

# SecDevOps(**DevSecOps**) con contenedores en los dockers V3

By **Antonio Juanilla**(Specter)



# \$Whoami

## Antonio Juanilla

- Autodidacta.
- Desarrollador de software.
- Amante del hacking y la seguridad en los ratos libres.
- Amante de la tecnología.
- Defensor de la democratización de la tecnología para la mejora de la sociedad.
- Twitter: **@spectertj**
- Linkendin: <https://www.linkedin.com/in/spectertj>
- Github: **spectertj**



**Sólo el conocimiento nos hace libres**



<https://hackmadrid.org>

<https://twitter.com/hackmadrid>

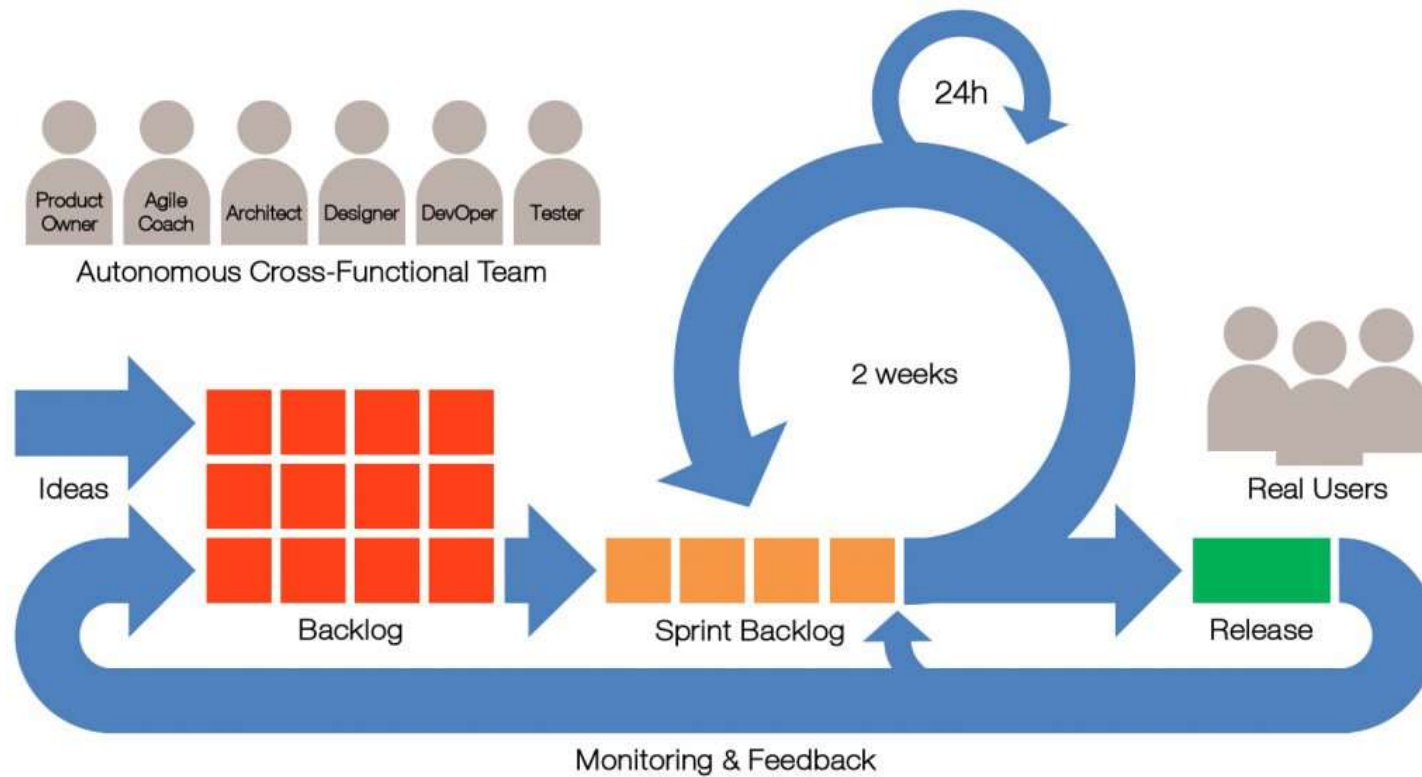


Telegram: [t.me/hackmadrid](https://t.me/hackmadrid)

