VII Jornadas Nacionales de Investigación en Ciberseguridad
Del 27 al 29 de junio de 2022

A Review of Kubernetes Security Vulnerabilities, Attacks and Practices

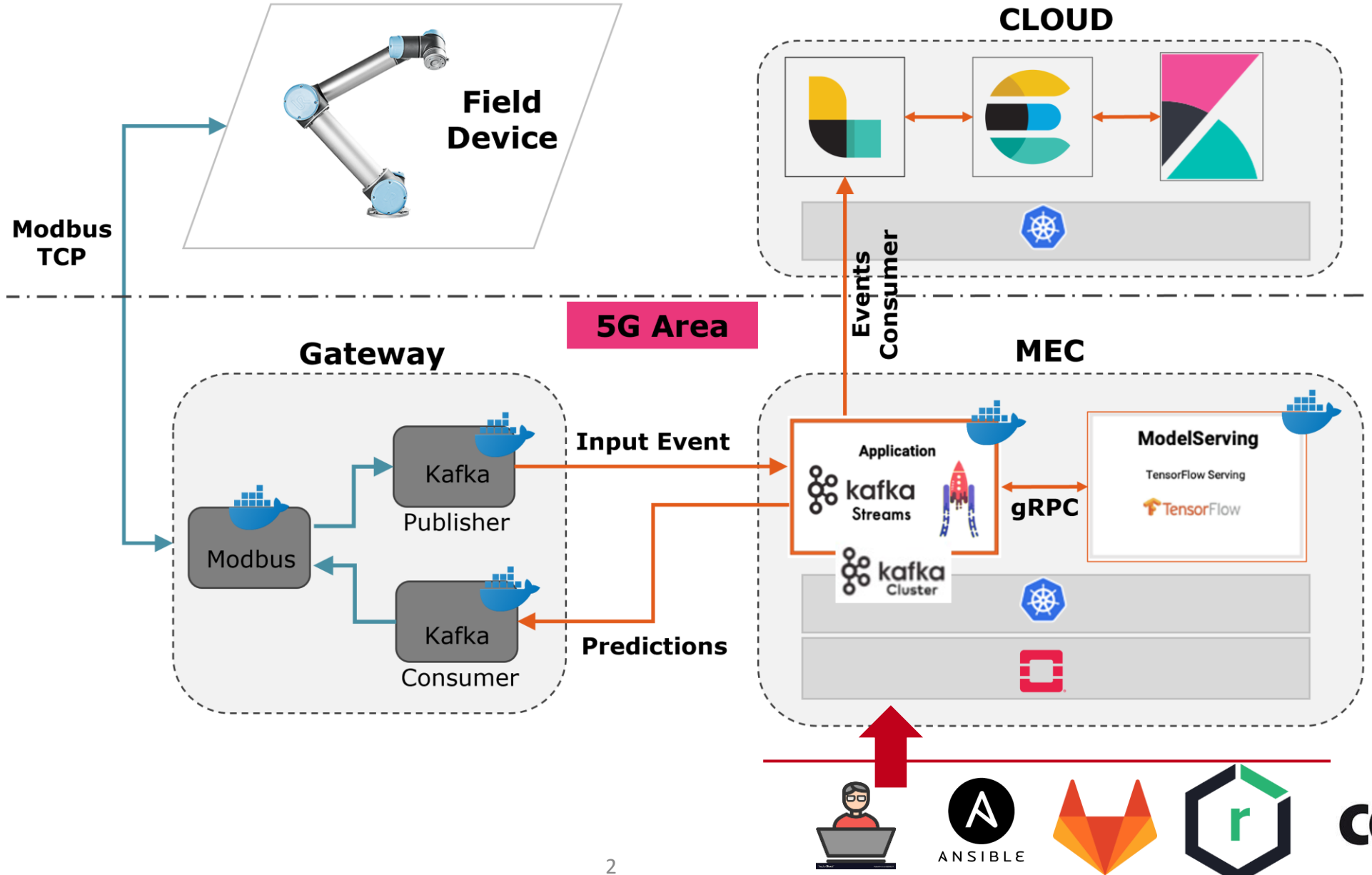
Santiago Figueroa
Saioa Arrizabalaga

Introducción

- Kubernetes es un sistema de orquestación de contenedores para automatizar el despliegues, escalado y gestión de software.
- Adopción de Kubernetes[1]:
  - *~5.6 millones de desarrolladores* usan Kubernetes a nivel mundial, el *31%* de los desarrolladores de Backend.
  - Herramientas de monitorización como *Prometheus* vieron en el segundo semestre de 2021 un 43% de incremento de usabilidad gracias a su integración sobre Kubernetes.
    - El Departamento de Defensa de Estados Unidos ha habilitado DevSecOps con Kubernetes en *F – 16* y *acorazados*[2].

