

**XIII
JORNADAS
STIC
CCN-CERT**



Ciberseguridad vs la Infraestructura Abstracta Microservicios, Docker y Kubernetes



*¡No hay
cuchara, Neo!*

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT



Alberto Cita Sánchez

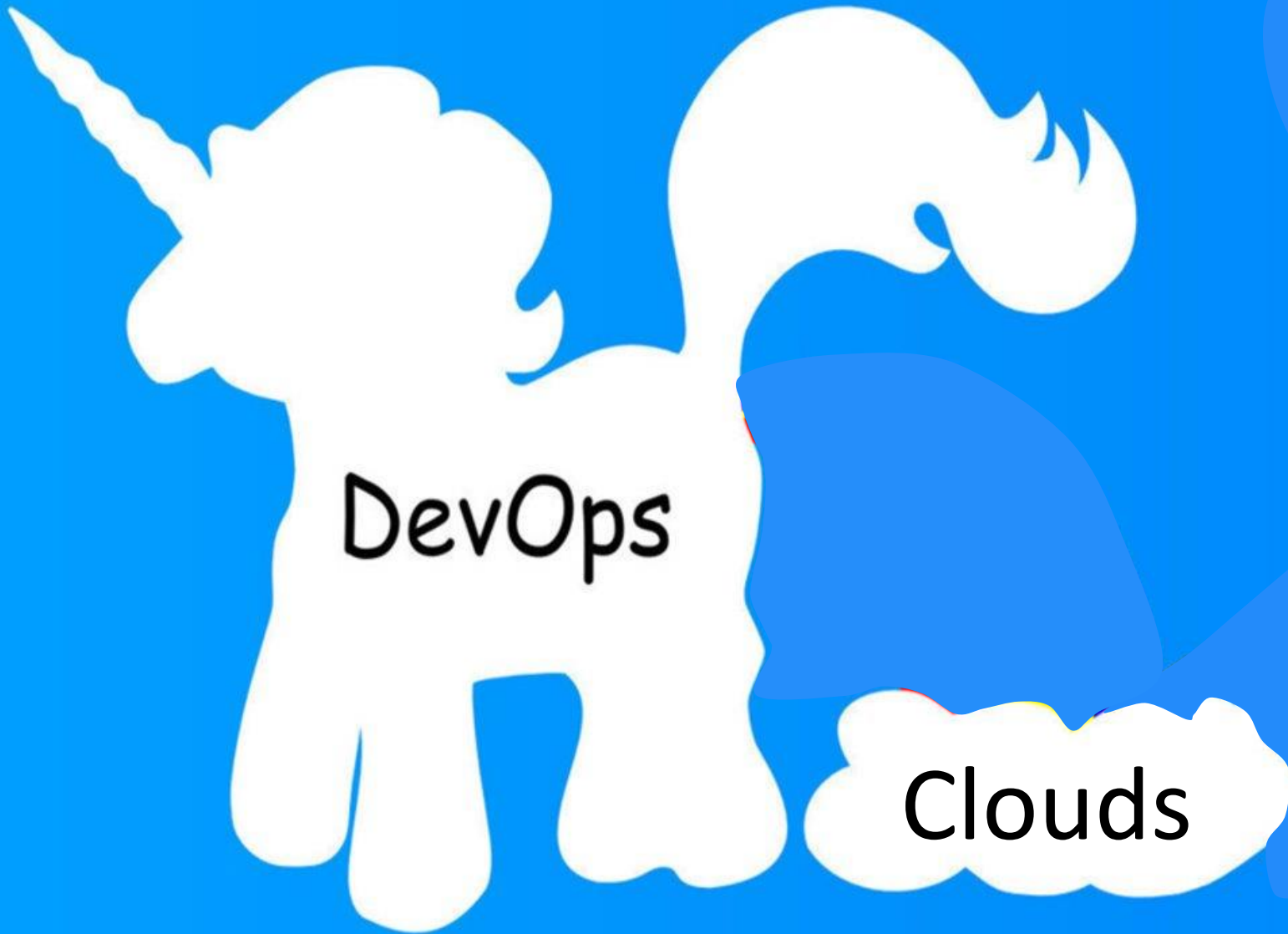
Director Técnico Symantec

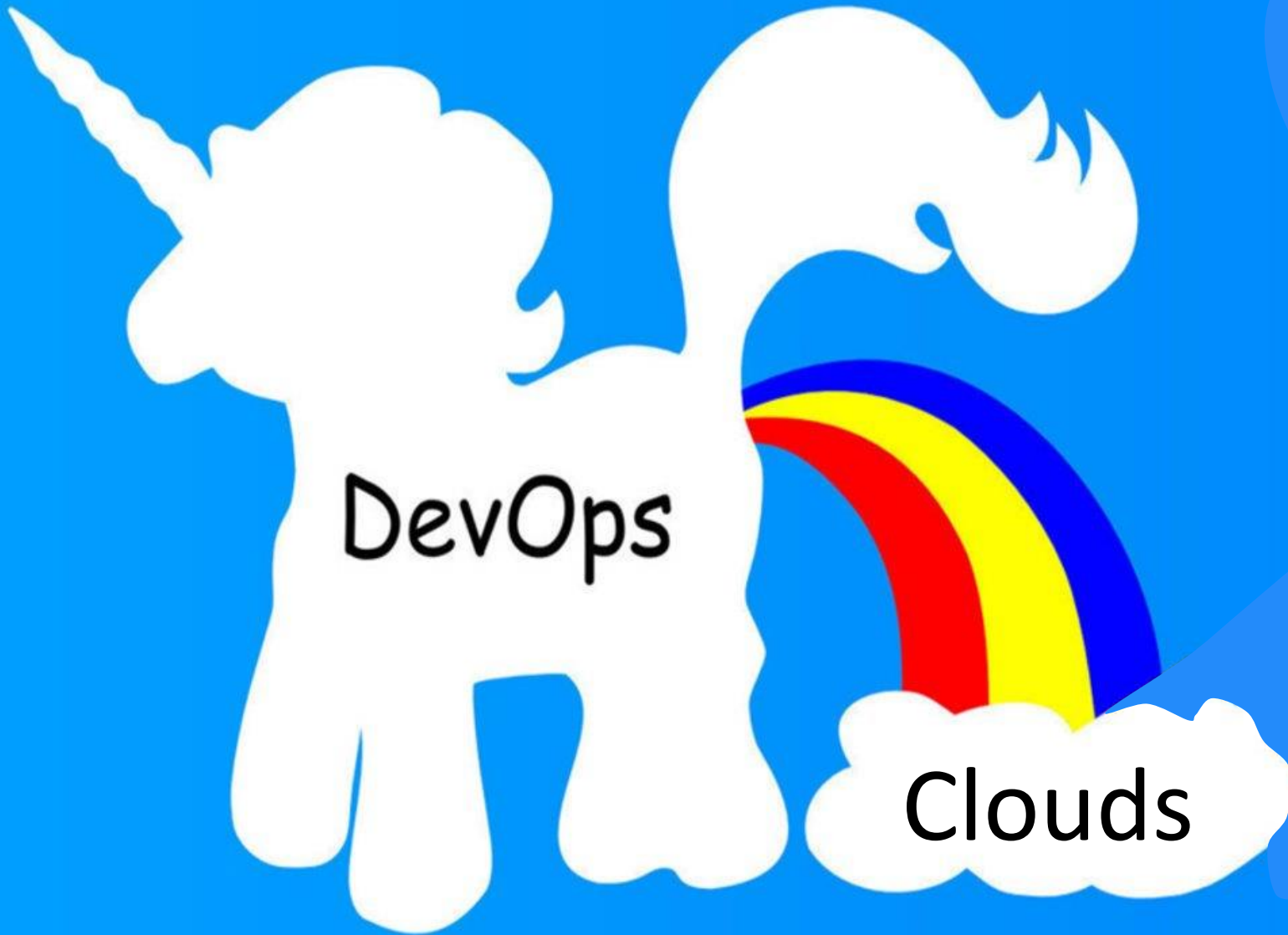
alberto@citasanchez.com

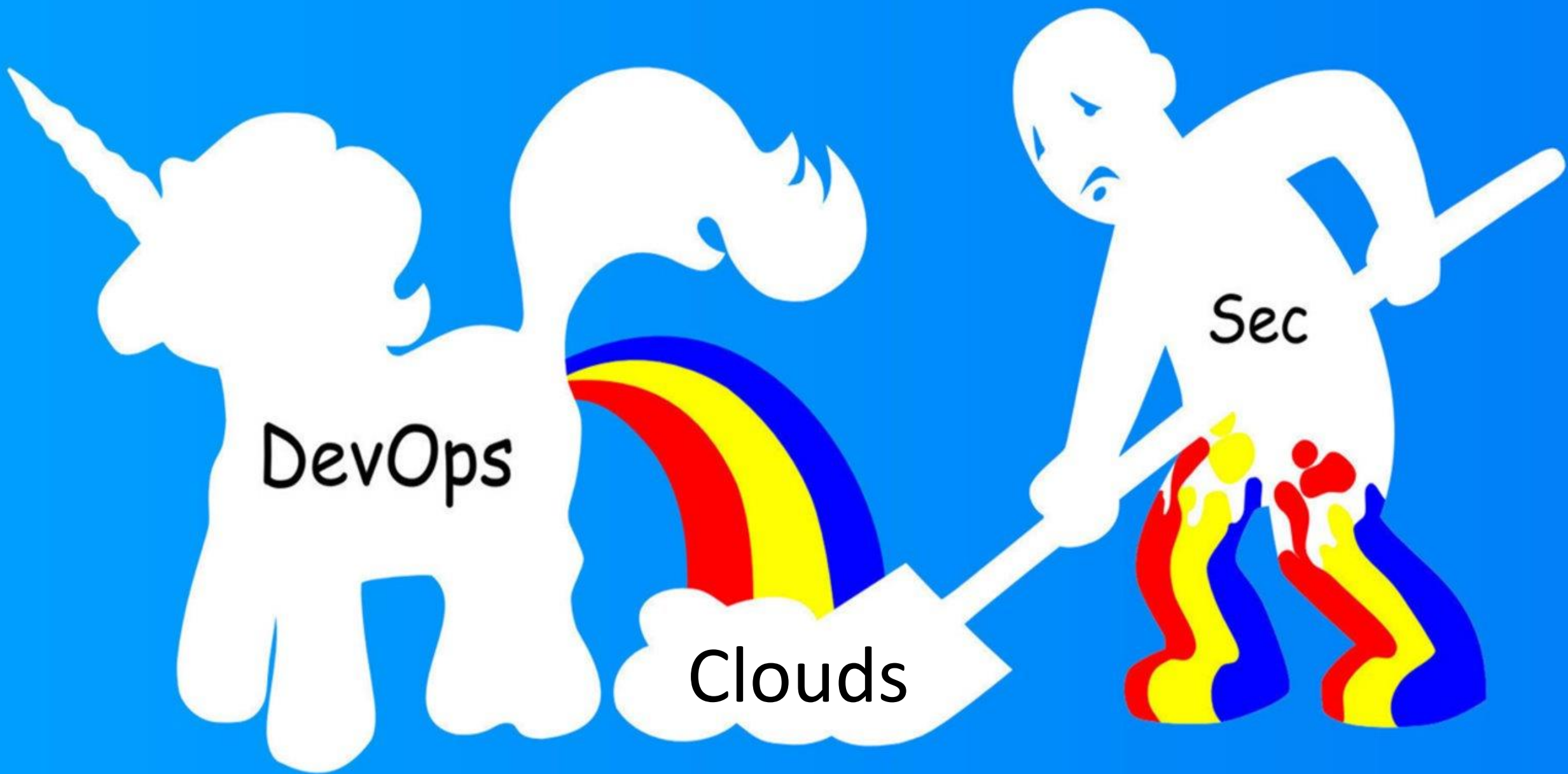
Índice

1. Conceptos Básicos de DevOps para Ingenieros de Ciberseguridad
2. De Docker a Kubernetes
3. K8s en $t < 5$ min
4. Todo está muy bien... ¿Dónde está el problema?
5. Desarrollo de un programa de seguridad para Docker y K8s
6. Conclusiones









Sec Dev Ops

Conceptos Clave de DevOps

Para Ingenieros de Ciberseguridad

Infraestructura IT desplegada como código

- La SEGURIDAD debe desplegarse COMO CÓDIGO y empleando herramientas de DevOps (***“Lift & Shift”***)

