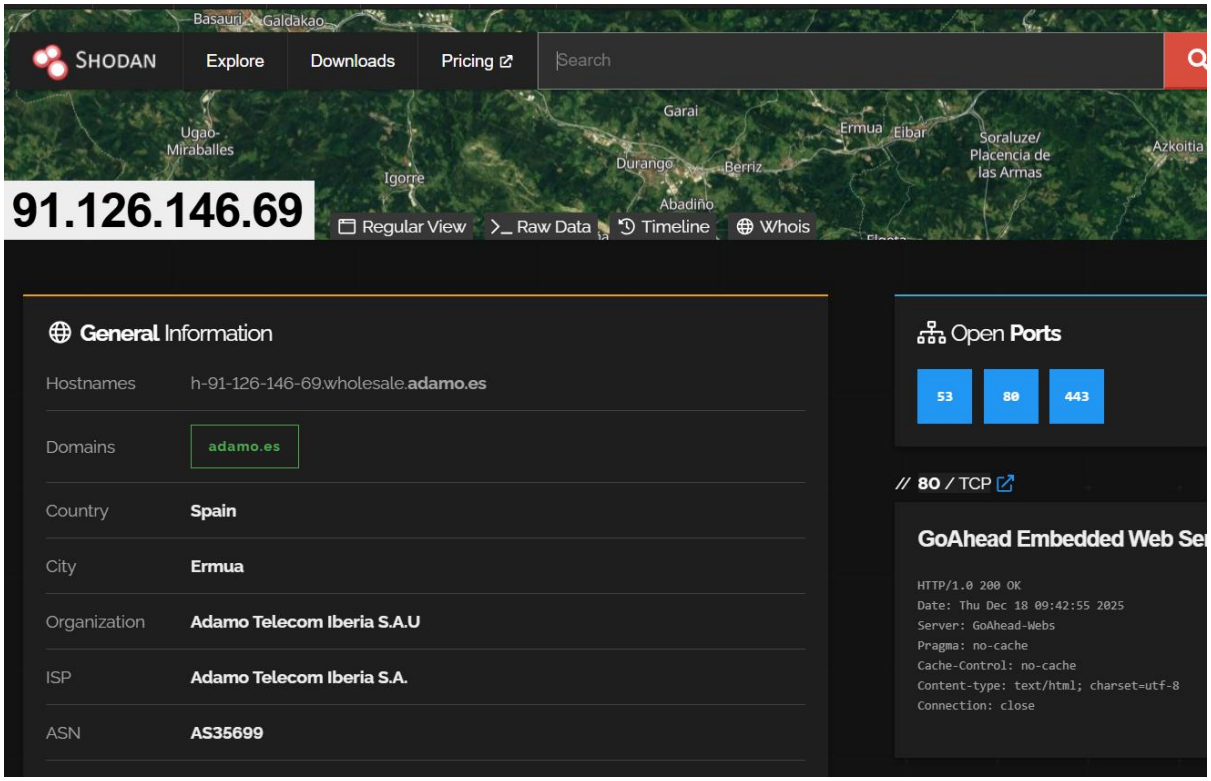
```
IP: 82.X.X.X
org: "Ayuntamiento de ___"
port 443 running nginx 1.18.0
```