[1] https://github.com/cncf/surveys/tree/main/cloudnative
[2] https://www.cncf.io/blog/2020/05/07/with-kubernetes-the-u-s-department-of-defense-is-enabling-devsecops-on-f-16s-and-battleships/

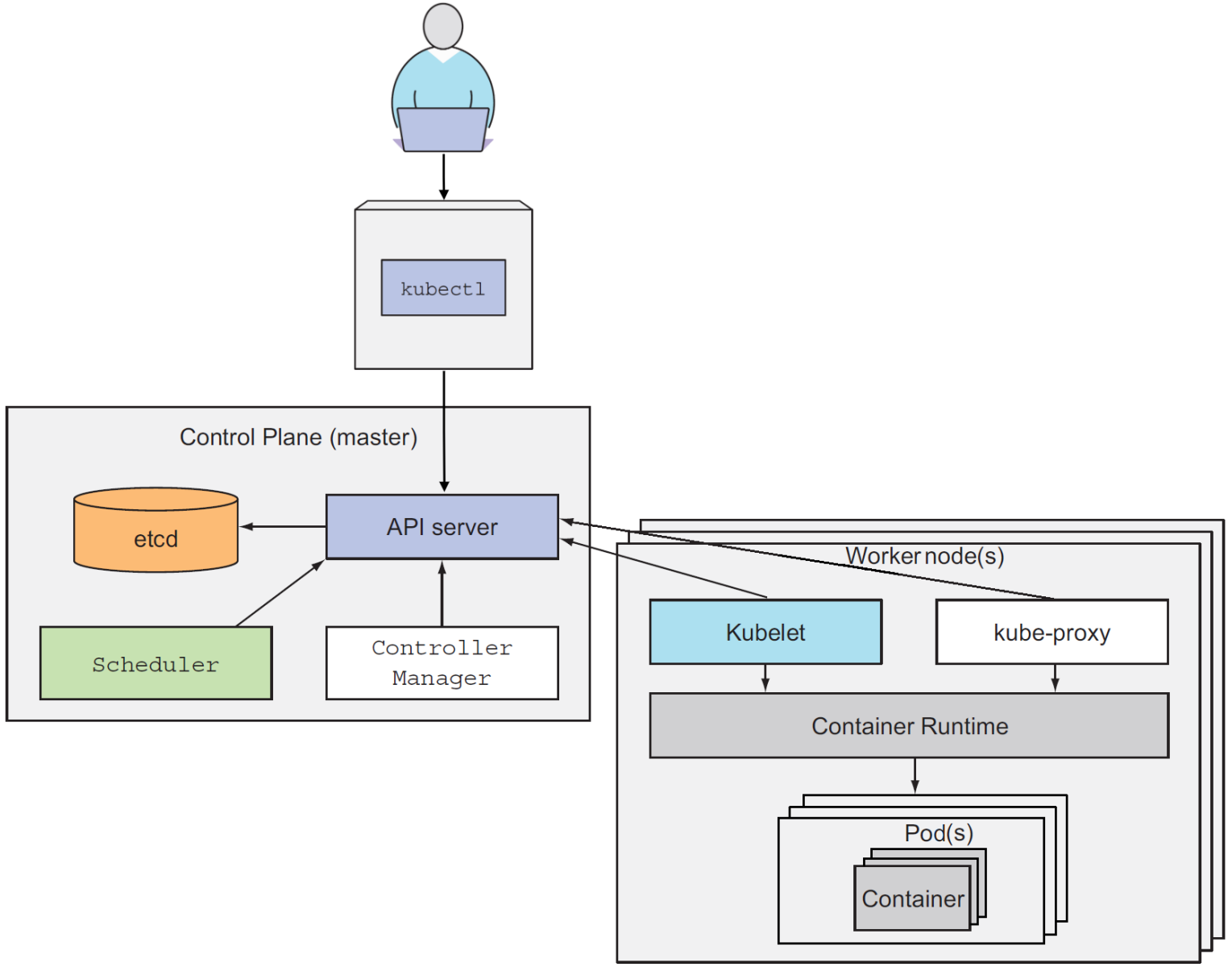
Motivación