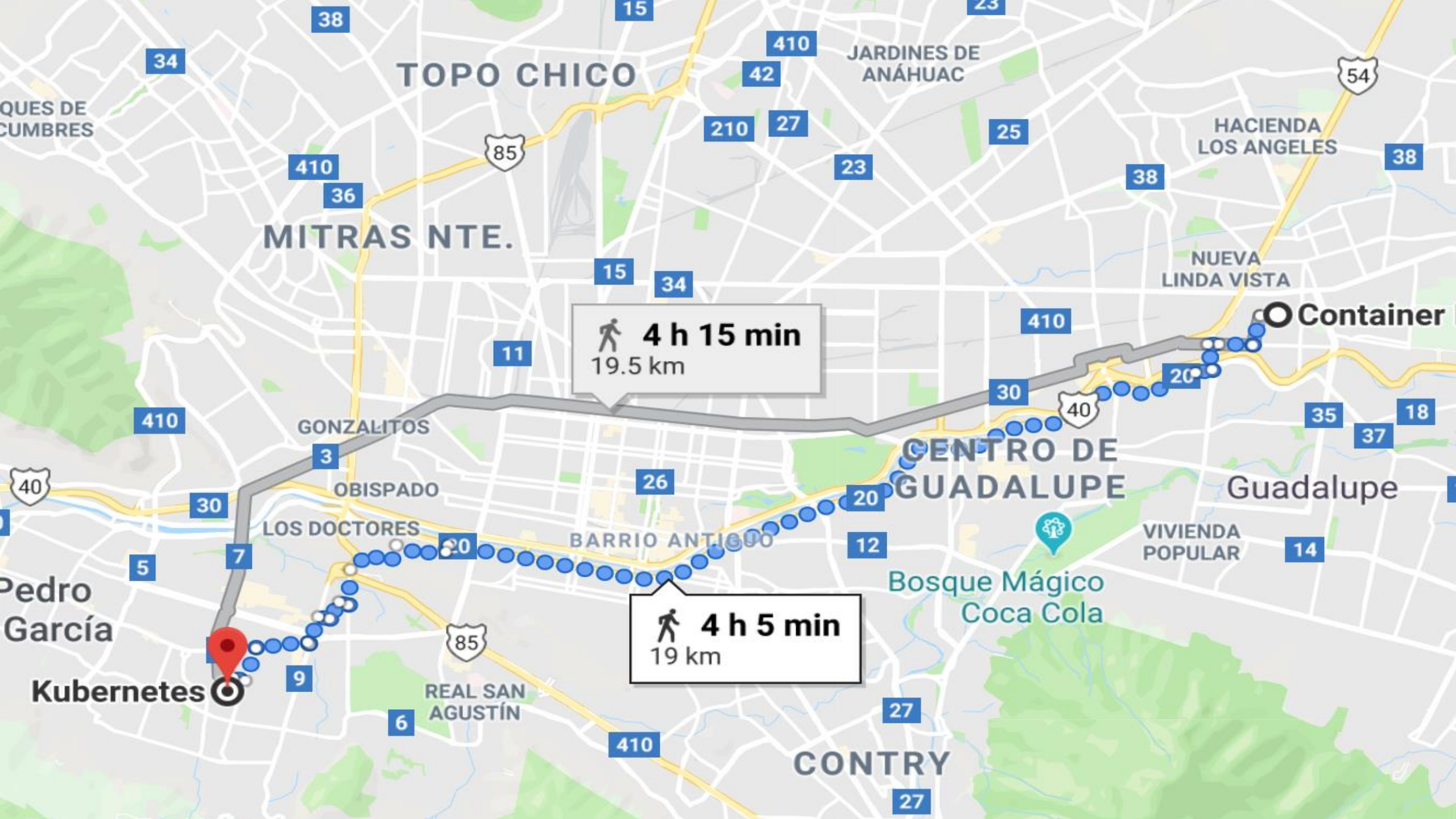
Cualquier mecanismo de seguridad que rompa el *Pipeline* de CI/CD es inviable

- Incluir la SEGURIDAD tan pronto como sea posible EN EL CICLO de CI

DevOps demanda nuevas arquitecturas de aplicaciones

Microservicios

- Adopción de Contenerización (p.e.: Docker) para su implementación práctica



Gestionando Infraestructura IT en Nube

Mascotas vs Ganado (*Pets vs Cattle*)



Gestión Tradicional de Infraestructura (Inelástica)

Mascotas

- Únicos e indispensables
- Hechos a mano
- “Alimentados” a mano
- GUI
- Escalan verticalmente



Gestión Moderna de Infraestructura (Elástica)

Ganado

- Muchos servidores homogéneos
- “Desechables” (tan sólo uno más del rebaño)
- Automatizado y diseñado para fallar
- API (vs GUI)
- Escala horizontalmente



La diferencia fundamental en la gestión de infraestructura IT

Los Criterios de Disponibilidad

- 99.9% en las aplicaciones
- 99.999% en la infraestructura
- (€€€€€)

Tradicional
(Inelástica)



- 99.999% en las aplicaciones
- 99.5% en la infraestructura
- (€)

Moderna
(Elástica)