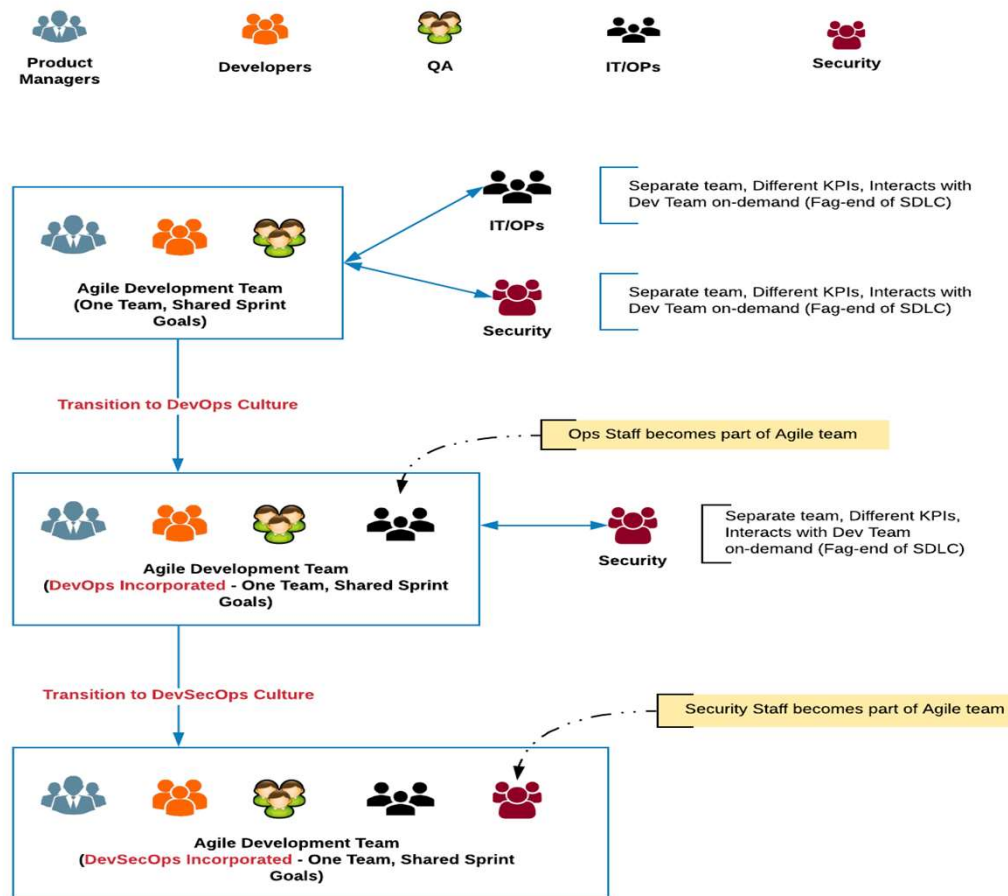
<https://meetup.com/HackMadrid-27>

<https://linkedin.com/company/hackmadrid>

# Flujo del agilismo



# Transición





Sec – Dev – Ops  
Dev – Sec – Ops

## SECURITY

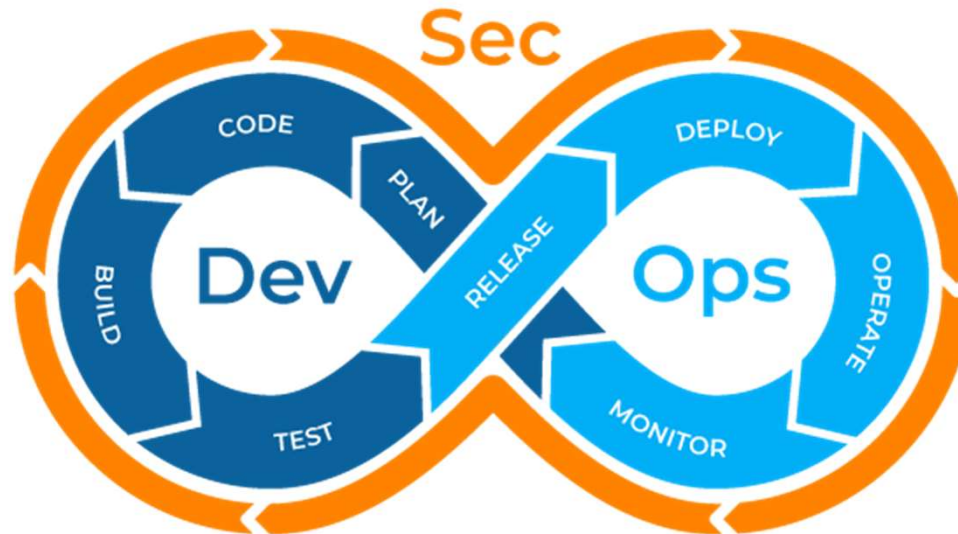
Seguridad en el desarrollo de aplicaciones y en los entornos de desarrollo y despliegue