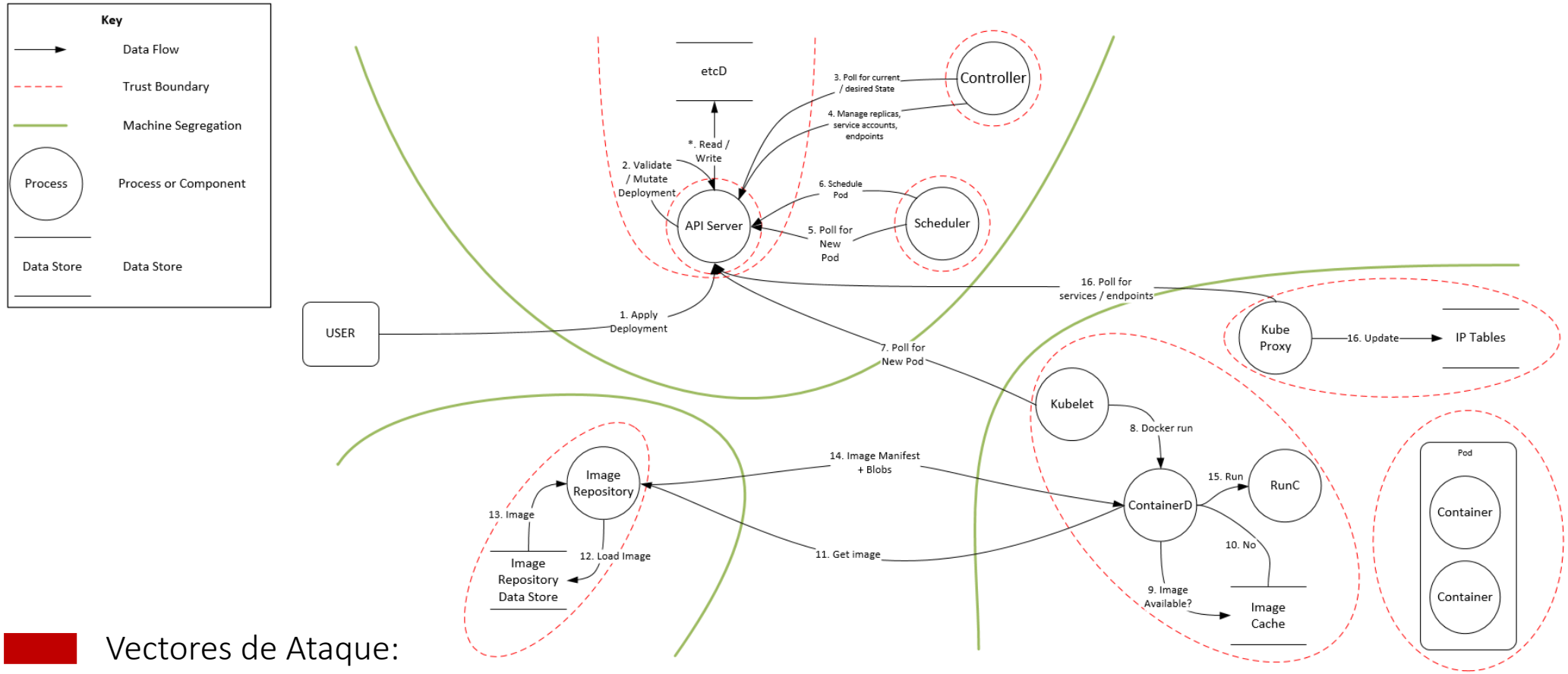
Objetivos

- Revisar los principales vectores de ataques que afectan a Kubernetes.
- Asociar los vectores de ataque con las vulnerabilidades recogidas en CVE.
- Revisar las principales prácticas de seguridad para Kubernetes.