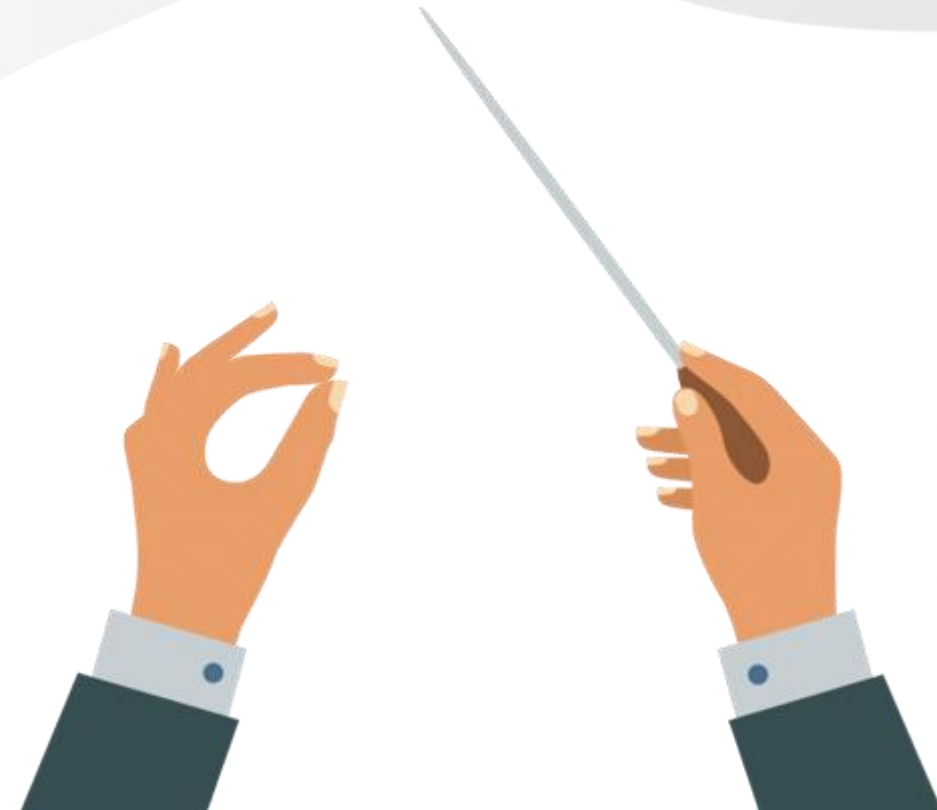


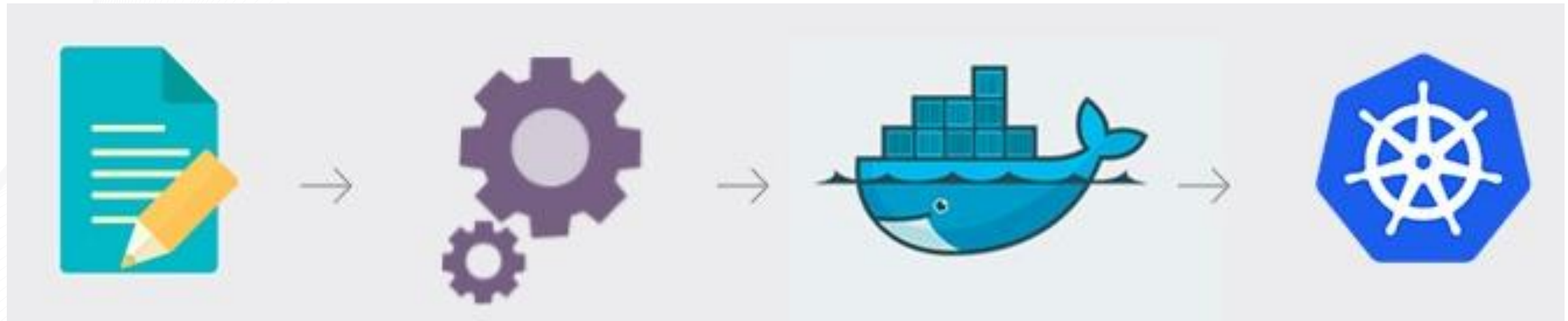
Todo Rebaño Necesita un Pastor

Trabajando con “Ganado” no se asigna manualmente en qué máquinas correrán los microservicios de una aplicación

Para eso está el orquestador: gestión del ciclo de vida de los contenedores

Kubernetes, Mesos, Swarm





La Tarea

Desarrollar
la Aplicación

Crear los “Docker”
para la aplicación

Lanzar la aplicación
en Kubernetes

K8s en pocas palabras

Orquestador de código abierto para el despliegue de aplicaciones “contenerizadas”

Software para construir y desplegar sistemas distribuidos escalables de alta disponibilidad

Principales Beneficios

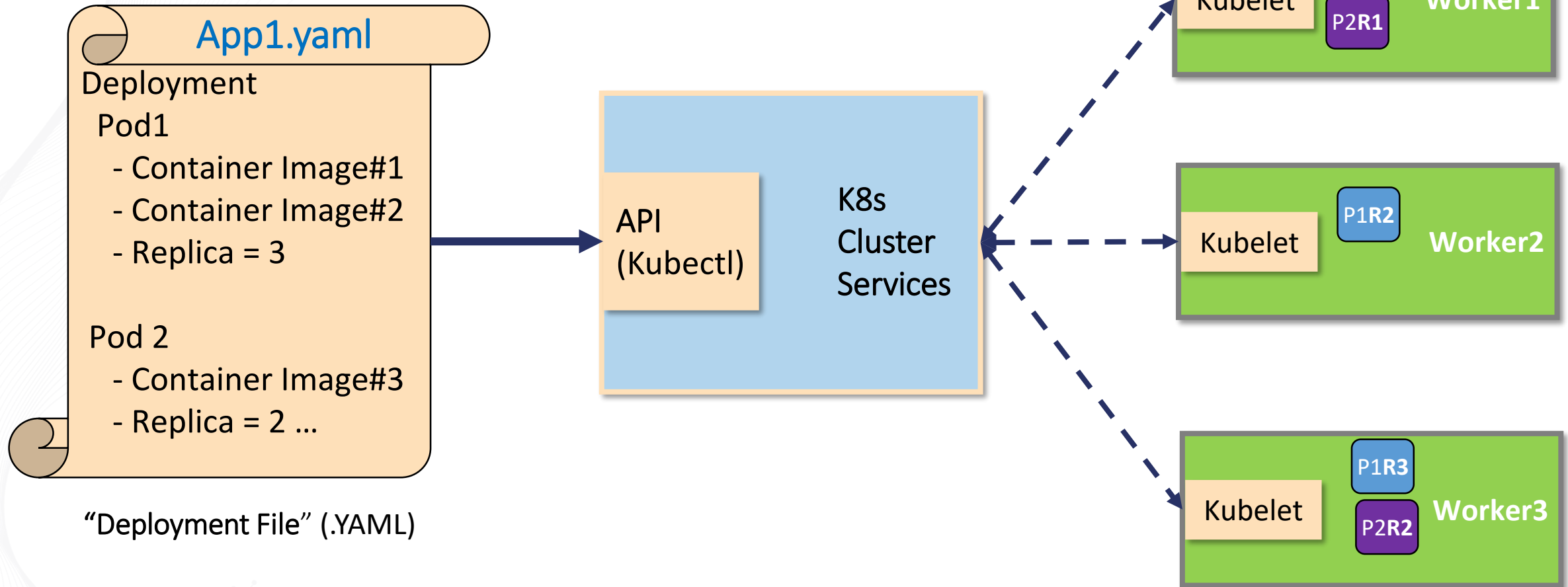
- **Velocidad** (*# nuevas funcionalidades entregables por hora sin perder disponibilidad*)
- **Escalado:** aplicaciones y equipos de DevOps
- **Abstracción de la infraestructura** **¡No hay cuchara, Neo!**
- **Eficiencia**



No intentes doblar la cuchara. Eso es imposible. En vez de eso sólo procura comprender la verdad: ¡que no hay cuchara!