## DEVELOPMENT

Desarrollo de aplicaciones

## OPERATIONS

Orquestación del despliegue de aplicaciones, configuración de entornos, monitorización de las aplicaciones y los entornos



# Desarrollo Seguro

## Seguridad de principio a fin

1. Owasp **top 10** son una lista que contiene el top 10 de vulnerabilidades en aplicaciones web.
2. Validaciones de datos de entrada.
3. Validaciones de datos de salida.
4. Validaciones de llamadas a **BBDD**.
5. Escaneo de código fuente para encontrar vulnerabilidades
6. Escaneo de código para calidad.
7. Pruebas y mas pruebas.





# Tipos de Test

1. Pruebas unitarias.
2. Pruebas de integración.
3. Pruebas de regresión.



# Cultura Devops y Contenerizacion



# CONTAINERIZATION VIRTUALIZATION

## Containers

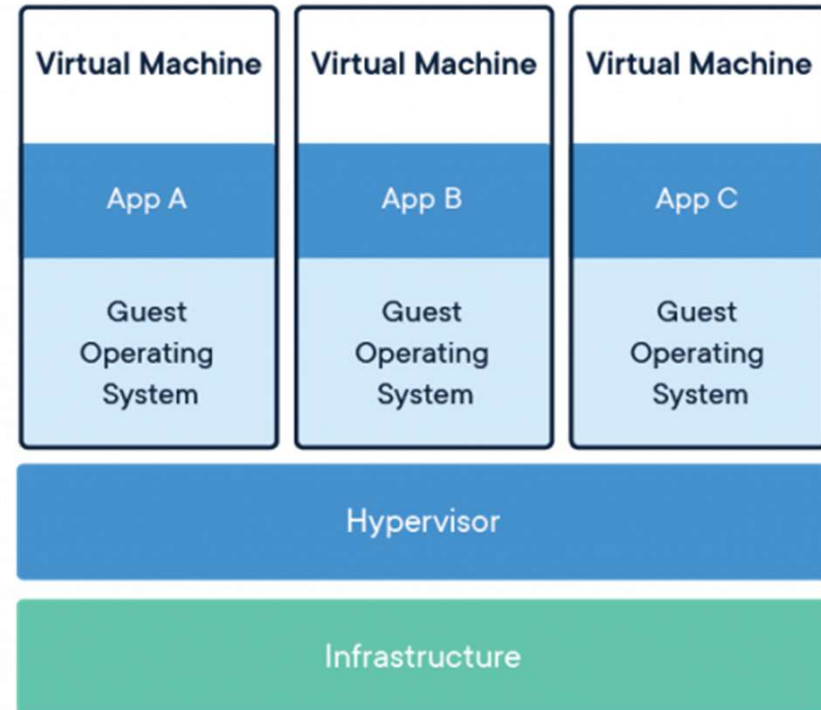
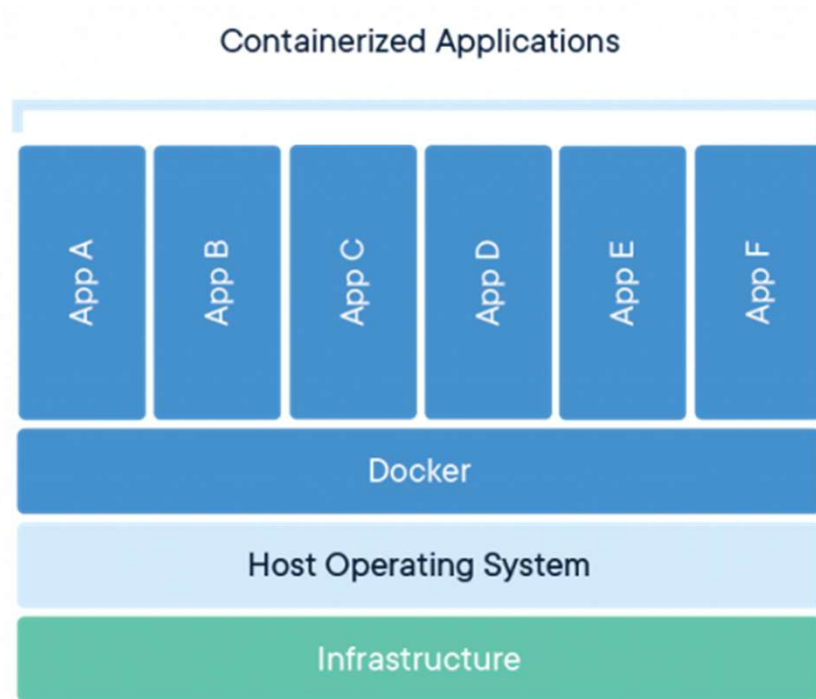
- Dockers
- LxC

