/RootedCON

PROTAAPP

¡ATTACK SURFACE MANAGEMENT

DIY for free!

Miguel de la Cal Bravo
Félix Paniagua Mérida

External Attack Surface Management: DIY for free!

Miguel de la Cal Bravo
Félix Paniagua Mérida

8 de marzo de 2024

/RootedCON x PROTAAPP

Agenda

1. Introducción
2. Necesidades y objetivos
3. Inventario de activos
4. Tecnologías y herramientas
5. Demostración y ejemplos
6. Futuras mejoras

1. Introducción

1. Introducción

01

External ASM (Attack Surface Management)

Exploración de la superficie expuesta en Internet de una organización (activos, tecnologías, servicios, versiones, …)

02

DIY (Do It Yourself)

- Organizaciones con pocos recursos
- *“La imaginación al poder.”*
- Desarrollo “sencillo”, con scripting en Python y otras utilidades

03

For free!

Herramientas y utilidades gratuitas

2. Necesidades y objetivos

2. Necesidades y objetivos

Esquema Nacional de Seguridad (RD 311/2022)

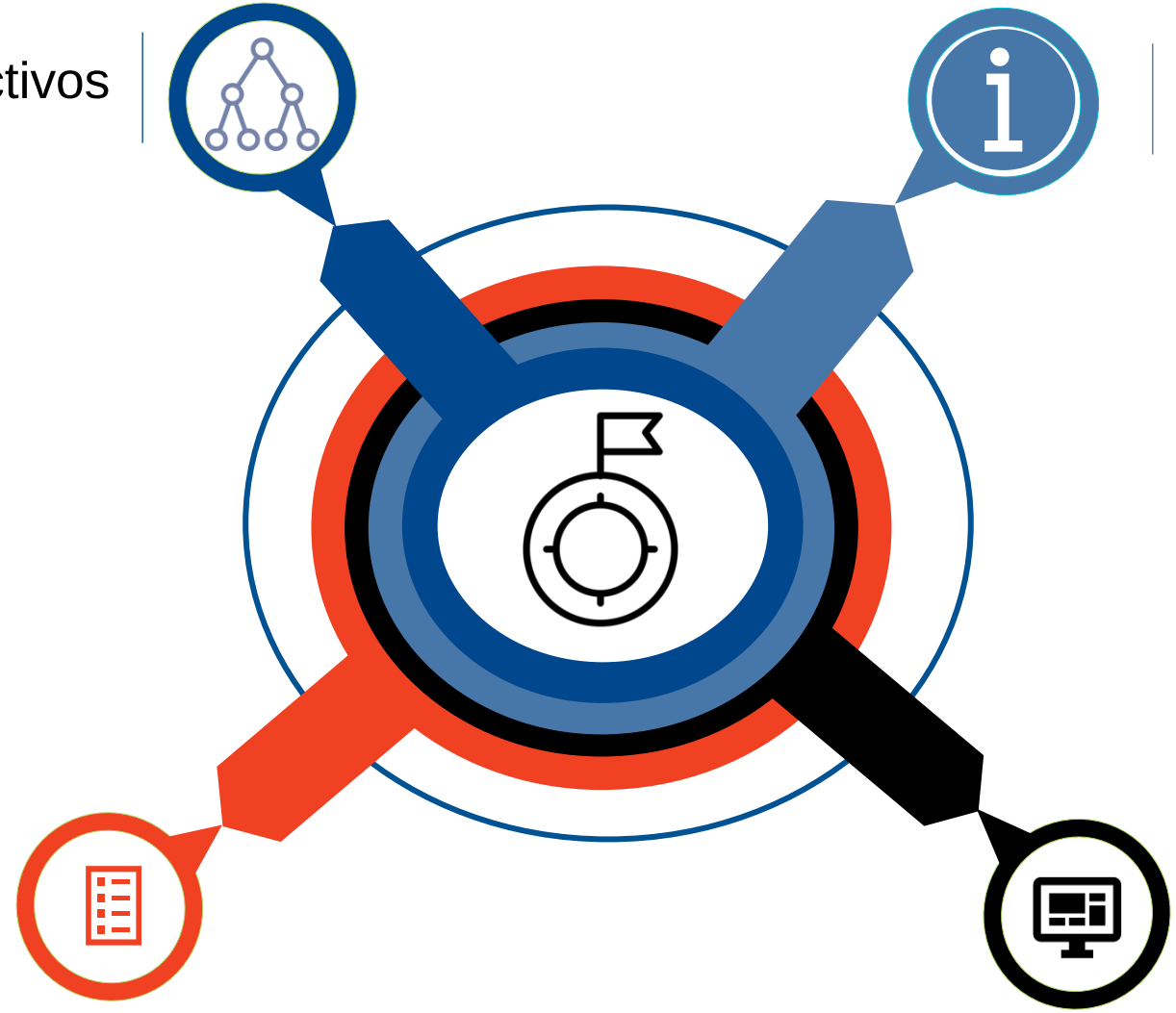
- **Artículo 8. Prevención, detección, respuesta y conservación**
  - *"2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse"*

