Wall-do

zionSpartans

Andoni Alonso Fernández
Rafael Villaverde González

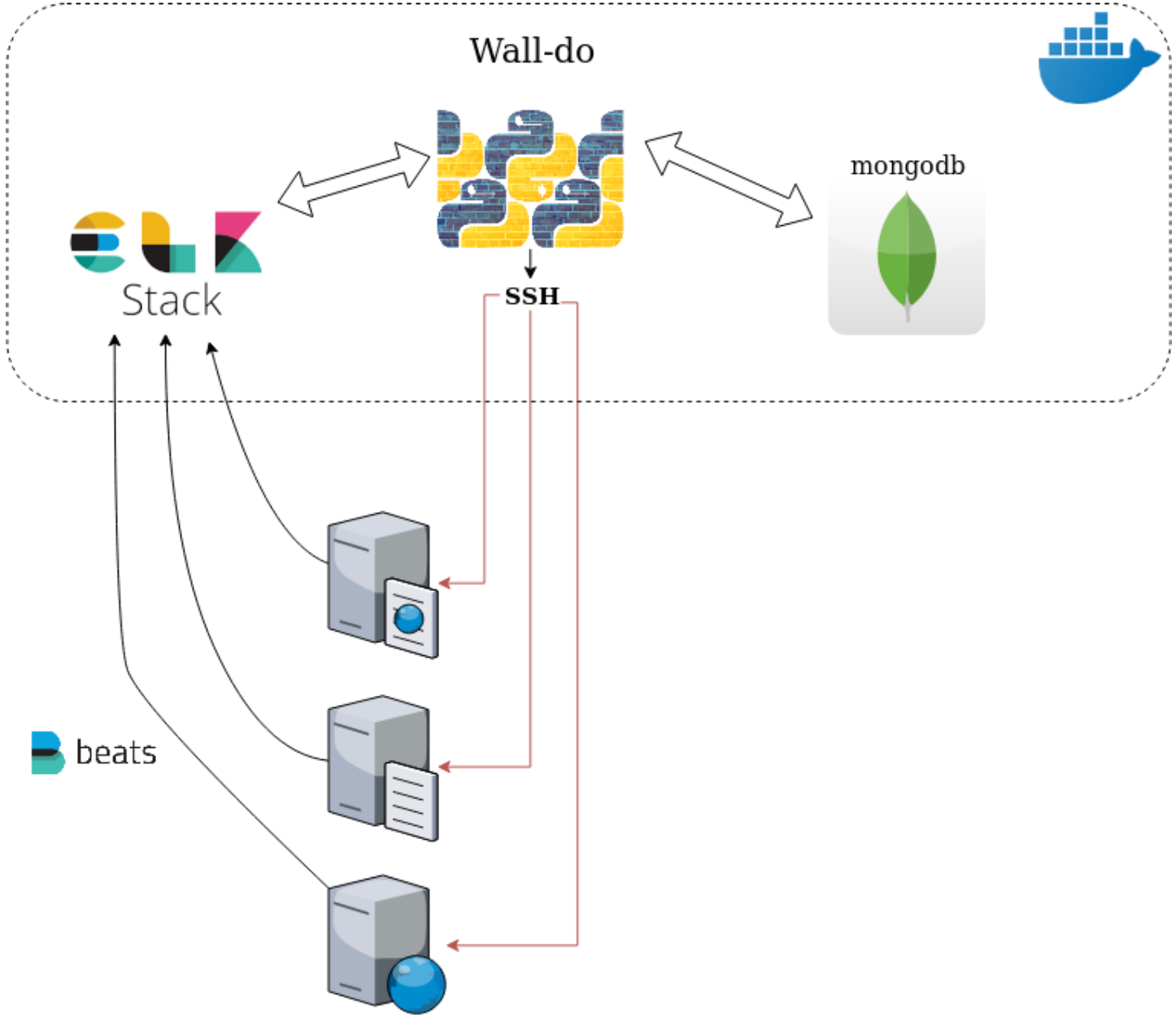
- Herramienta para la detección y prevención de ataques.

- Inspirada en fail2ban, pero de forma distribuida.

- Analiza la interacción de las diferentes IPs en los logs a traves de ELK.

- Se basa en la frecuencia de interacción, comportamiento y el contraste con blacklist.

- En base a esta puntuación se determinan las acciones a realizar.


Wall-do
mongodb
Stack
SSH
beats

Planteamiento general para la competición

- Desarrollo de dos ejemplos de uso:
  - Conexiones SSH
  - Fail2ban

- Fases:
  - Extracción y tratamiento de la información de Elasticsearch
  - Consulta blacklist
  - Calculo de puntuaciónes de las IPs
  - Ejecución de medidas: Alerta via telegram y baneos temporales.