VS

## VM

- VmWare
- VirtualBox
- HyperV





# Beneficios de los Contenedores

1. Multi plataforma en la **nube**
2. Comparte el mismo **OS**.
3. Velocidad.
4. Costes de eficiencia.
5. Portabilidad.
6. Pruebas y **CI-CD**.







# Desventajas de los Contenedores

1. Seguridad.
2. Falta de aislamiento.
3. Monitorización.



# Securizando Dockers

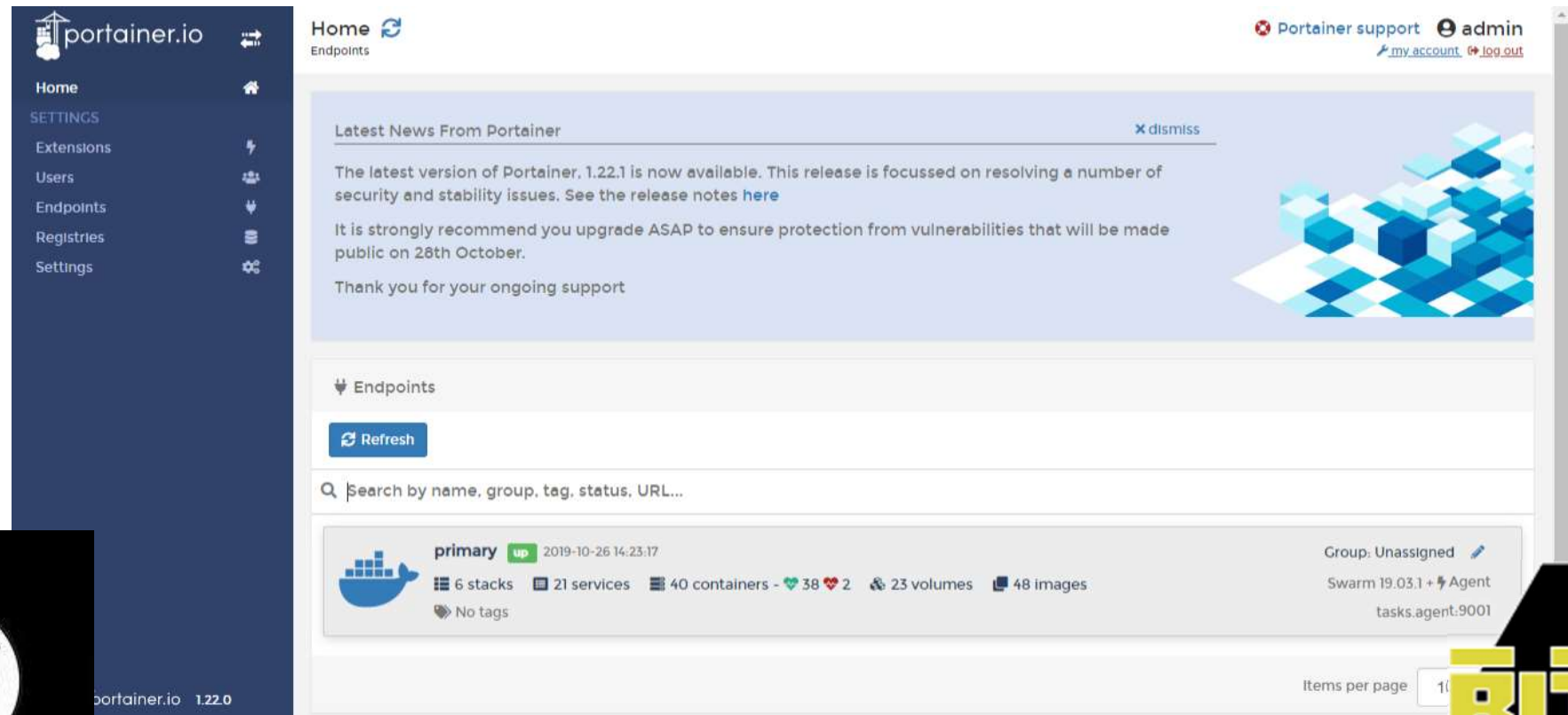


# Herramientas para Contenedores

1. Google Kubernetes Engine(**GKE**).
2. Portainer.
3. AWS **EKS**.
4. Azure Kubernetes Services(**AKS**).
5. Docker **Swarm**.
6. Swarmpit



# Herramientas para Contenedores



The screenshot displays the Portainer.io web interface. On the left is a dark blue sidebar with the Portainer.io logo and a menu containing: Home, SETTINGS, Extensions, Users, Endpoints, Registries, and Settings. The main content area is titled 'Home Endpoints' and features a 'Latest News From Portainer' banner. The banner text states: 'The latest version of Portainer, 1.22.1 is now available. This release is focussed on resolving a number of security and stability issues. See the release notes [here](#). It is strongly recommend you upgrade ASAP to ensure protection from vulnerabilities that will be made public on 28th October. Thank you for your ongoing support'. Below the banner is a section for 'Endpoints' with a 'Refresh' button and a search bar labeled 'Search by name, group, tag, status, URL...'