- **Nuevo principio básico**
  - Art. 10. Vigilancia continua y reevaluación periódica

2. Necesidades y objetivos

Activos

Recopilar tecnologías y servicios



Análisis y reducción de la exposición

Dashboard

3. Inventario de activos

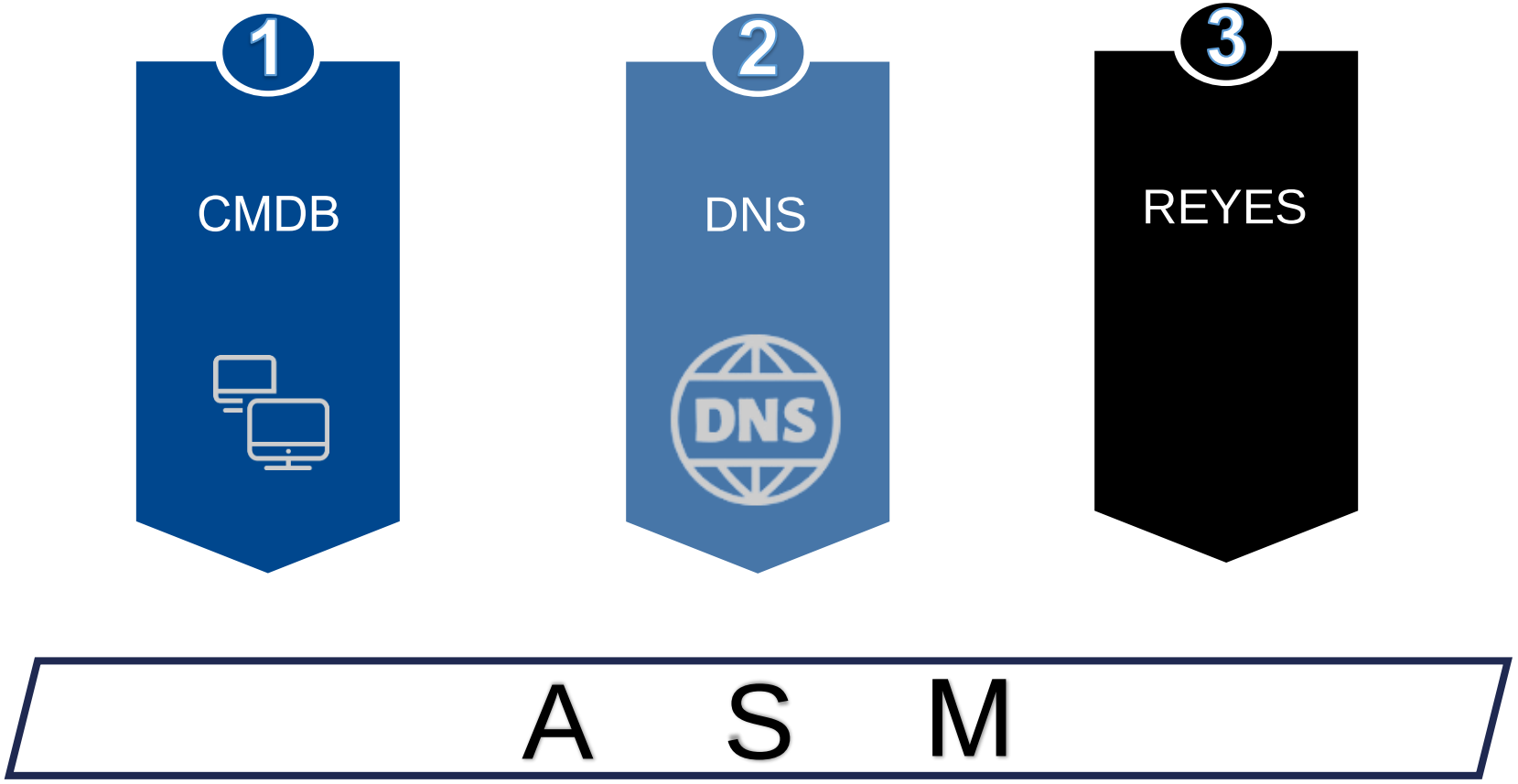
3. Inventario de activos

🔎 Búsqueda de dominios y subdominios (pasivas/activas)

- Crt.sh
- DNSDumpster
- OWASP Amass
- SecurityTrails
- Sublist3r
- ViewDNS.info
- Google Dorks:
  - *site:*.dominio.es filetype:…*

3. Inventario de activos

Fuentes internas



4. Tecnologías y herramientas

4. Tecnologías y herramientas

🔎 Recopilación de información

Direcciones IP

Activo (SÍ/NO)

¿HTTP/S?

Certificados: emisor, fecha de validez, nº serie, versión TLS

Tecnologías y versiones

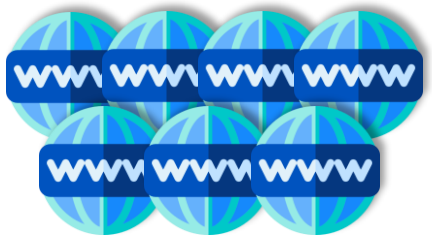
Otros: códigos de estado, agrupar por dominios, TLD

4. Tecnologías y herramientas

🛠 Herramientas

Scripting en Python

Librerías: DNS, requests, ssl, re, socket, datetime, pytz, json, ...




```
{
  ¿está activa?: “true”,
  ¿HTTP/S?: “true”,
  Tecnologías: “x”,
  Versiones: “y”,
  …
}
```