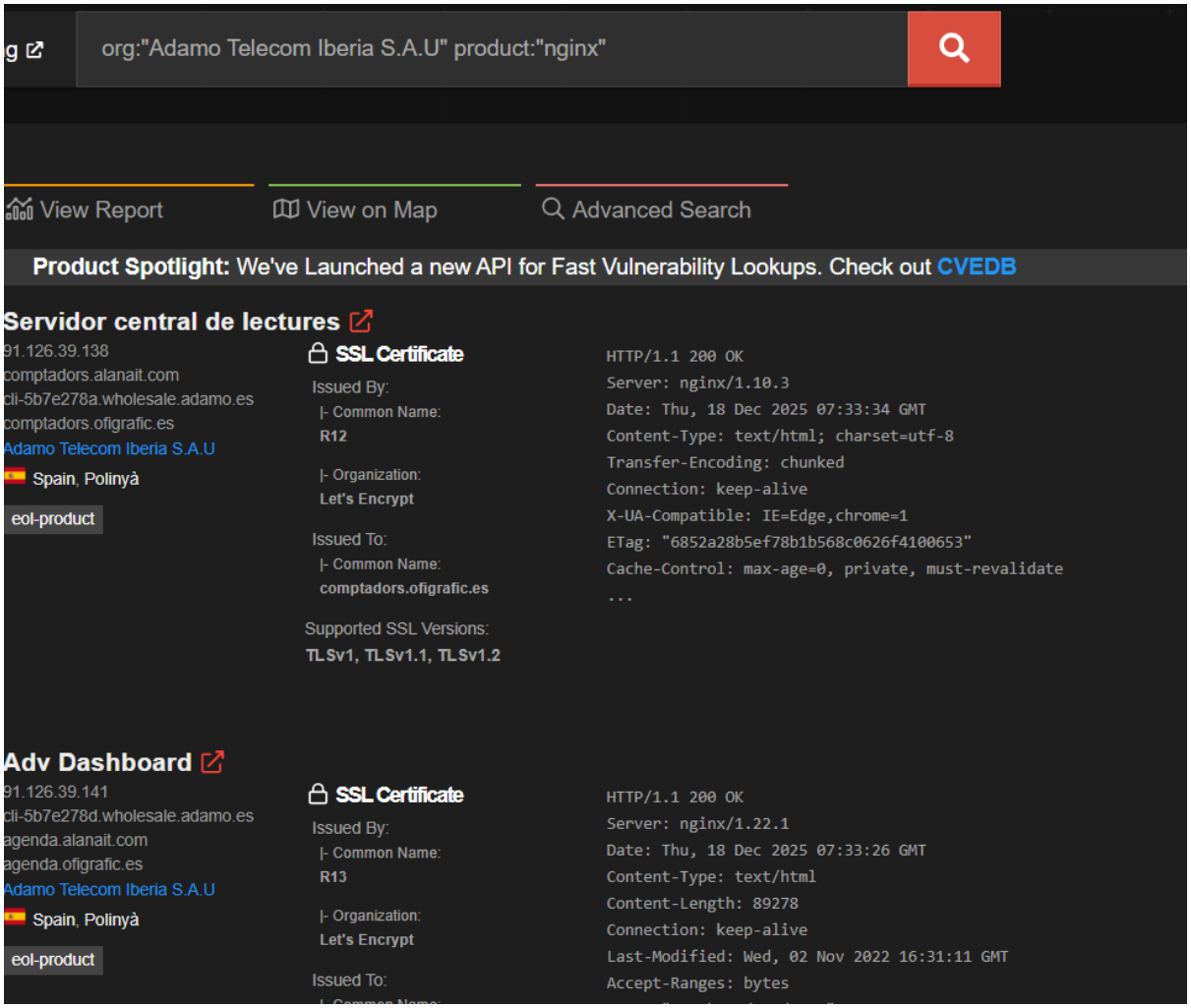
Entonces buscar:

```
org:"Ayuntamiento de ___"
product:"nginx"
```

O incluso por **ASN**:

```
asn:3352 (o el ASN que toque)
```


SHODAN
Explore
Downloads
Pricing
Search
91.126.146.69
Regular View
Raw Data
Timeline
Whois
General Information
Hostnames h-91-126-146-69.wholesale.adamo.es
Domains adamo.es
Country Spain
City Ermua
Organization Adamo Telecom Iberia S.A.U
ISP Adamo Telecom Iberia S.A.
ASN AS35699
Open Ports
53
80
443
// 80 / TCP
GoAhead Embedded Web Se
HTTP/1.0 200 OK
Date: Thu Dec 18 09:42:55 2025
Server: GoAhead-Webs
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html; charset=utf-8
Connection: close


org:"Adamo Telecom Iberia S.A.U" product:"nginx"
View Report
View on Map
Advanced Search
Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB
Servidor central de lectures
91.126.39.138
comptadors.alanait.com
cli-5b7e278a.wholesale.adamo.es
comptadors.ofigrafic.es
Adamo Telecom Iberia S.A.U
Spain, Polinyà
eol-product
SSL Certificate
Issued By:
|- Common Name:
R12
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
comptadors.ofigrafic.es
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 18 Dec 2025 07:33:34 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-UA-Compatible: IE=Edge,chrome=1
ETag: "6852a28b5ef78b1b568c0626f4100653"
Cache-Control: max-age=0, private, must-revalidate
...
Adv Dashboard
91.126.39.141
cli-5b7e278d.wholesale.adamo.es
agenda.alanait.com
agenda.ofigrafic.es
Adamo Telecom Iberia S.A.U
Spain, Polinyà
eol-product
SSL Certificate
Issued By:
|- Common Name:
R13
|- Organization:
Let's Encrypt
Issued To:
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Thu, 18 Dec 2025 07:33:26 GMT
Content-Type: text/html
Content-Length: 89278
Connection: keep-alive
Last-Modified: Wed, 02 Nov 2022 16:31:11 GMT
Accept-Ranges: bytes