SECDEVOPS(DEVSECOPS) CON CONTENEDORES EN LOS DOCKERS

BY ANTONIO JUANILLA(SPECTER)

¿QUIEN SOY?

- Autodidacta
- Procactivo
- 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
HACKMADRID
%27

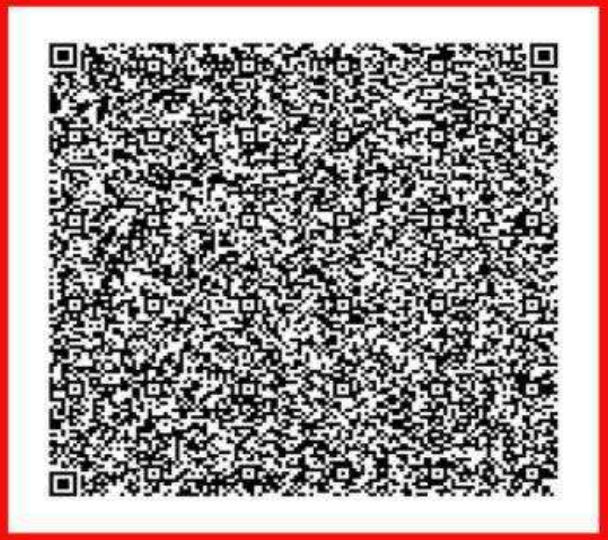
https://hackmadrid.org

https://twitter.com/hackmadrid

Telegram: t.me/hackmadrid

https://meetup.com/HackMadrid-27