WebAnalyzer: https://github.com/webanalyzer/webanalyzer.py

WebAnalyzer (rules): https://github.com/webanalyzer/rules

4. Tecnologías y herramientas

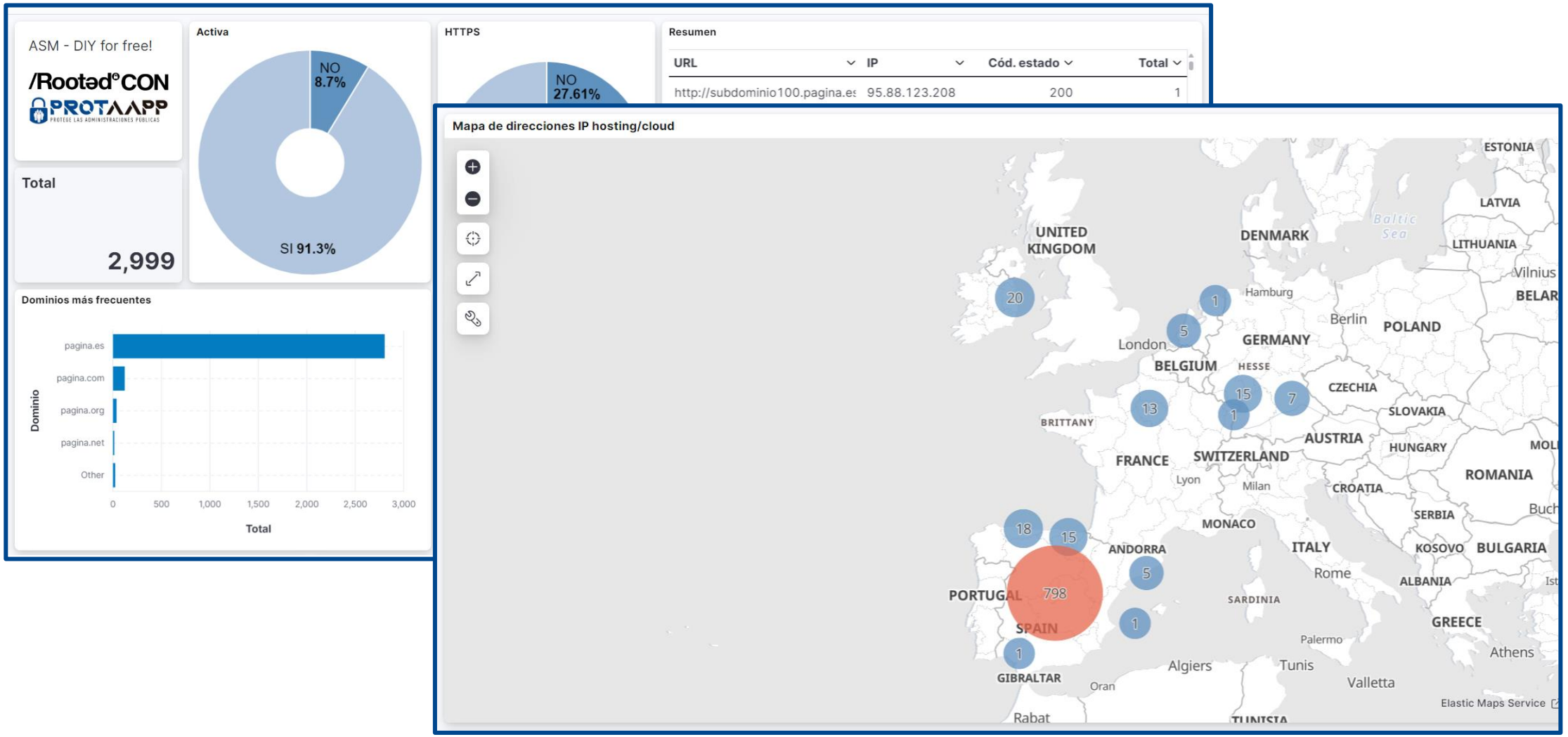
📈 Cuadro de mandos interactivo (aplicación web)

- Utilización del stack de **Elastic – ELK** (open source)