. A single endpoint is listed: 'primary' (status: up, timestamp: 2019-10-26 14:23:17). Its statistics are: 6 stacks, 21 services, 40 containers (38 green hearts, 2 red hearts), 23 volumes, and 48 images. It has 'No tags'. The endpoint is 'Group: Unassigned', running 'Swarm 19.03.1' with 'Agent tasks.agent:9001'. The bottom right of the interface shows 'Items per page' set to 10.



# Recomendaciones de Seguridad

1. Securizar el host.
2. Incorporar proxy inversos.
3. Incorporar balanceadores de carga.
4. Uso de certificados **SSL/TLS**.
5. Forzar **Https**.
6. Herramientas contra ataques **DoS**.
7. Uso de WAF (**Web Applications Firewall**) si es aplicación web.
8. Pruebas de carga.
9. Usar **Dockerfile** y forjar imágenes propias.
10. Verificar el uso de imágenes **Docker** publicas.



# Recomendaciones de Seguridad

✓ **Your SSL/TLS encryption mode is Full**  
This setting was last changed a few seconds ago



☐ Off (not secure) ⓘ  
No encryption applied

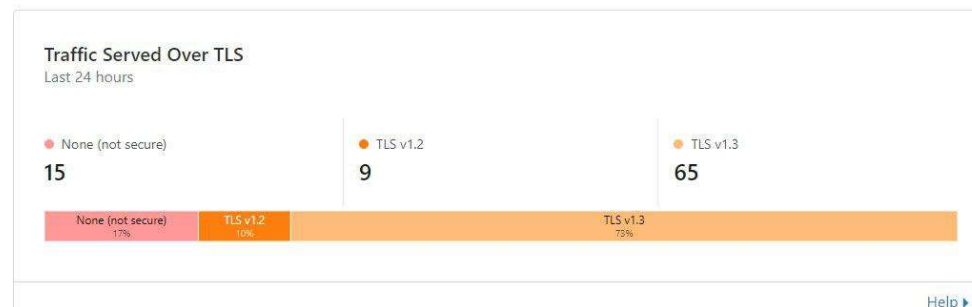
☐ Flexible  
Encrypts traffic between the browser and Cloudflare

