SecOps

OWASP

Open Web Application Security Project

Sevilla CHAPTER

¿Quién soy?

- Sysadmin/DevOps
- Automatización
- ML
- @_2500Hz aViNash
- Me encanta mi trabajo :-)

I automate things to do less. I use things like Ansible, K8s, AWS, Python, Docker, Jenkins… to do magic with things. @OWASP-Sevilla @awsSevilla @elastic_fans

github.com/melozo
carmelo.zubeldia@gmail.com

¿Qué es OWASP?

- Open Web Application Application Security Project
  - Internacional, **sin ánimo de lucro***
  - Promueve el desarrollo de software seguro
  - Web, plataformas móviles e IoT
  - **Un foro abierto para el debate** (expertos de todo el mundo)
  - Builders, Breakers (red), **Defenders** (blue)
  - Multitud de recursos gratuitos

  [*]Libre de influencias comerciales

¿Qué ofrece OWASP?

Materiales formativos:

- OWASP Top 10
- OWASP Mobile Top 10
- OWASP Top 10 IoT Vulnerabilities
- Guía de Desarrollo OWASP
- Guía de PENTesting OWASP
- Guía OWASP para aplicaciones Web Seguras
- Muchos mas

- Comunidades locales

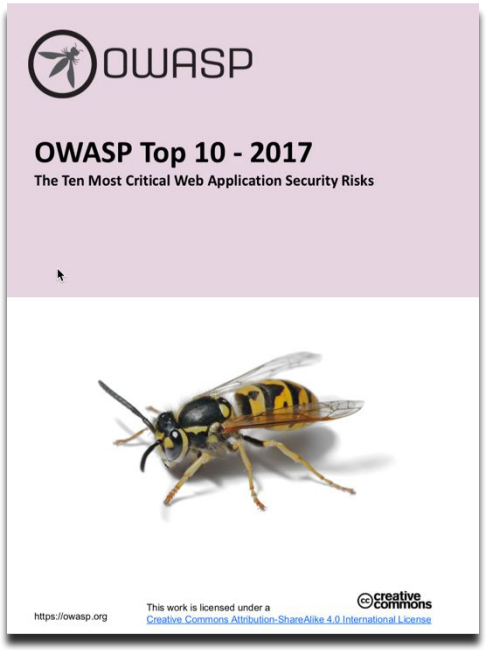
OWASP-SEVILLA

Software

- ZAP
- ModSecurity Rules
- Dependencies Check
- WebGoat
- WebScarab
- ESAPI
- bWAPP
- Muchos más

¿Qué es el OWASP Top 10?

- **Clasificación** de los mayores riesgos a los que se enfrentan las aplicaciones web.
- Ofrece **guía** para desarrolladores, organizaciones y auditores de seguridad.
- **Basado en la comunidad**:
  - Profesionales
  - Empresas colaboradoras
  - Estudio de más de **100.000** aplicaciones y APIs



OWASP Top 10 - 2017

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring



A6: 2017 – Errores en la configuración

A6: 2017 – Errores en la configuración

Las malas configuraciones es el problema más común. Configuraciones por defecto defectuosas, incompletas, que permitan el almacenamiento abierto en la nube, unas cabeceras HTTP inadecuadas, información demasiado detallada sobre cosas sensibles, etc. constituyen un riesgo. Además de configurarse de manera segura los SSOO, frameworks, librerías y aplicaciones también deben estar actualizados y parcheados.

- No refuerza la seguridad en cualquier parte de la aplicación web que así lo requiera.
- Aumenta la exposición a un ataque teniendo características innecesarias. - }:-) JDK -> JRE
- Cuentas por defecto habilitadas y funcionales.
- Manejo de errores que muestra información detallada. - Mucho tiempo
- No fuerza el uso de cifrado cuando se requiere. - Coñazo
- Software anticuado o no parcheardo.