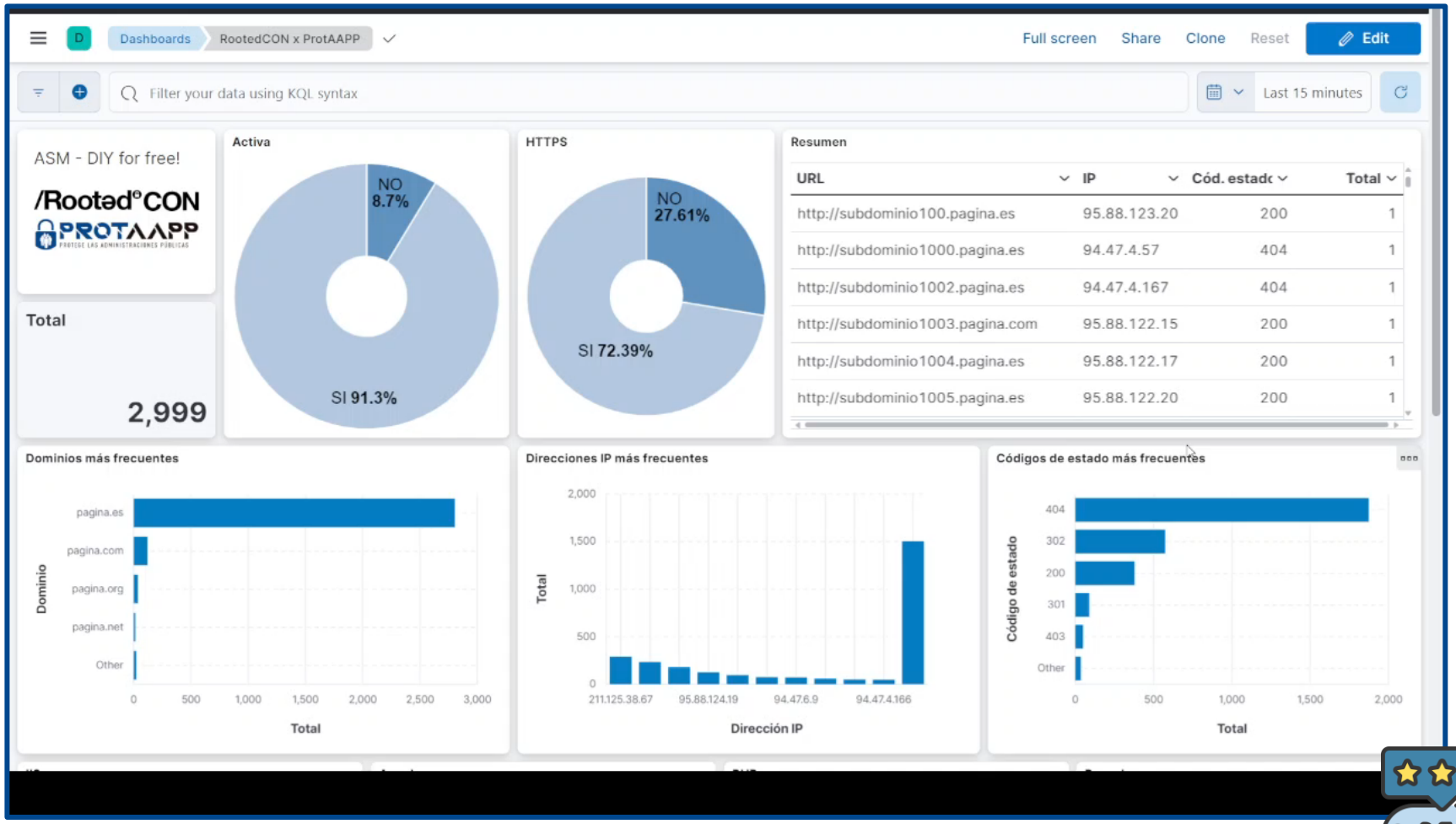
- Herramientas:
  - **Logstash**: ingesta de datos y procesamiento de **JSON**
  - **Elasticsearch**: indexado y almacenamiento de datos
  - **Kibana**: interfaz gráfica, cuadro de mandos