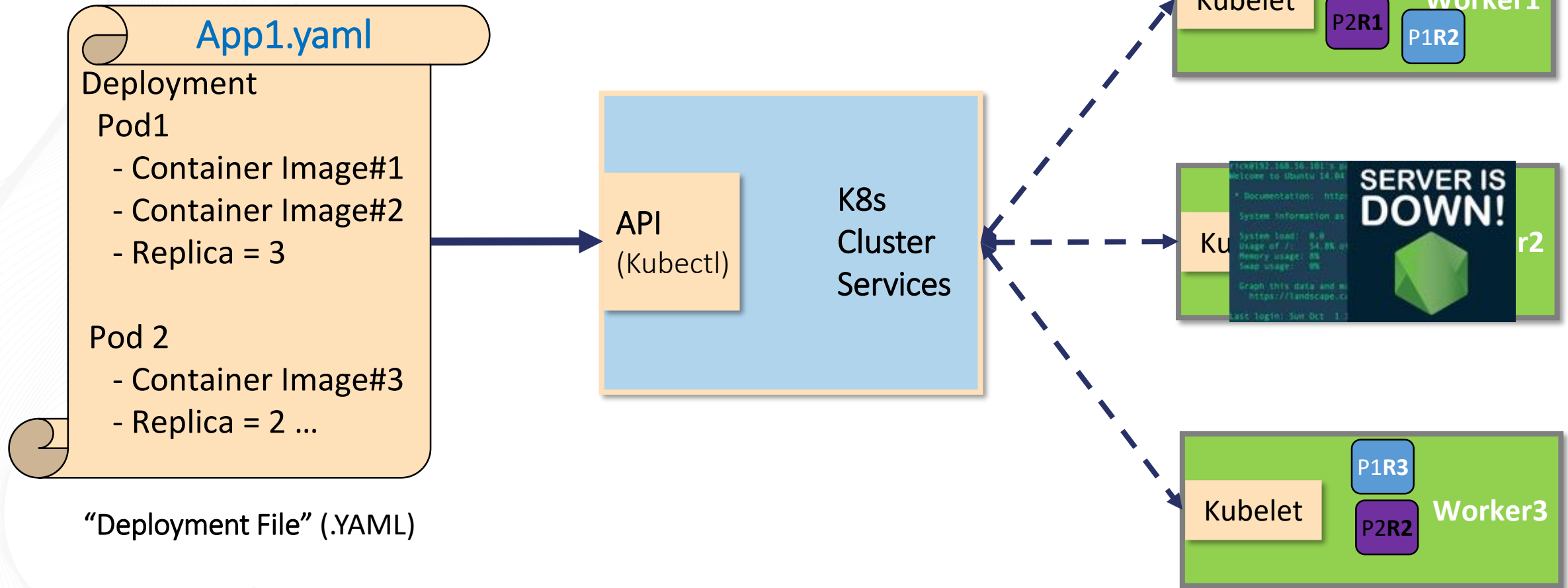
Kubernetes en t < 5 min

Gestión del “Estado Deseado”



Kubernetes en $t < 5$ min

Gestión del “Estado Deseado”



La in-Seguridad de Docker



An Attacker Looks at Docker: Approaching Multi-Container Applications

Black Hat

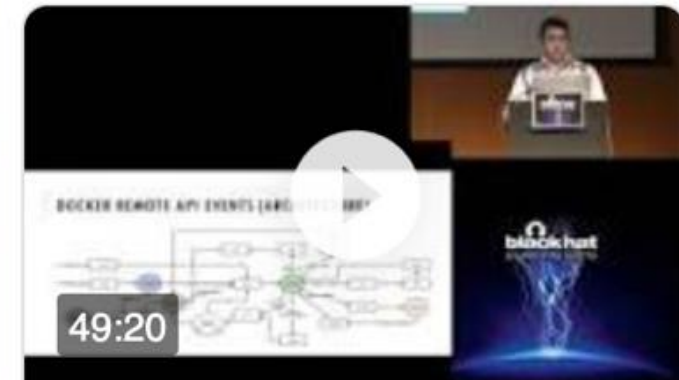
YouTube - Aug 28, 2018



How Abusing Docker API Led to Remote Code Execution, Same ...

Black Hat

YouTube - Dec 18, 2017



Vulnerability Exploitation In Docker Container Environments

Black Hat

YouTube - Mar 5, 2016

La in-Seguridad de Docker

Malicious Container Escape Exploit (CVE-2019-5736) PoC Demo ...

<https://www.youtube.com> › watch



Feb 12, 2019 - Uploaded by Ethical Hackers Club

Proof of concept (PoC) demo for CVE-**2019**-5736. A flaw has been detected in runc which allows a malicious ...

Escape Docker Container Using waitid() | CVE-2017-5123 | Twistlock

<https://www.twistlock.com> › labs-blog › escaping-docker-container-using-waitid-cve-20...



Dec 27, 2017 - Uploaded by Daniel Shapira

Escaping **Docker** container using waitid() – CVE-2017-5123 security researcher who embarked on this path ...

La in-Seguridad de K8s

La seguridad por defecto de K8s puede describirse como pobre, siendo generosos



Hacking kubernetes part 1 - Kubelet exec and reverse shell from pod.

pohackblog • 798 views • 1 year ago

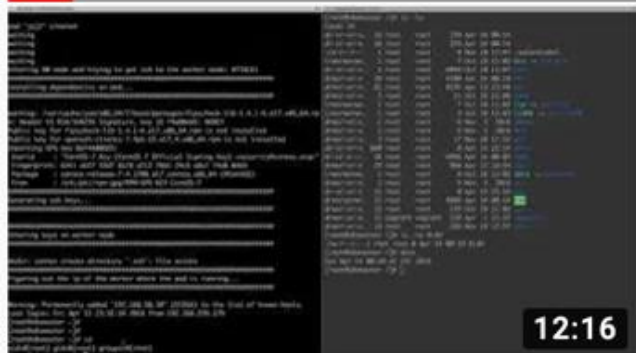
Hacking kubernetes part 1. This is a video from <https://poc-hack.blogspot.co.uk/2018/04/hacking-kubernetes-part-1.html> Please ...



Hacking kubernetes part 2 - Getting root access to the worker node method 1 (By misconfiguration)

pohackblog • 161 views • 1 year ago

Hacking kubernetes part 2. Before watching this video, please check part 1 ...



Hacking kubernetes part 3 - Five ways to get root access to the worker node using CVE-2017-1002101

pohackblog • 346 views • 1 year ago

In this video I demonstrate five ways to get root access on a kubernetes worker node using the vulnerabitly CVE-2017-1002101.

La in-Seguridad de K8s

La seguridad por defecto de K8s puede describirse como pobre, siendo generosos

August 29, 2019

DNS Spoofing on Kubernetes Clusters

In this post I'll describe how an attacker, who manages to run malicious code on a cluster can, with no special permissive permissions, successfully spoof DNS responses to all the applications running on the cluster, and from there execute a MITM (Man In The Middle) on all network traffic of pods. Before we get into ...

August 01, 2019

Kubernetes Pod Escape Using Log Mounts

Kubernetes has many moving parts, and sometimes combining them in certain ways can create unexpected security flaws. In this post you'll see how a pod running as root and with a mount point to the node's `/var/log` directory can **expose the entire contents of its host filesystem** to any user who has access to its logs. ...

July 08, 2019

Crypto-Mining Malware Outsmarting Image Scanners

In previous crypto-mining attacks, we observed hackers investing little to no effort in hiding their malicious activities. They just ran the malicious container with all of its scripts and configuration files in clear text. This made the analysis of their malicious intent fairly easy.