A6: 2017 – Errores en la configuración

A6: 2017 – Errores en la configuración

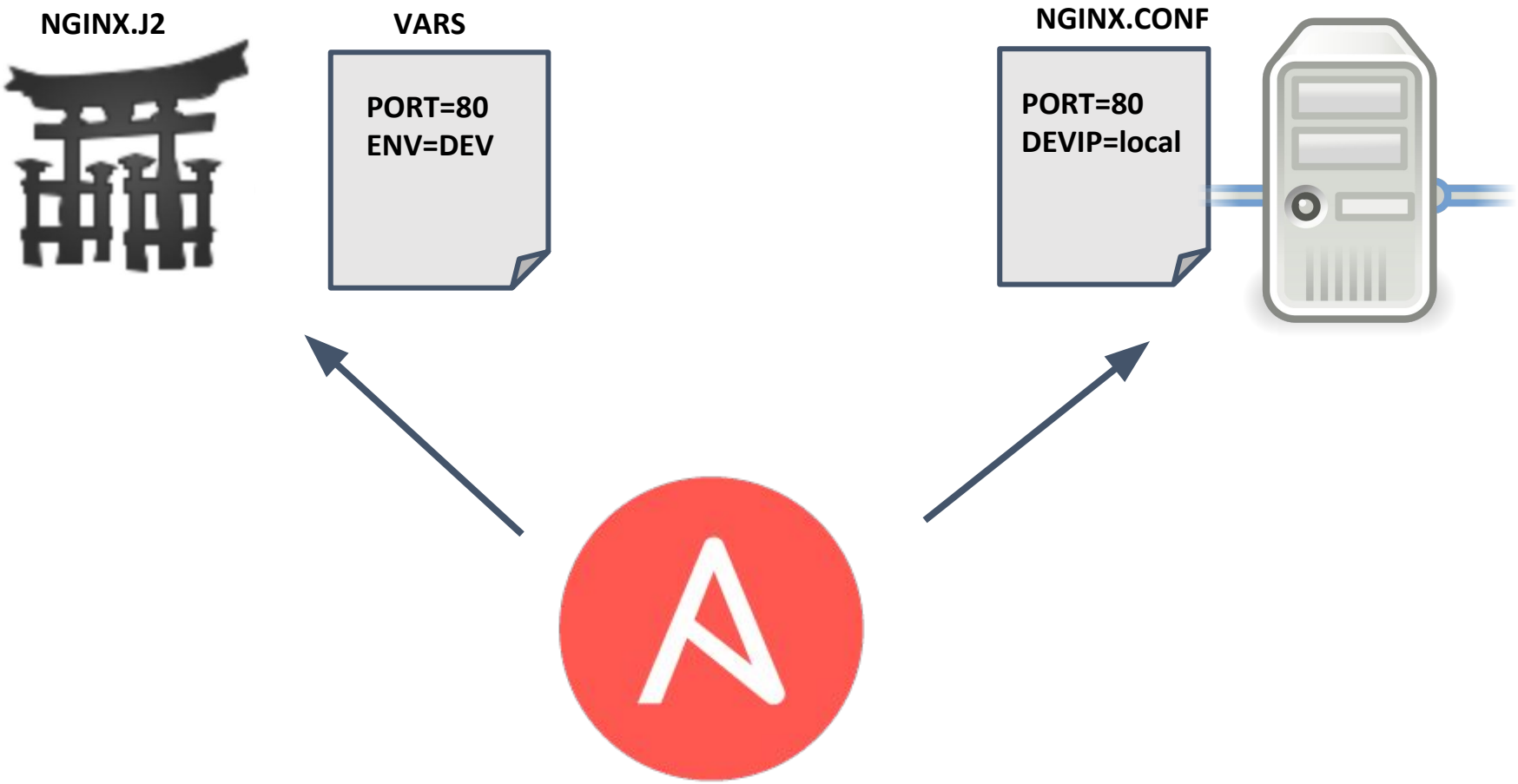
¿CÓMO GESTIONAMOS LAS CONFIGURACIONES?

- ¿Versionado?
- ¿Cómo gestionamos el cambio?
- ¿Medimos el impacto de los cambios? - WTF?
- ¿Podemos hacer Rollbacks?
- Distintos entornos (dev/pro)

A6: 2017 – Errores en la configuración


```
…
[mysqld]
port = {{ mysql_port }}
bind-address = {{ mysql_bind_address }}
datadir = {{ mysql_datadir }}
socket = {{ mysql_socket }}
pid-file = {{ mysql_pid_file }}
{% if mysql_skip_name_resolve %}
skip-name-resolve
{% endif %}
…
```

A6: 2017 – Errores en la configuración



DEMO

DEMO
TestInfra

A10: 2017 – Monitorización y registro insuficiente (Nuevo)

A10: 2017 – Monitorización y registro insuficiente

Una monitorización y registro insuficiente acompañado de una mala respuesta a incidentes puede permitir a un atacante hacerse persistente en el sistema atacado, pivotar hacia otros, volcar, extraer y destruir datos.

- Eventos como inicios de sesión, intentos de éstos y transacciones importantes no se registran y/o no se monitorizan.
- Escaneados de puertos o análisis externos automatizados no son registrados.
- Los registros sólo se almacenan de manera local.

A10: 2017 – Monitorización y registro insuficiente (Nuevo)

A10: 2017 – Monitorización y registro insuficiente

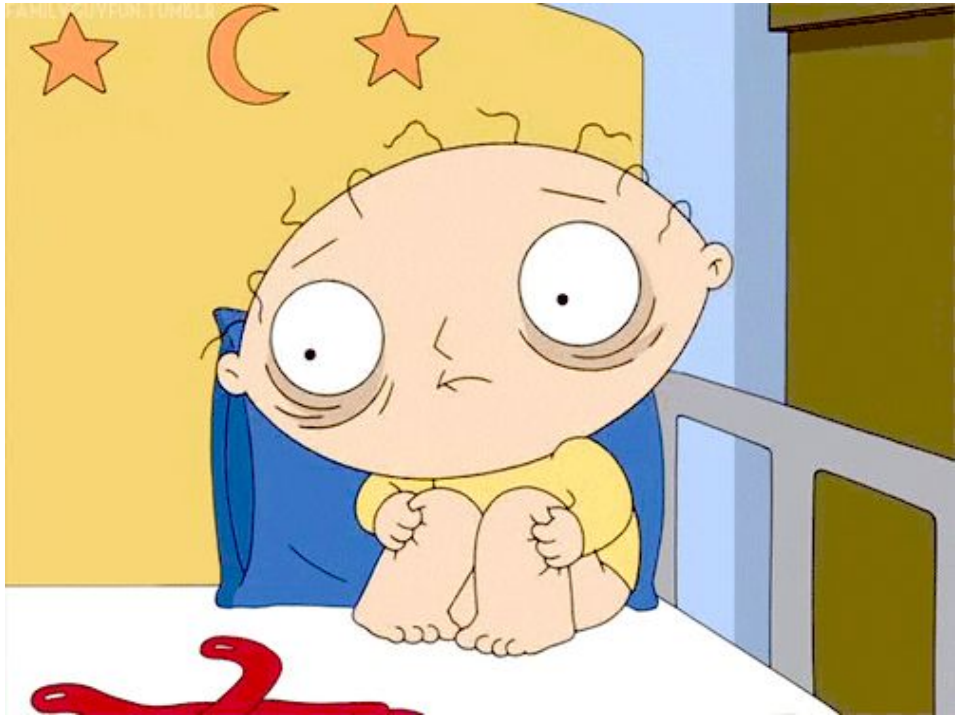
Una monitorización y registro insuficiente acompañado de una mala respuesta a incidentes puede permitir a un atacante hacerse persistente en el sistema atacado, pivotar hacia otros, volcar, extraer y destruir datos.

La importancia del cómo...

- **Automatización**
  - **!Personalización**
  - !Scripticos (script+críptico)*
- **Selección de un stack (Operaciones)**
  - **git, ansible, jenkins...**
- **Trabajar con humanos**
- **Nadie lo sabe todo**

¿ Por qué ...?

Cloud, virtualización, sistemas operativos, contenedores, configuraciones, redes, seguridad, backups...

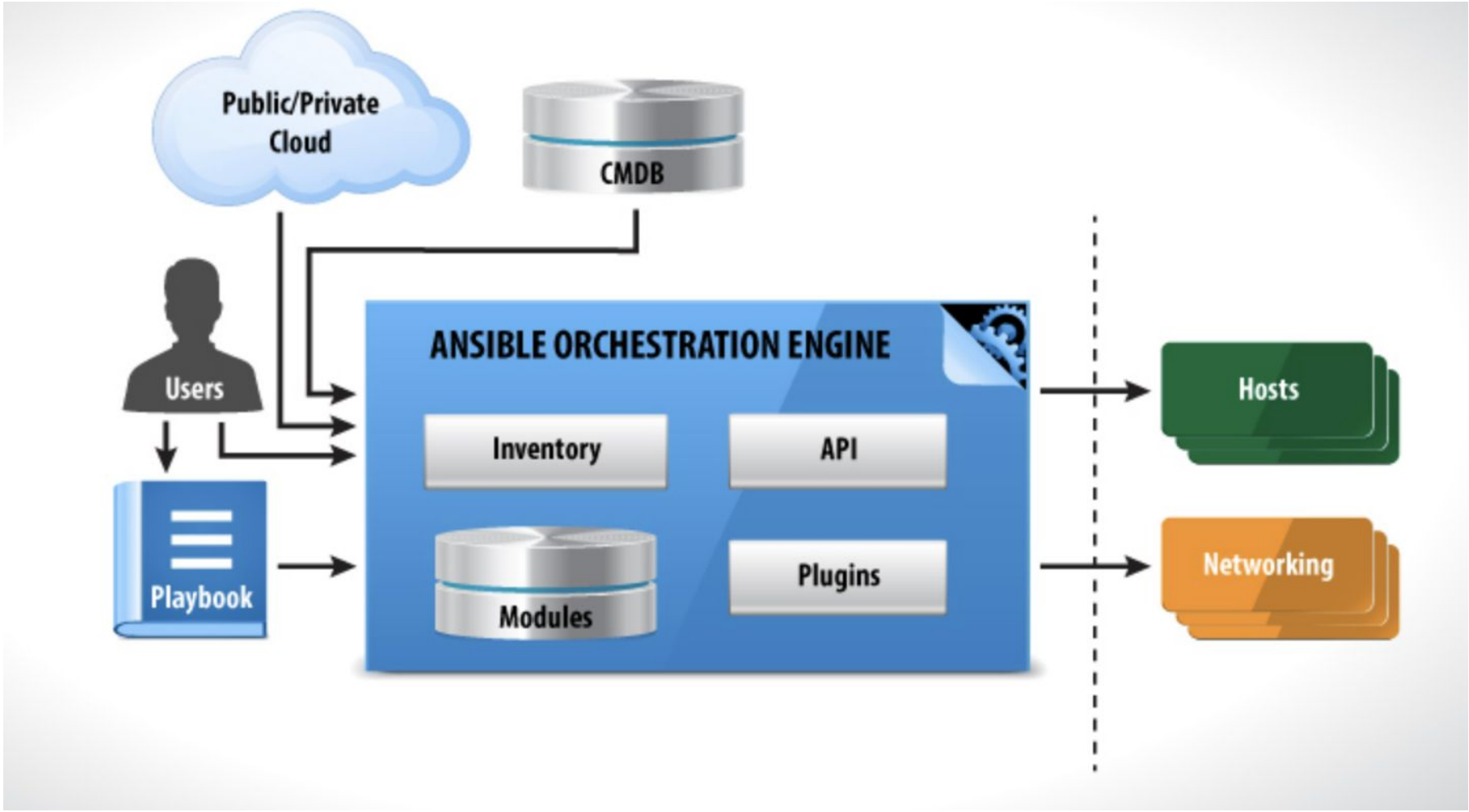


Ansible… DSL para operaciones

```
- name: download the docker bench security
  git:
    repo: https://github.com/docker/docker-bench-security.git
    dest: /opt/docker-bench-security

- name: running docker-bench-security scan
  command: docker-bench-security.sh -l /tmp/output.log
  args:
    chdir: /opt/docker-bench-security/
```