5. Demostración y ejemplos

5. Demostración y ejemplos

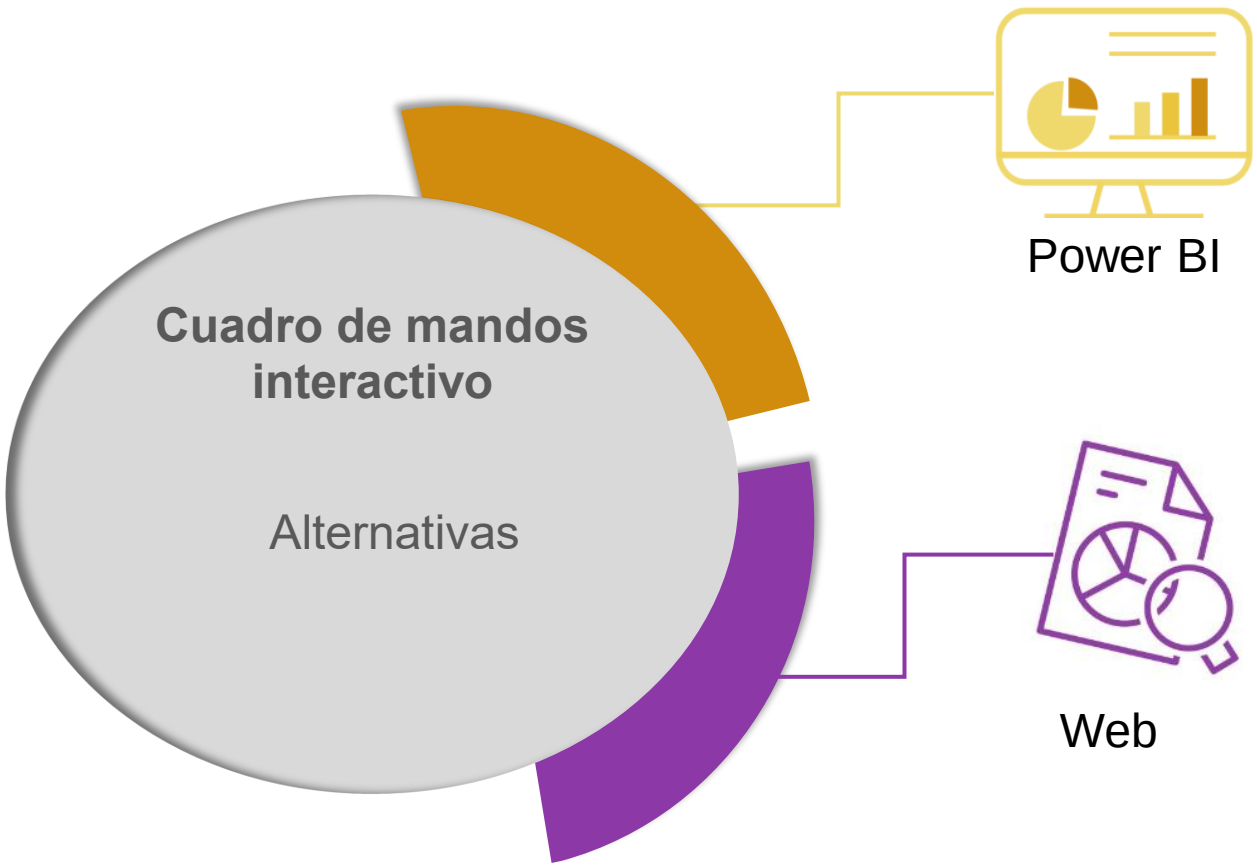


5. Demostración y ejemplos

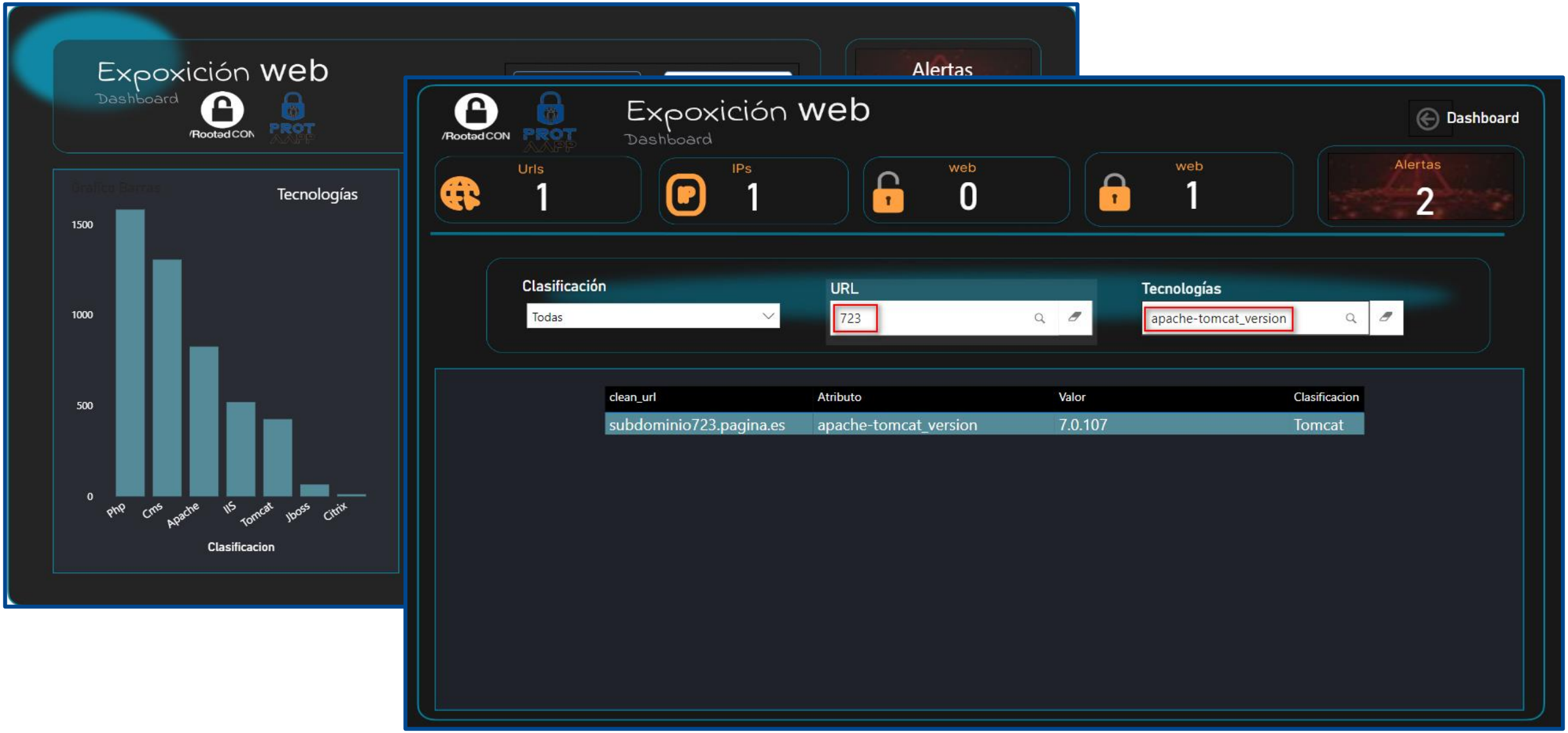


6. Futuras mejoras

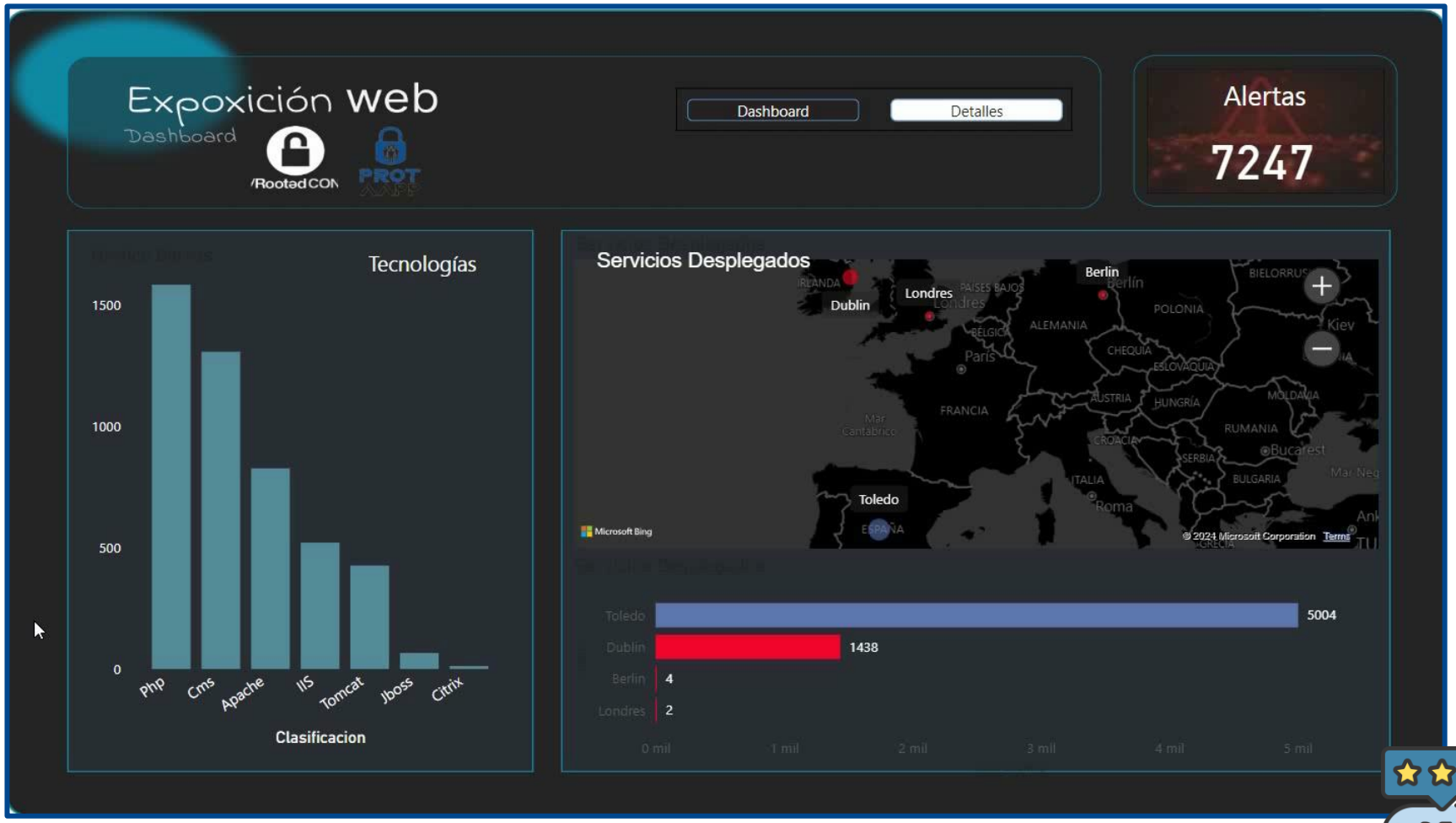
6. Futuras mejoras



6. Futuras mejoras



6. Futuras mejoras



6. Futuras mejoras

6. Futuras mejoras

➡ SOON Mejoras y algunas limitaciones:

- Detección automática de **nuevos dominios**/subdominios
  - *¡OJO al ruido! Comprobar si los activos nos pertenecen*
- Obtención de **vulnerabilidades**
  - *¡OJO a los falsos positivos!*
- **Scoring**/puntuación de **riesgo** de los activos
  - *No es tan fácil de determinar*

External Attack Surface Management: DIY for free!

Miguel de la Cal Bravo
Félix Paniagua Mérida

8 de marzo de 2024

/RootedCON x PROTAAPP