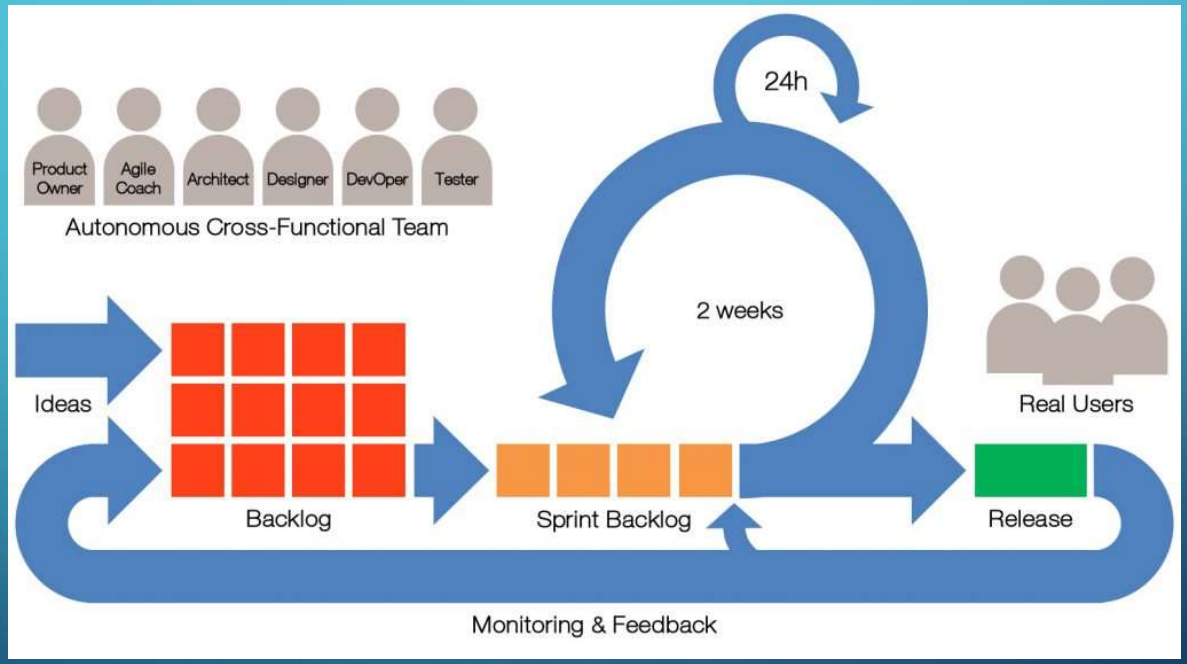
https://linkedin.com/company/hackmadrid



HACKMADRID

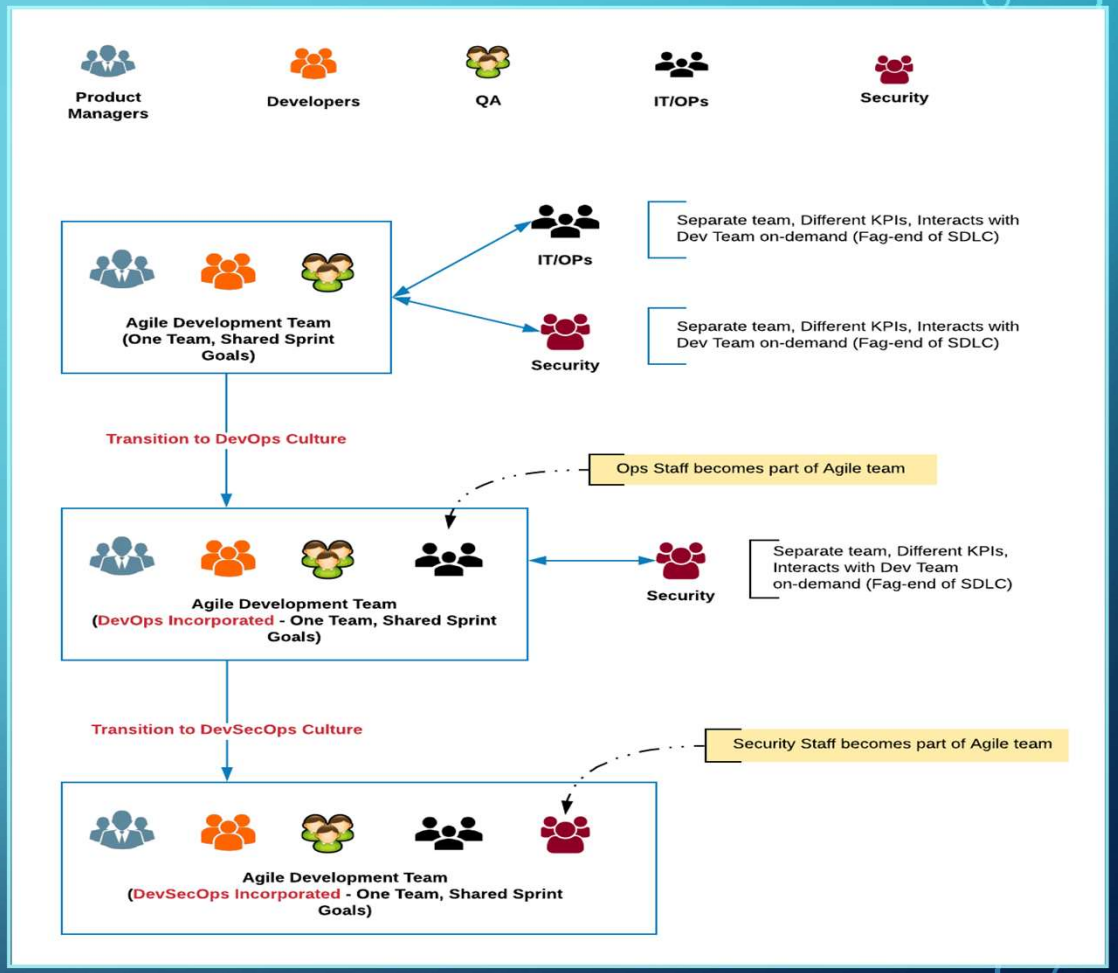
%27

FLUJO DEL AGILISMO



TRANSICIÓN

1. Equipos de desarrollo
2. Equipos DevOps
3. Equipos SecDevOps



SEC – DEV – OPS

SECURITY

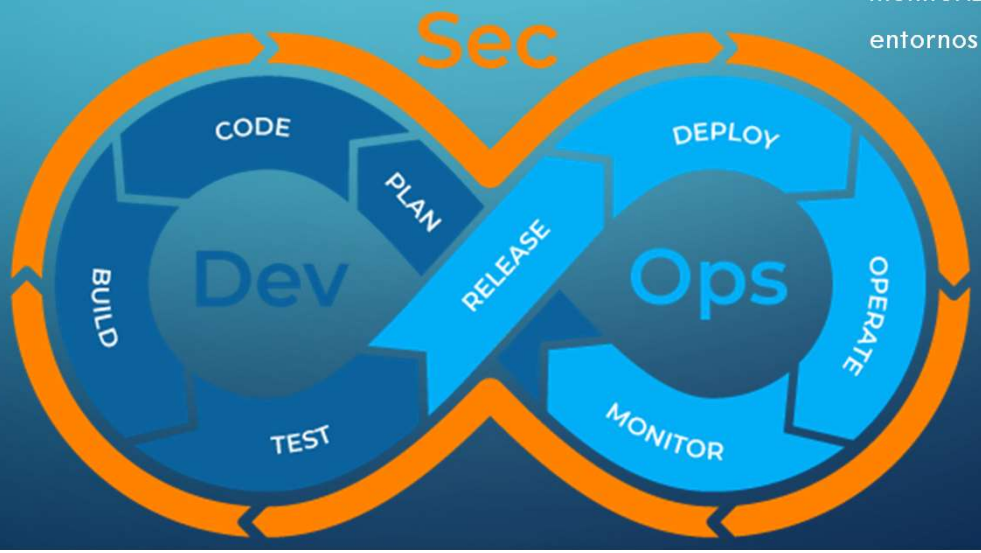
Seguridad en el desarrollo de aplicaciones y en los entornos de desarrollo y despliegue

DEVELOPMENT

Desarrollo de aplicaciones

OPERATIONS

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



DESARROLLO SEGURO

1. VALIDACIONES DE DATOS DE ENTRADA
2. VALIDACIONES DE DATOS DE SALIDA
3. VALIDACIONES DE LLAMADAS A BBDD
4. ESCANEO DE CÓDIGO FUENTE PARA ENCONTRAR VULNERABILIDADES
5. ESCANEO DE CÓDIGO PARA CALIDAD
6. PRUEBAS Y MAS PRUEBAS