Ansible componentes



Ansible Conexiones

➜ ansible-doc -t connection -l

➜ ansible-doc -t httpapi -l

DEMO

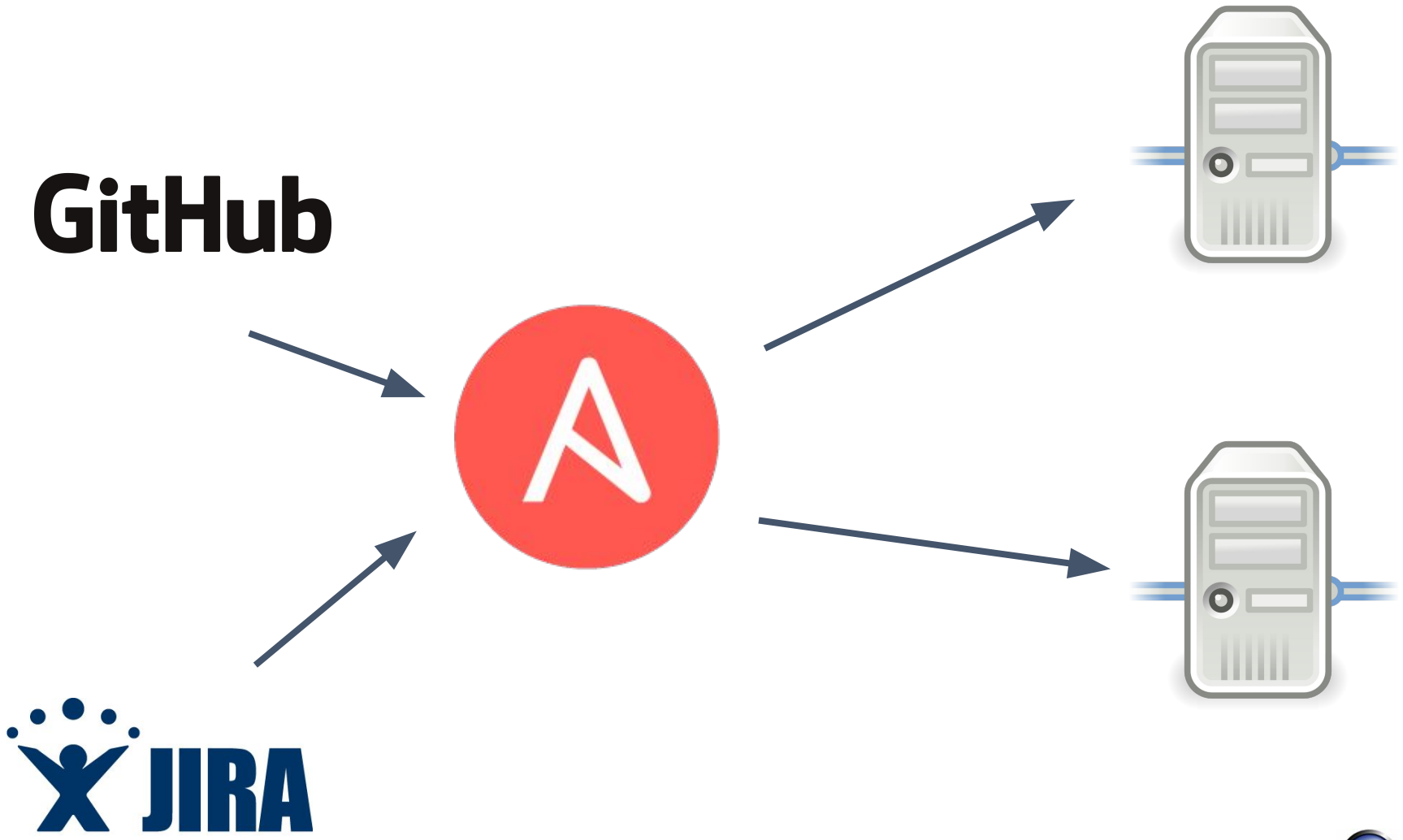
Docker Bench for Security:

Script que comprueba docenas de buenas prácticas comunes en el despliegue de contenedores Docker en producción.

Ansible es solo una herramienta

- Vocabulario
- Integraciones (APIs, productos)
- Producción (eventos, alertas)
- Automatización

Ansible Tower



Curso Ansible 101

MARZO - 2ª CONVOCATORIA

Viernes (tarde) y Sábado - 390 €

Carmelo Zubeldia:
carmelo.zubeldia@gmail.com
645041627