☒ **Full**  
Encrypts end-to-end, using a self signed certificate on the server

☐ Full (strict)  
Encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server

[Learn more about End-to-end encryption with Cloudflare](#)

[API ▶](#) [Help ▶](#)





# Recomendaciones de Seguridad

<b>Always Use HTTPS</b> Redirect all requests with scheme "http" to "https". This applies to all http requests to the zone. <small>This setting was last changed 3 months ago</small>	<input checked="" type="checkbox"/> On
<a href="#">API</a> <a href="#">Help</a>	
<b>HTTP Strict Transport Security (HSTS)</b> Enforce web security policy for your website. Status: On Max-Age: 6 months (Recommended) Include subdomains: On Preload: Off <small>This setting was last changed a month ago</small>	<a href="#">Change HSTS Settings</a>
<a href="#">API</a> <a href="#">Help</a>	
<b>Minimum TLS Version</b> Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.	<input type="text" value="TLS 1.2"/>
<a href="#">API</a> <a href="#">Help</a>	

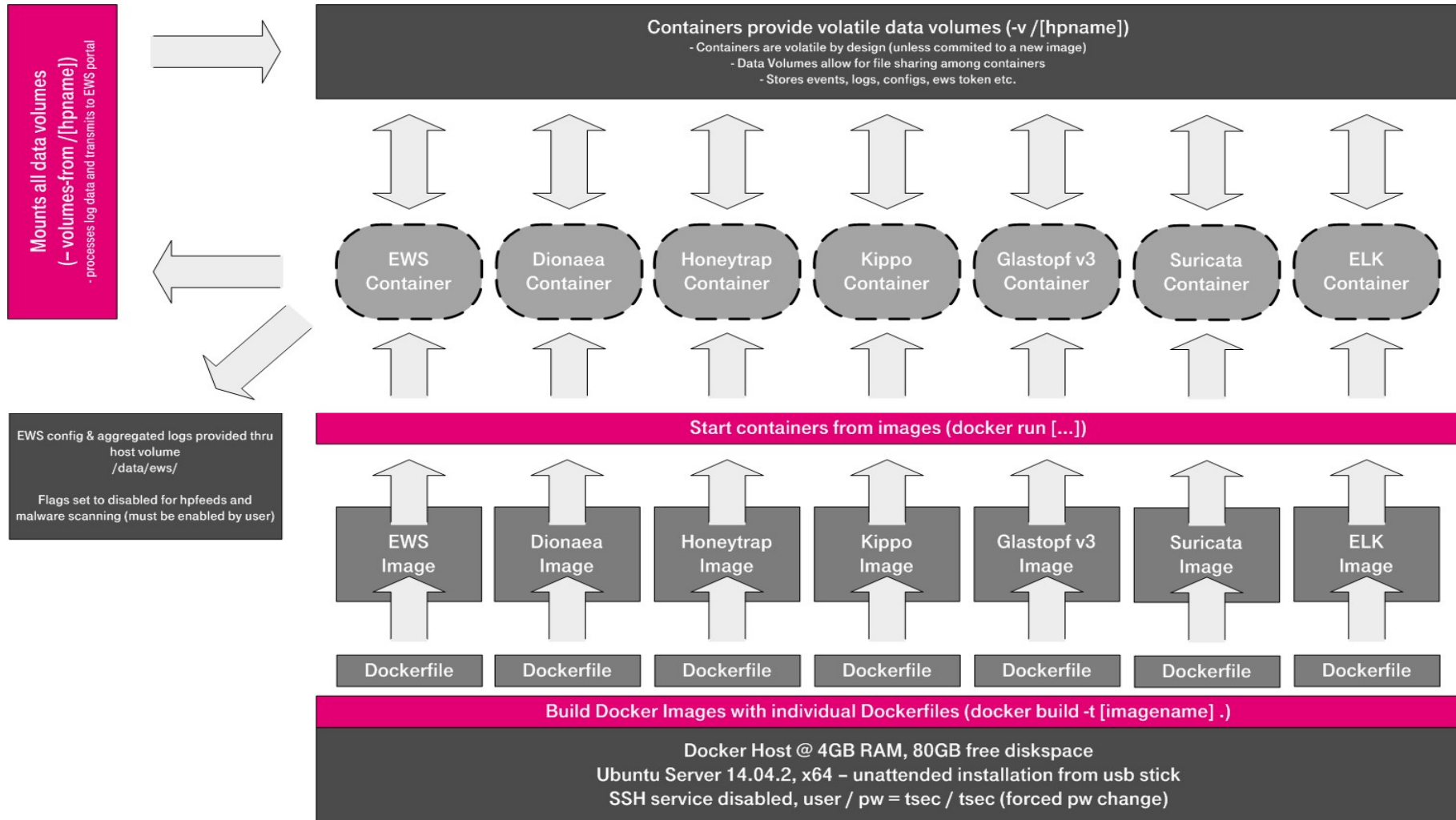


# Recomendaciones de Seguridad

CLOUDFLARE ciberinteligencia-osintlatinoamerica.com

Type	Name	Content	TTL	Proxy status
A	alertmanager	[REDACTED]	Auto	Proxied
A	ciberinteligencia-osintlatin...	[REDACTED]	Auto	Proxied
A	consul	[REDACTED]	Auto	Proxied
A	dev	[REDACTED]	Auto	Proxied
A	docker	[REDACTED]	Auto	Proxied
A	ftpresources	[REDACTED]	Auto	Proxied
A	grafana	[REDACTED]	Auto	Proxied
A	leader	[REDACTED]	Auto	Proxied
A	m	[REDACTED]	Auto	Proxied
A	portainer	[REDACTED]	Auto	Proxied
A	pre	[REDACTED]	Auto	Proxied
A	prometheus	[REDACTED]	Auto	Proxied
A	sonar	[REDACTED]	Auto	Proxied
A	swarm	[REDACTED]	Auto	Proxied
A	traefik	[REDACTED]	Auto	Proxied
A	unsee	[REDACTED]	Auto	Proxied
A	worker	[REDACTED]	Auto	Proxied
CNAME	www	ciberinteligencia-osintlatinoameric...	Auto	Proxied







# Herramientas

1. <https://www.ssllabs.com/ssltest/>
2. <https://mozilla.github.io/server-side-tls/ssl-config-generator/>
3. <https://www.cisecurity.org/cis-benchmarks/>
4. <https://www.cisecurity.org/benchmark/docker/>
5. [https://www.owasp.org/index.php/OWASP\\_WAP-Web\\_Application\\_Protection](https://www.owasp.org/index.php/OWASP_WAP-Web_Application_Protection)
6. <https://github.com/red-panda-ci/red-panda-ci-symfony>
7. <https://github.com/red-panda-ci/red-panda-ci-symfony/tree/master/ci-scripts/test/cucumber>
8. <https://www.cloudflare.com>
9. <https://hub.docker.com/r/chef/inspec/>
10. [https://www.owasp.org/index.php/OWASP\\_Dependency\\_Track\\_Project](https://www.owasp.org/index.php/OWASP_Dependency_Track_Project)
11. <https://observatory.mozilla.org/>
12. <https://github.com/zaproxy/zaproxy/wiki/ZAP-Baseline-Scan>
13. <https://github.com/coreos/clair>



# Referencias

<https://github.com/sergioortegagomez>

<https://github.com/pedroamador>

<https://medium.com/guayoyo>

<https://medium.com/guayoyo/hardening-fortaleciendo-ssh-ab3270e06661>

<https://medium.com/guayoyo/hardening-mejorando-configuraciones-ssl-tls-51d6a8bfb564>

<https://medium.com/guayoyo/asegurando-las-cabeceras-de-respuestas-http-en-servidores-web-apache-y-nginx-2f71e62ffda4>

<https://github.com/Spectertj>





## Eventos Fijos

**Jacqueando Kañas**

**Primer Martes de cada Mes**

**Beer Bang Madrid**  
**Mercado de La Guindalera**  
**Calle Eraso 14, 28028 Madrid**

**Hacking Hardware HackLab**

**Primer Sábado de cada mes**

**La Nave de Madrid**  
**Aula 7**





HACKMADRID

%27



**Gracias.....**