Kubernetes: Arquitectura básica



Vectores de Ataque



- Vectores de Ataque:
  - Service Token
  - Network Endpoint
  - RBAC Issues
  - Compromised container
  - Denial of Service

https://github.com/cncf/financial-user-group/tree/main/projects/k8s-threat-mod

Estudio de Vulnerabilidades

Cloud provider

Credentials:
- AWS Keys
- Tencent Keys
- Alibaba Keys

Networking:
- Load Balancer
- Region & AZ
- VPC
- Instance IP & ID

K8s cluster

Components:
- Kube-proxy
- Kube-admin
- Kubelet

Topology:
- Cluster IP
- Namespaces
- Nodes

Known Vulnerab(s):
- CVE-2020-8554
- CVE-2020-8558
- CVE-2020-8559
- CVE-2021-25735
- CVE-2021-25737
- CVE-2021-25741

Node

Node:
- Kernel
- OS
- Go version
- Git version
- Docker

Known Vulnerab(s):
- CVE-2022-0847
- CVE-2022-0185
- CVE-2018- 18955
- CVE-2021-3156

Pod/Container

Registry:
- docker.io

Image:
- Image-id

Service:
- Service-example
  - Website
  - API
  - …
  - https://example.com

Known Vulnerab(s):
- CVE-2021-44521
- CVE-2020-28035
- CVE-2018-16850
- CVE-2019-11043
- CVE-2021-44228
- CVE-2022-22963
- CVE-2020-13942

Kubernetes Secrets:
- Service auth tokens

Clasificación de Vulnerabilidades

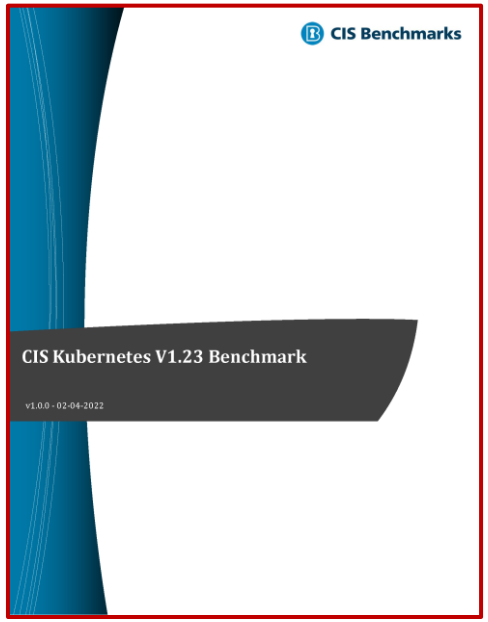
Vector de Ataque	Vulnerabilidades	Vulnerabilidades (%)
Service Token	13	9.3
Compromised container	32	23
Network endpoints	10	7.1
Denial of Service	3	2.1
RBAC Issue	3	2.1
Total	61	43.6

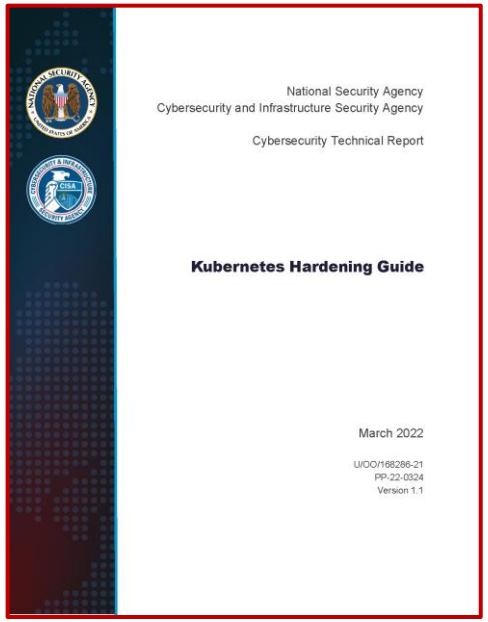
- 140 vulnerabilidades relacionadas con Kubernetes fueron recopiladas en CVE.
- 43.6 % de las vulnerabilidades de CVE[3] se relacionan con los vectores de ataques definidos.
- 23% se relacionan con el vector de ataque *compromised container*.

[3] https://cve.mitre.org/

Metodología

- Para resumir las buenas prácticas se ha utilizado la siguiente metodología:
  - Artículos científicos
  - Especificaciones técnicas
  - Artefactos de internet: *white papers*, *blogs y vídeos*.

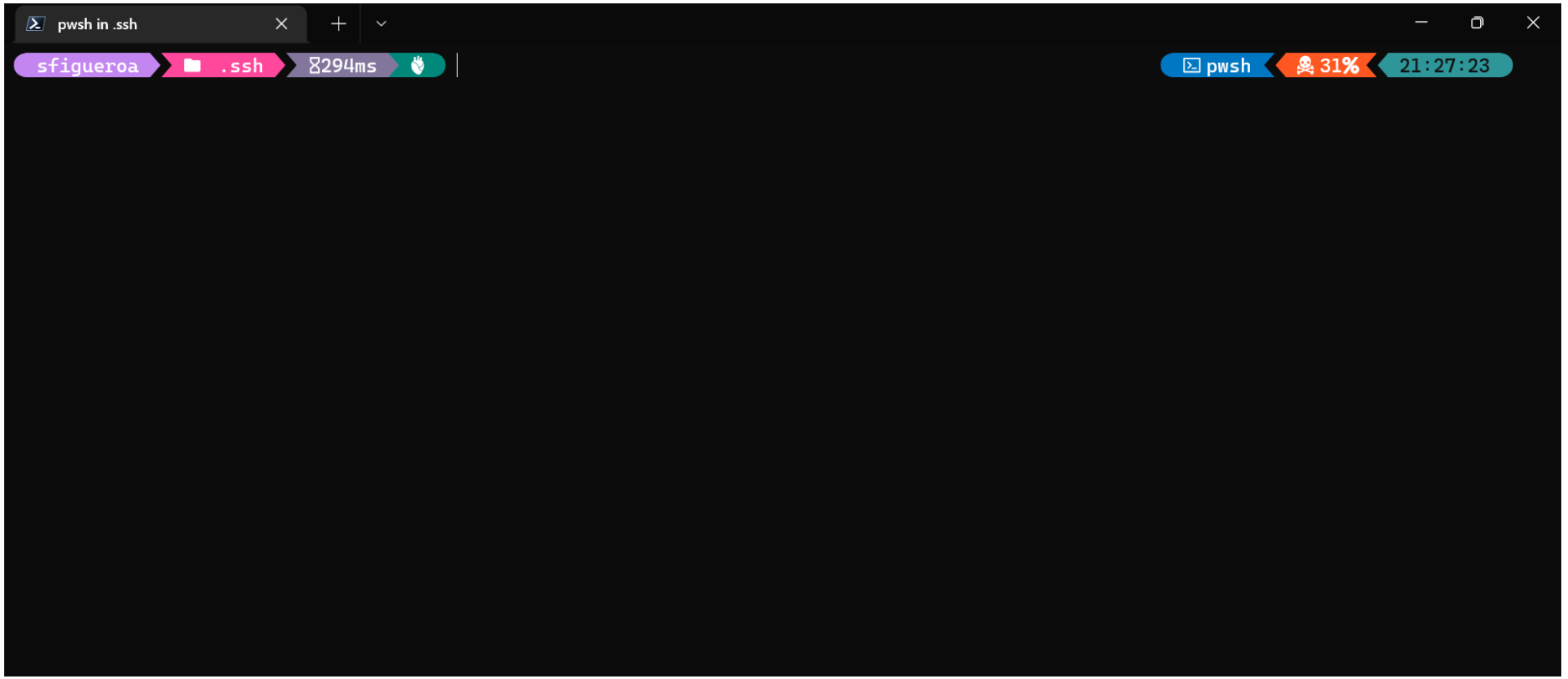




Buenas prácticas de seguridad

- Authentication and Authorization
- Kubernetes Security policies
- Vulnerability Scanning
- Logging
- Namespace separation
- Etcd security: encryption and access
- Continous update
- Sandbox Technologies
- TLS support in Kubernetes
- Separate sensitive workload
- Access to metadata
- CPU and memory limits

Demo



https://github.com/sfl0r3nz05/Conferences/blob/main/JNIC_2022/demo/Demo1_Confirm_Pod_Security_is_enabled.md