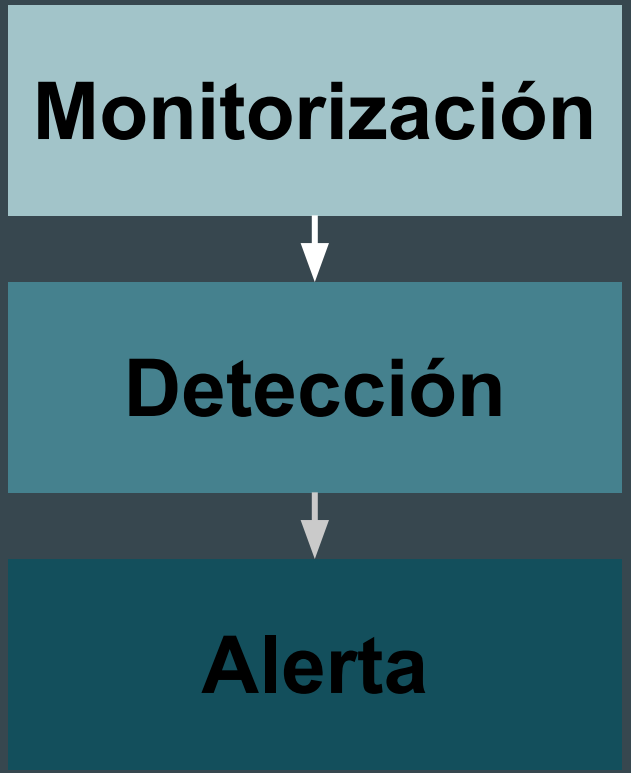
IoT Vigilant

...

Hackathon Cybercamp

Málaga 2018

Detección de amenazas en dispositivos IoT basada en comportamientos anómalos



Arquitectura

Sniffer

Captura de tráfico - Scapy/Netflow

Procesado básico

Envío de información al server

Servidor local

API Rest para recolección de información
Gunicorn + Flask

Envío de datos a la DB
Elasticsearch

Representación de los datos
Grafana

Detector de anomalías

Recolección de datos agregados
Elasticsearch

Modelado de comportamiento y detección
Suma de Gaussianas

Almacenamiento de los resultados
Elasticsearch

DEMO