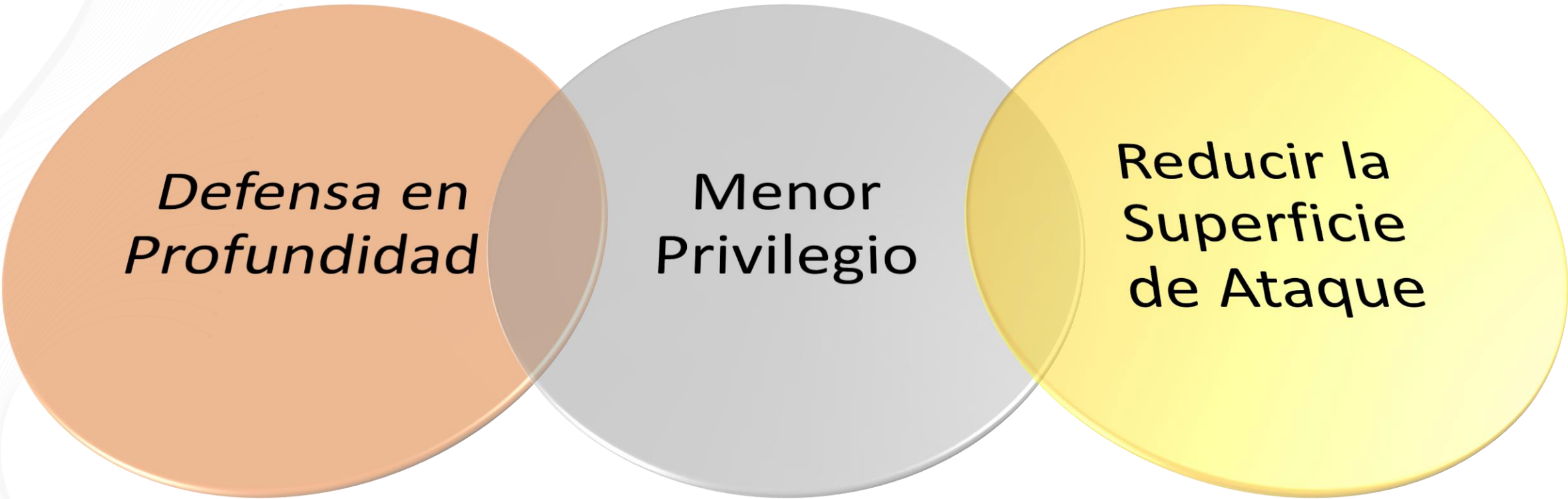
June 27, 2019

CVE-2019-11246: Another kubectl Path Traversal Vulnerability Disclosed

A new vulnerability (CVE-2019-11246) was disclosed that enables path traversal in kubectl, the popular command line interface for running commands on Kubernetes clusters. What's interesting about this CVE is that we've already seen two previous variations of the same vulnerability disclosed and patched. Read on to ...

Desarrollo de un programa de seguridad para Docker & K8s

Atenerse a los principios fundamentales de la seguridad IT



*Defensa en
Profundidad*

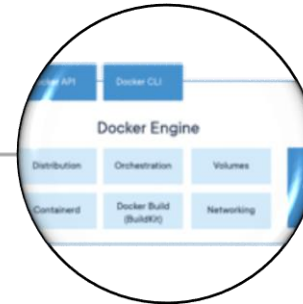
Menor
Privilegio

Reducir la
Superficie
de Ataque

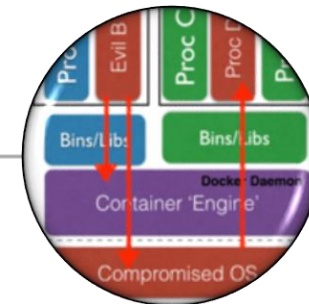
Docker: Superficie de Amenazas



Amenazas al Entorno de Automatización de Compilación (*Build*)



Amenazas al Entorno de Runtime



Amenazas al *Docker Engine* y al OS Subyacente

Asegurando Docker

Amenazas específicas

Cambios maliciosos en código fuente

Alteraciones maliciosas / erróneas en los controladores de compilación automática (Jenkins, Bamboo)

Scripts de configuración con errores o que exponen credenciales

Uso de bibliotecas inseguras o versiones antiguas / inseguras del código existente

Bibliotecas y paquetes innecesarios olvidados en contenedores (+ superficie de ataque)

Asegurando Docker

Recomendaciones Generales

CIS Docker Benchmark

Bloquear configuración de *build controllers* + RTFIM*

Enviar los logs de Jenkins/Bamboo logs al SIEM

Añadir test de seguridad unitarios al proceso de build automático de DevOps

Usar Contenedores Inmutables

Reducir la Longevidad de los Contenedores

Firmado de Contenedores & Cadena de Custodia

Chequear Librerías y Código vs CVEs

Microsegmentación a nivel de Contenedor

*RTFIM: Real-Time File Integrity Monitoring

Asegurando Docker

Recomendaciones y Mejores Prácticas: Entorno de Compilación

Entorno de Compilación

Recordatorio: **CI/CD pasa código nuevo a producción varias veces al día**

Restringir quién puede modificar el entorno de compilación y actualizar el código y auditar este proceso

Asegurar y segregar los servidores Jenkins/Bamboo

No ejecutar contenedores como root

Aplicar el principio de menores privilegios

¿Passwords “hard-codeados” / claves / auth tokens en Contenedores?

Segregar entornos: Dev, Test, Prod

*El menos seguro
y en el que
resulta más
sencillo plantar
código
malicioso*

Amenazas vs Gestores de Orquestación (K8s, Mesos, Swarm)