TIPOS DE TEST

1. PRUEBAS UNITARIAS
2. PRUEBAS DE INTEGRACIÓN
3. PRUEBAS DE REGRESIÓN

CULTURA DEVOPS Y CONTENERIZACION

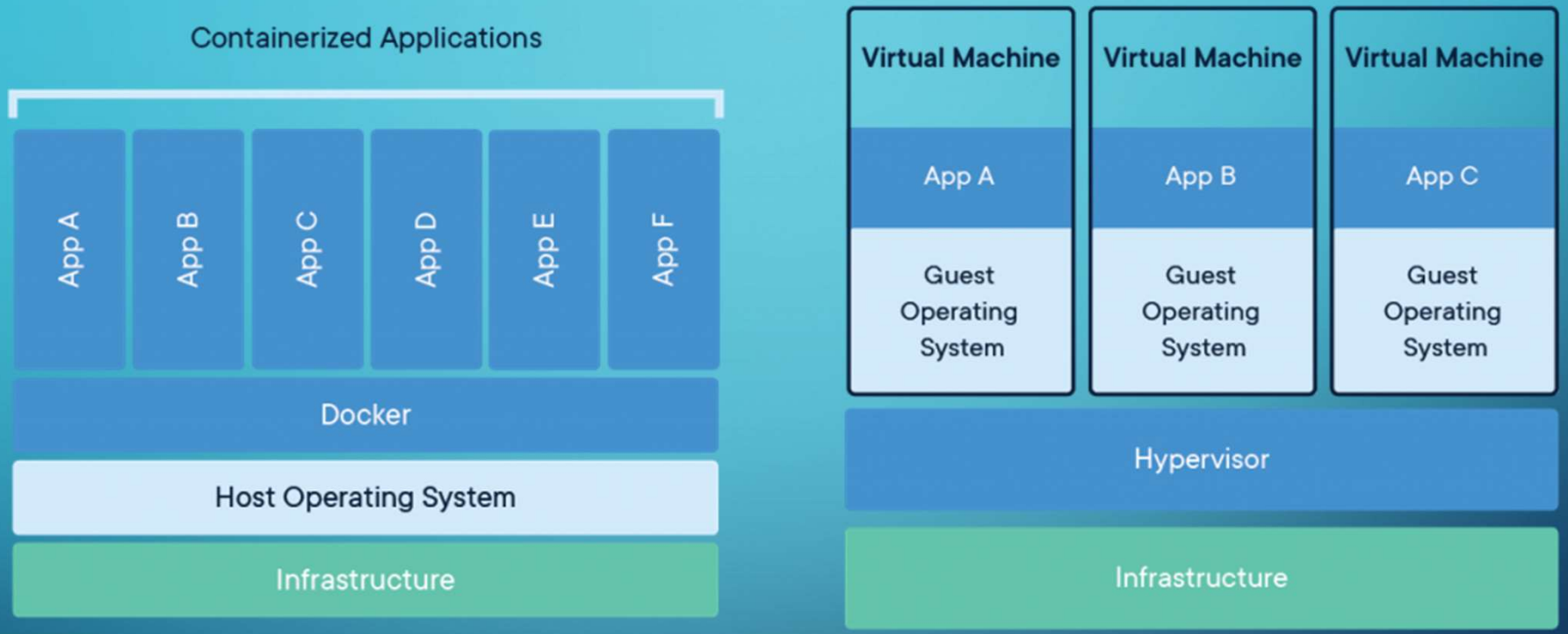
CONTAINERIZATION VS. VIRTUALIZATION

CONTAINERS

- Dockers
- LxC

VM

- VmWare
- VirtualBox
- HyperV


Containerized Applications
App A
App B
App C
App D
App E
App F
Docker
Host Operating System
Infrastructure
Virtual Machine
Virtual Machine
Virtual Machine
App A
App B
App C
Guest Operating System
Guest Operating System
Guest Operating System
Hypervisor
Infrastructure

BENEFICIOS DE LOS CONTENEDORES

- Multi plataforma en la nube
- Comparte el mismo OS
- Velocidad
- Costes de eficiencia
- Versionado
- Portabilidad
- Pruebas y **CI-CD**


Build, Ship, Run, Any App Anywhere
From Dev
To Ops
Any App
ASP.NET
.NET
Java
MORE
CONTAINERIZATION ENGINE
Any OS
Windows
Linux
Anywhere
Physical
Virtual
Cloud

DESVENTAJAS DE LOS CONTENEDORES

- Seguridad
- Falta de aislamiento
- Monitorización

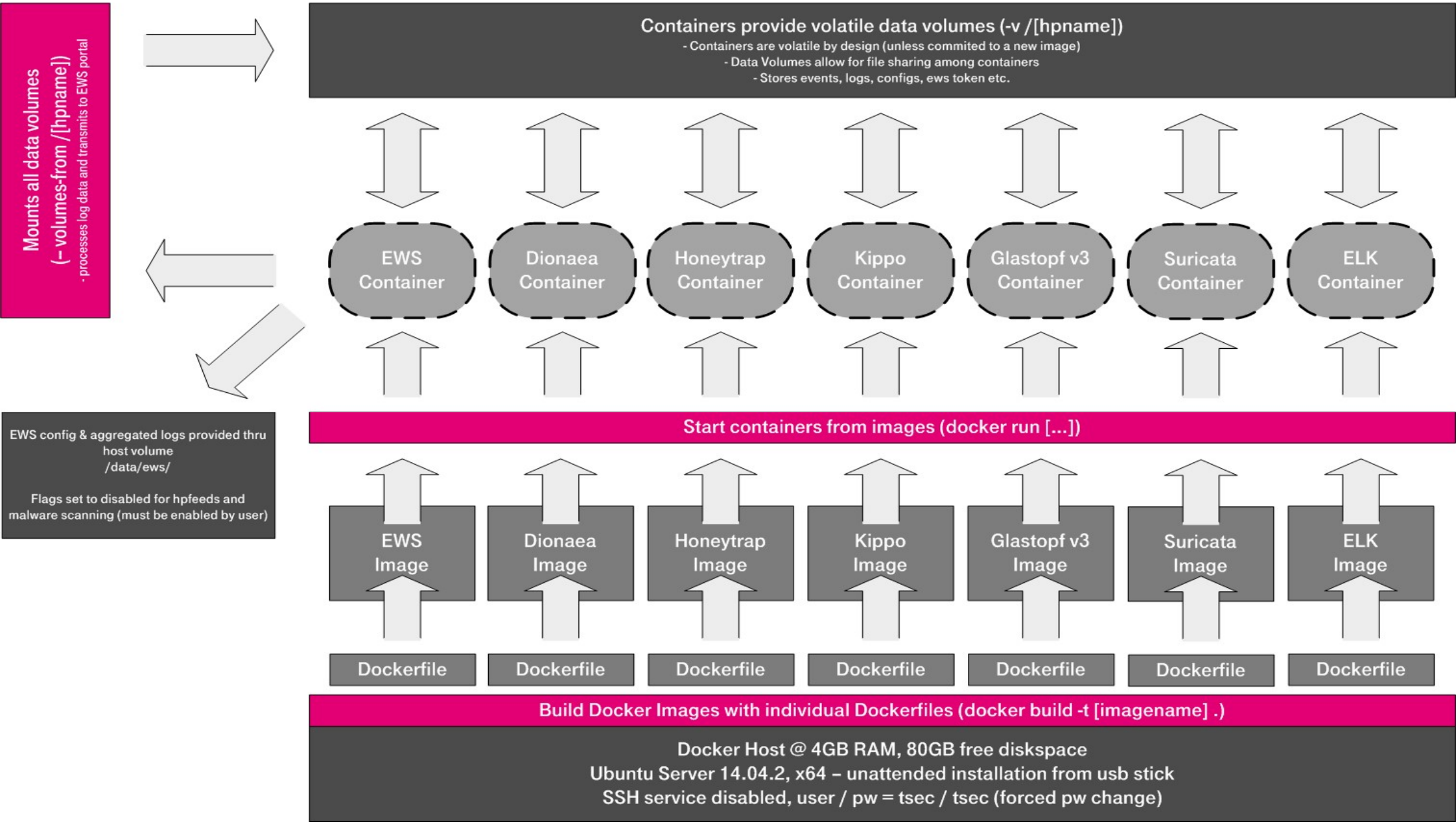
SECURIZANDO DOCKERS

PLATAFORMAS DE CONTENEDORES

- Google Kubernetes Engine
- CoreOS'rkt (Rocket)
- Portainer
- AWS ECR
- Azure Kubernetes Service
- Swarm
- Marathon
- Hashicorp Nomad
- Open Stack Magnum

RECOMENDACIONES DE SEGURIDAD

- Securizar el host
- Incorporar proxy inversos
- Incorporar balanceadores de carga
- Uso de certificados ssl/tls
- Forzar https
- Herramientas contra ataques DoS
- Uso de WAF (Web Applications Firewall) si es aplicación web
- Pruebas de carga
- Usar Dockrfile y forjar imágenes propias
- Verificar el uso de imágenes Docker publicas


Mounts all data volumes
(– volumes-from /[hpname])
- processes log data and transmits to EWS portal
Containers provide volatile data volumes (-v /[hpname])
- Containers are volatile by design (unless commited to a new image)
- Data Volumes allow for file sharing among containers
- Stores events, logs, configs, ews token etc.
EWS Container
Dionaea Container
Honeytrap Container
Kippo Container
Glastopf v3 Container
Suricata Container
ELK Container
EWS config & aggregated logs provided thru host volume
/data/ews/
Flags set to disabled for hpfeeds and malware scanning (must be enabled by user)
Start containers from images (docker run [...])
EWS Image
Dionaea Image
Honeytrap Image
Kippo Image
Glastopf v3 Image
Suricata Image
ELK Image
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Build Docker Images with individual Dockerfiles (docker build -t [imagename] .)
Docker Host @ 4GB RAM, 80GB free diskspace
Ubuntu Server 14.04.2, x64 – unattended installation from usb stick
SSH service disabled, user / pw = tsec / tsec (forced pw change)

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
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/

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

Gracias.....