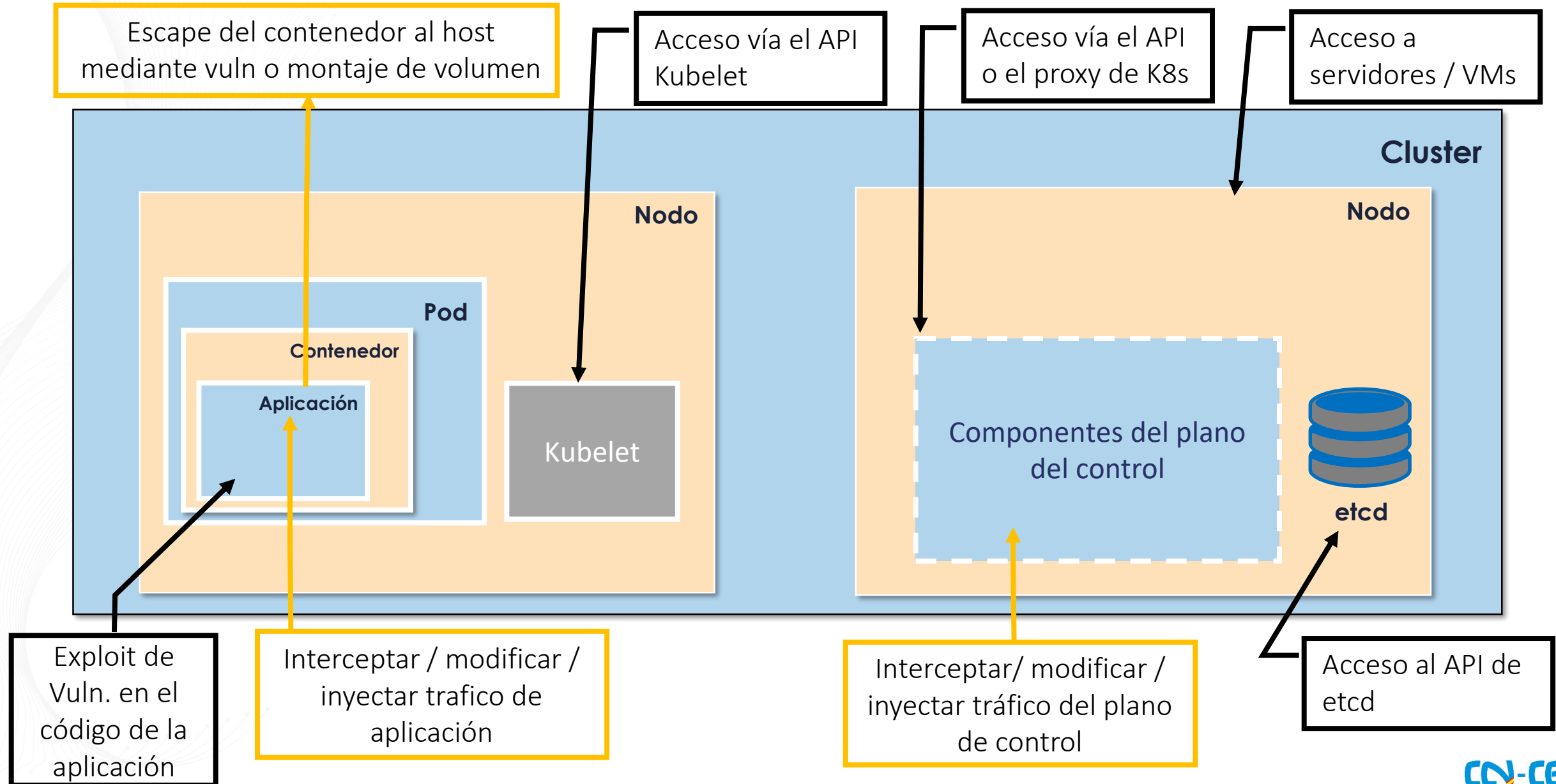
Herramientas MUY complejas

- ... su desarrollo se ha enfocado en la escalabilidad y facilidad de gestión, NO EN LA SEGURIDAD

Traen consigo un nuevo conjunto de vulnerabilidades y otros problemas de seguridad

- Configuraciones por defecto NO seguras
- Vulns. de escalado de privilegios
- Vulns. de inyección de código
- Emisión de certificados DESDE EL GESTOR DE ORQUESTACIÓN, según se van lanzando nuevos contenedores

K8s: Principales Vectores de Ataque



Asegurando el Plano de Control de K8s

**CIS Benchmark for
Kubernetes**

**Revisar a fondo la
configuración los
servidores de K8s!**

La configuración de
seguridad por defecto de
K8s ha ido mejorando en
cada versión...

... configuraciones
inseguras pueden
haberse quedado atrás

Cambiar acceso anónimo
a Kubelets por
autenticación basada en
certificado

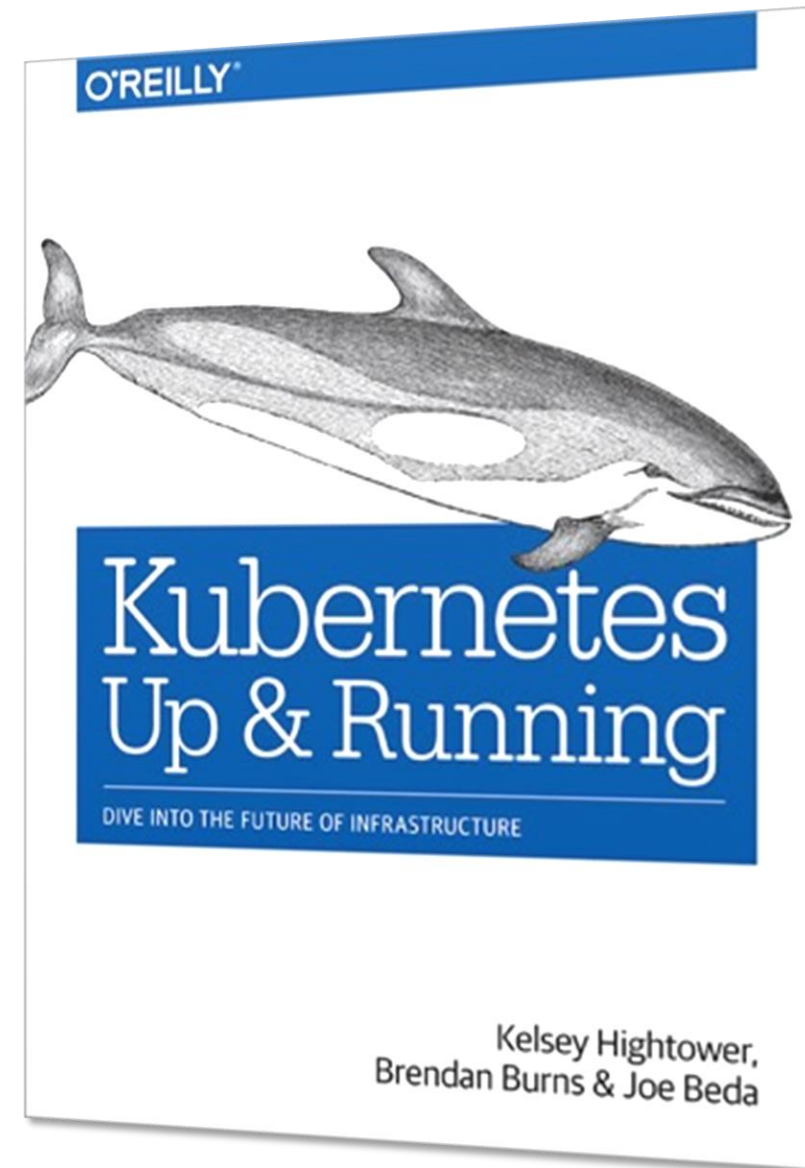
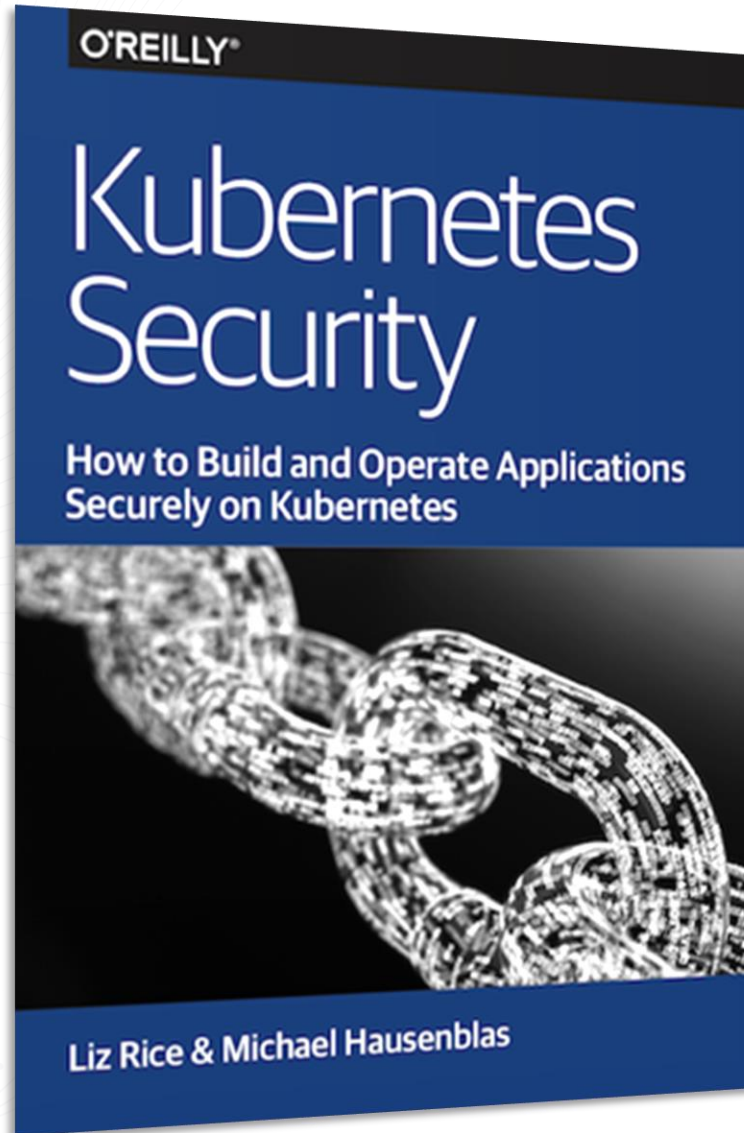
**Asegurar el
“Cluster Server”**

Evitar que usuarios /
máquinas no autorizados
controlen lo que pasa en
el clúster de K8s

Si alguien puede correr
software en tu
implementación, podrá, al
menos, consumir recursos
computacionales
(**Cryptojacking, Bots
DDoS**)

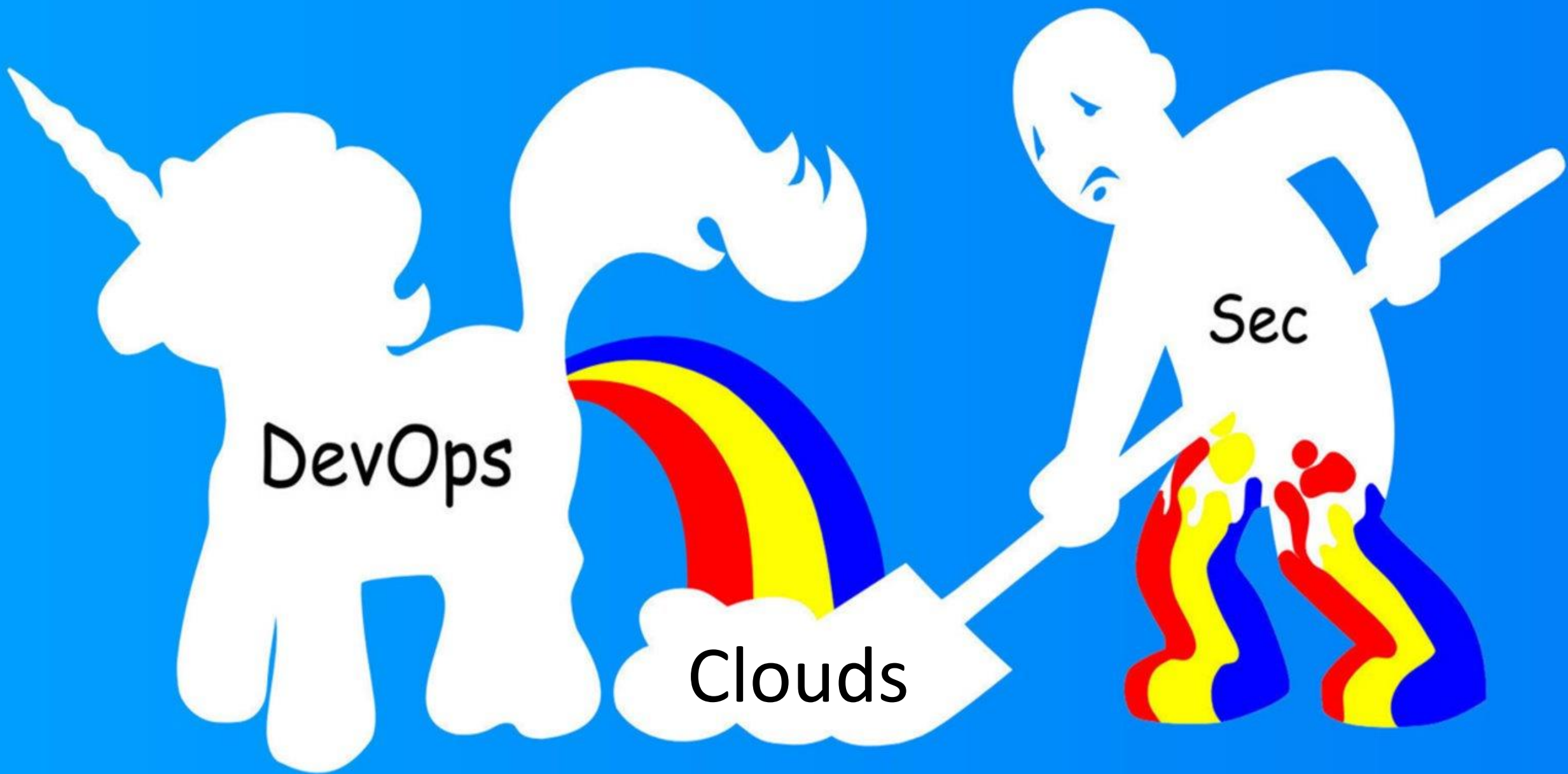
**Implementar
RBAC para el
acceso a los APIs
del Cluster K8s**

Asegurando K8s: “*Read the Books*”





*The force is weak
with me today...*





*O al menos,
...haceros quedar
bien en el bar...*

Gracias!

A simple, hand-drawn smiley face in blue ink, consisting of two vertical lines for eyes and a curved line for a mouth.

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional