HoneyPots

Javier Béjar Méndez
Antonio Jose Rodriguez Alaminos

HoneyPots

Motivación

Cada año:

- Número de ataques
- Complejidad
- Herramientas para disimular sus acciones

Antiguamente:

- Reinstalación y actualización de equipos atacados
- Notificación al servidor atacante

Además, los atacantes:

- Borran su rastro
- Dejan binarios para recolección de datos y puertas traseras

HoneyPots ¿Qué son?

Es un sistema diseñado para analizar a los ciberdelincuentes mediante el uso de un servidor falso

Además desviamos la atención del servidor principal

Mediante

Herramientas de monitorización

Detectamos

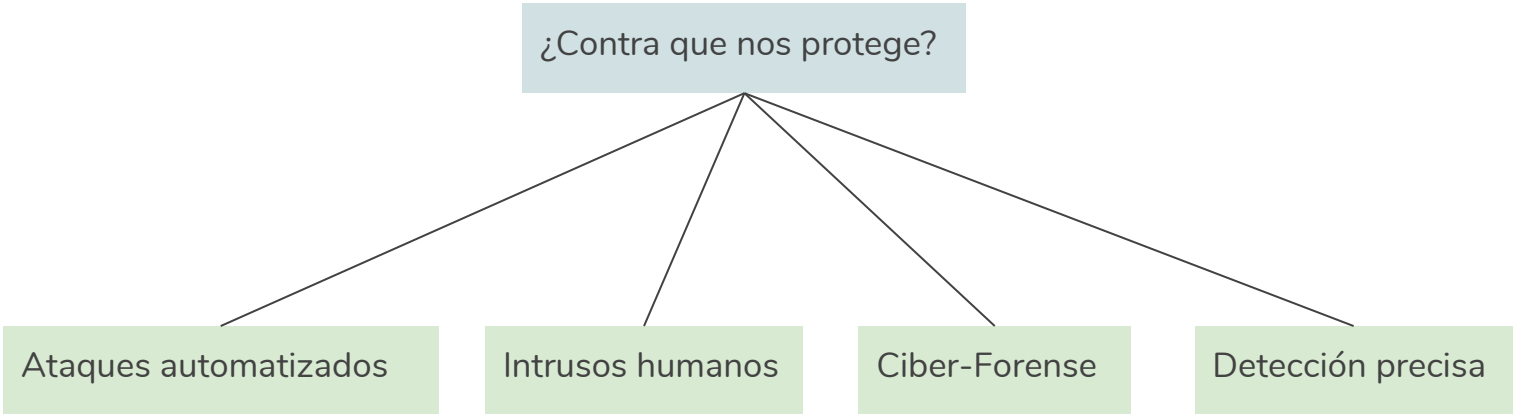
Vulnerabilidades

Perfiles de atacantes

Nuevos malwares

HoneyPots

Prevención de ataques

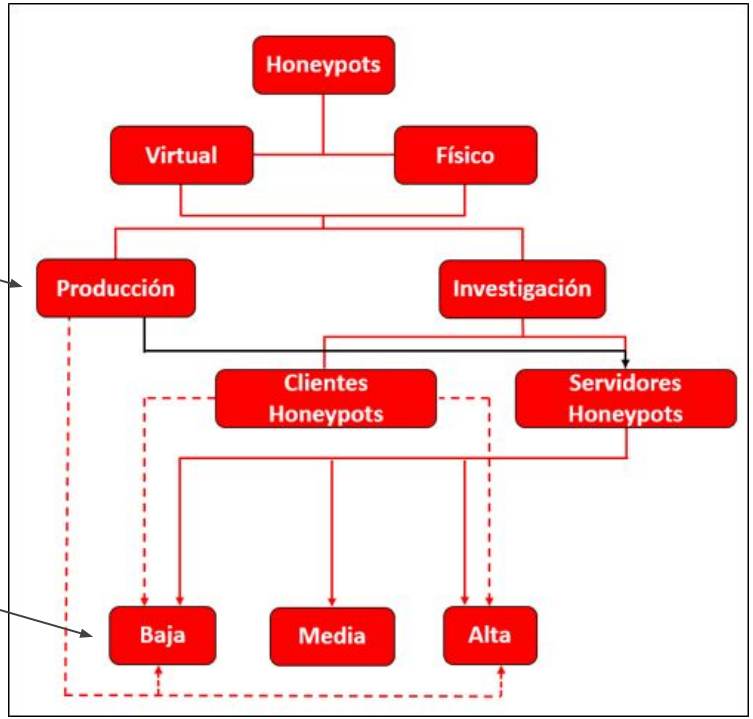


HoneyPots

Clasificación

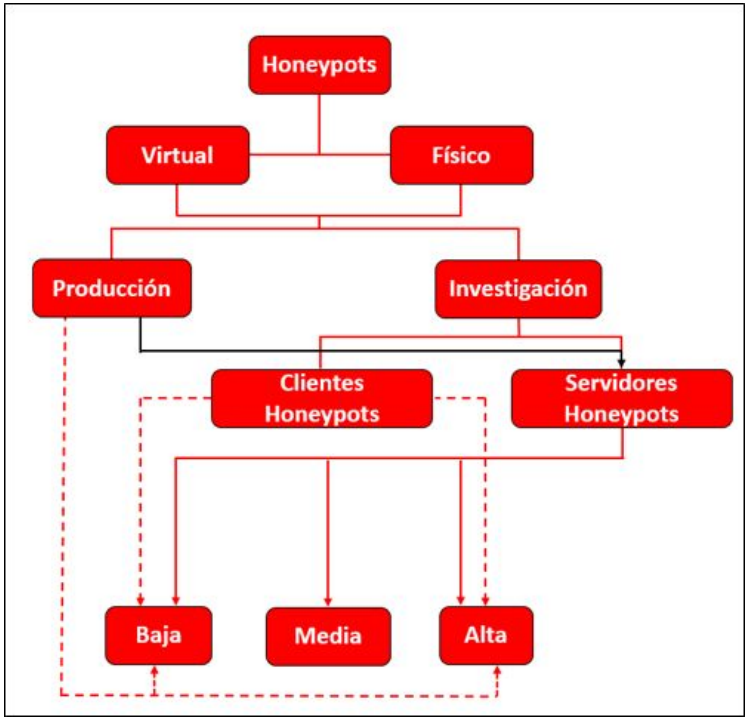
Ambiente de implementación

Nivel de interacción

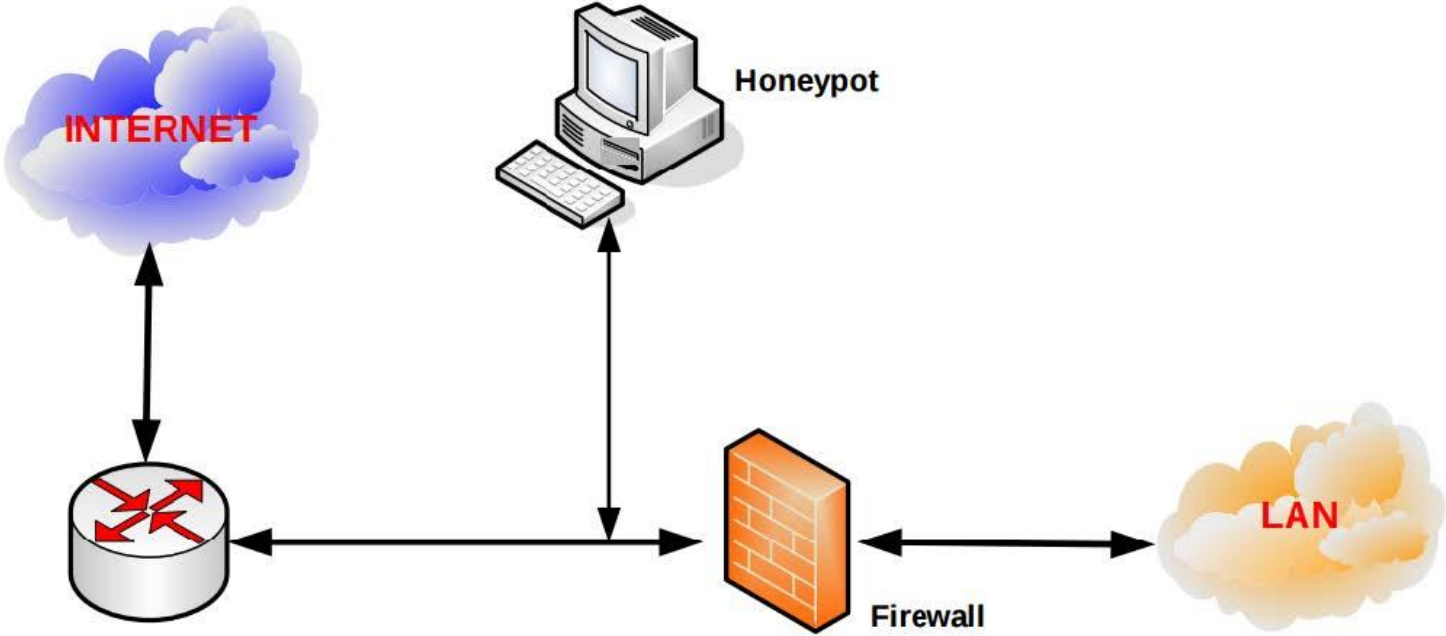


HoneyPots Clasificación

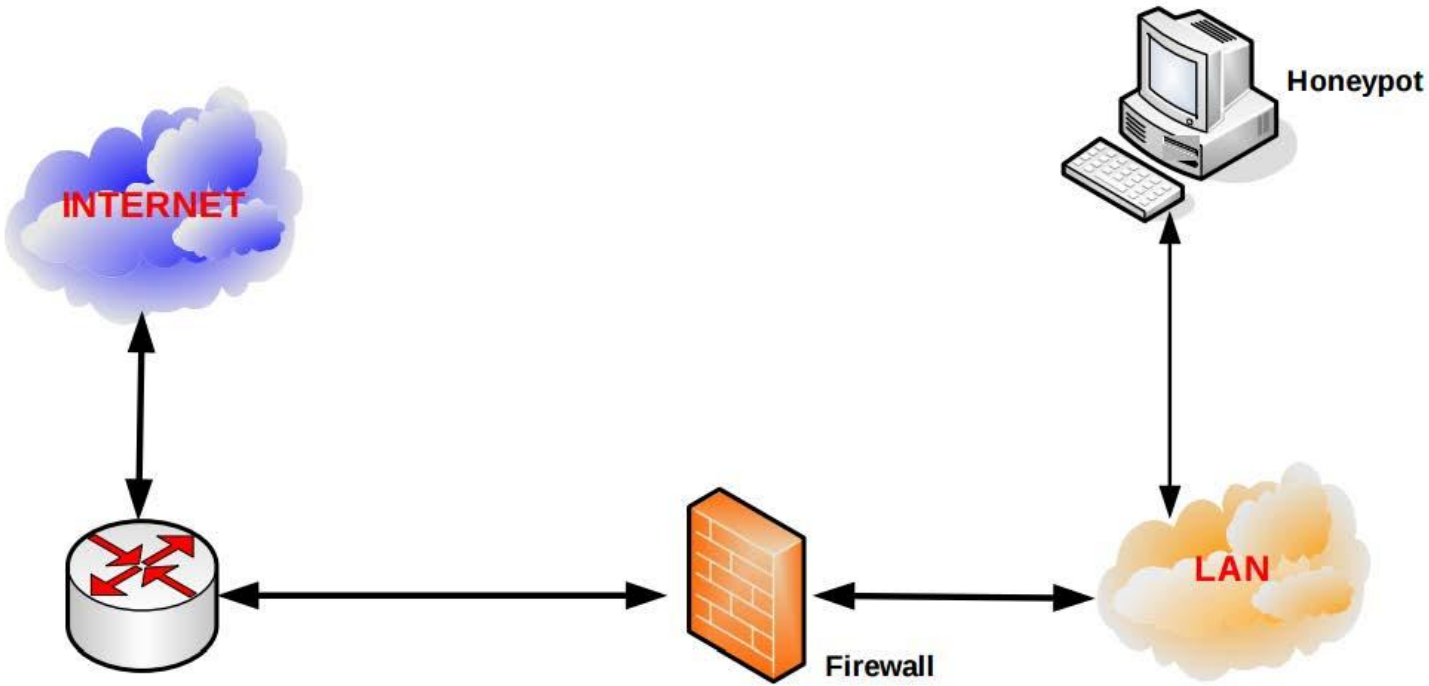
	Alta interacción	Baja interacción
Simulación	Simulan servicios reales, aplicaciones o dispositivos. Su identificación suele ser compleja.	Simulan servicios o sistemas operativos. Tiene muchas posibilidades de detectarse como trampa fácilmente.
Amenazas	Descubrir nuevos ataques o comportamientos anómalos anteriormente no detectados.	Descubrir herramientas automatizadas o de vulnerabilidades ya conocidas en servicios concretos.
Información	Capturan una gran cantidad de información de gran valor por contener en ocasiones registros de ataques no conocidos. Su implementación es perfecta para investigaciones y análisis en profundidad.	La cantidad de recursos recopilados es limitada. No son muy aconsejables si se quiere realizar un análisis en profundidad del sistema.



Ubicación

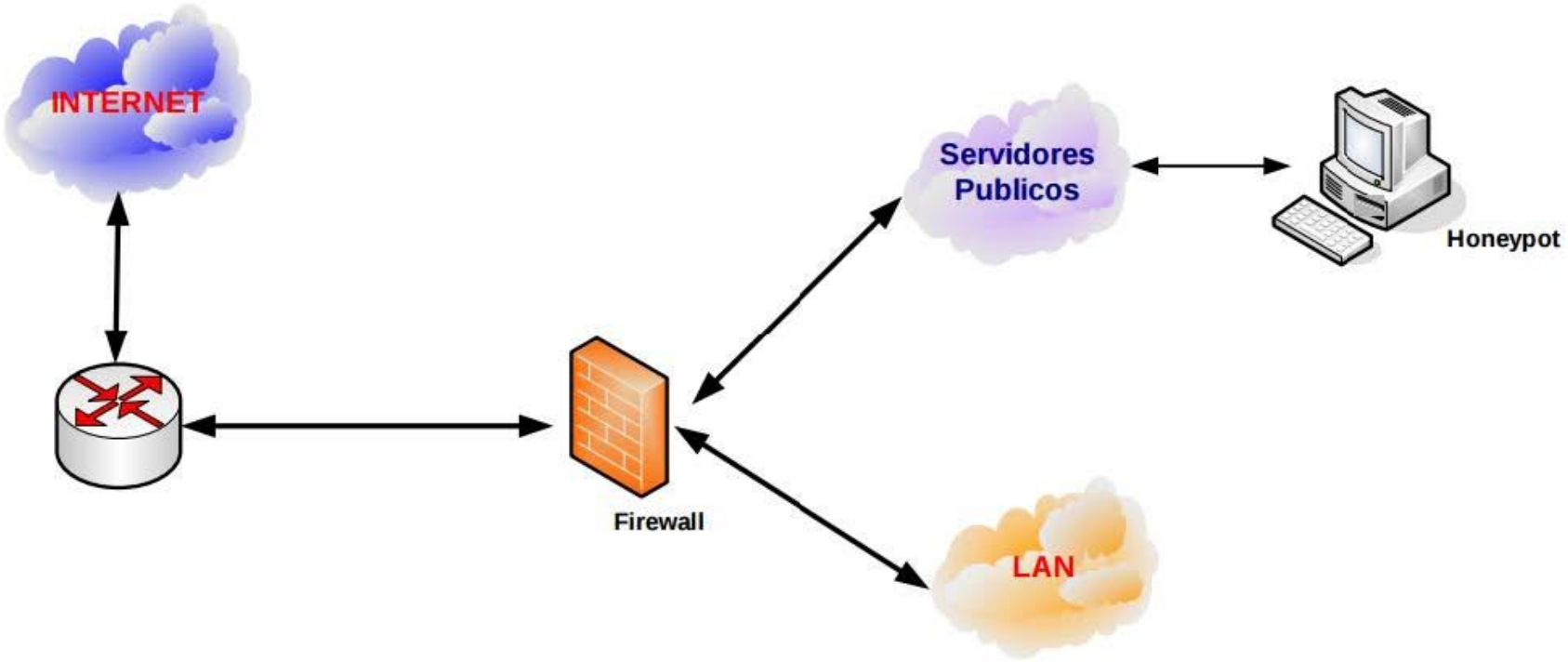


Ubicación



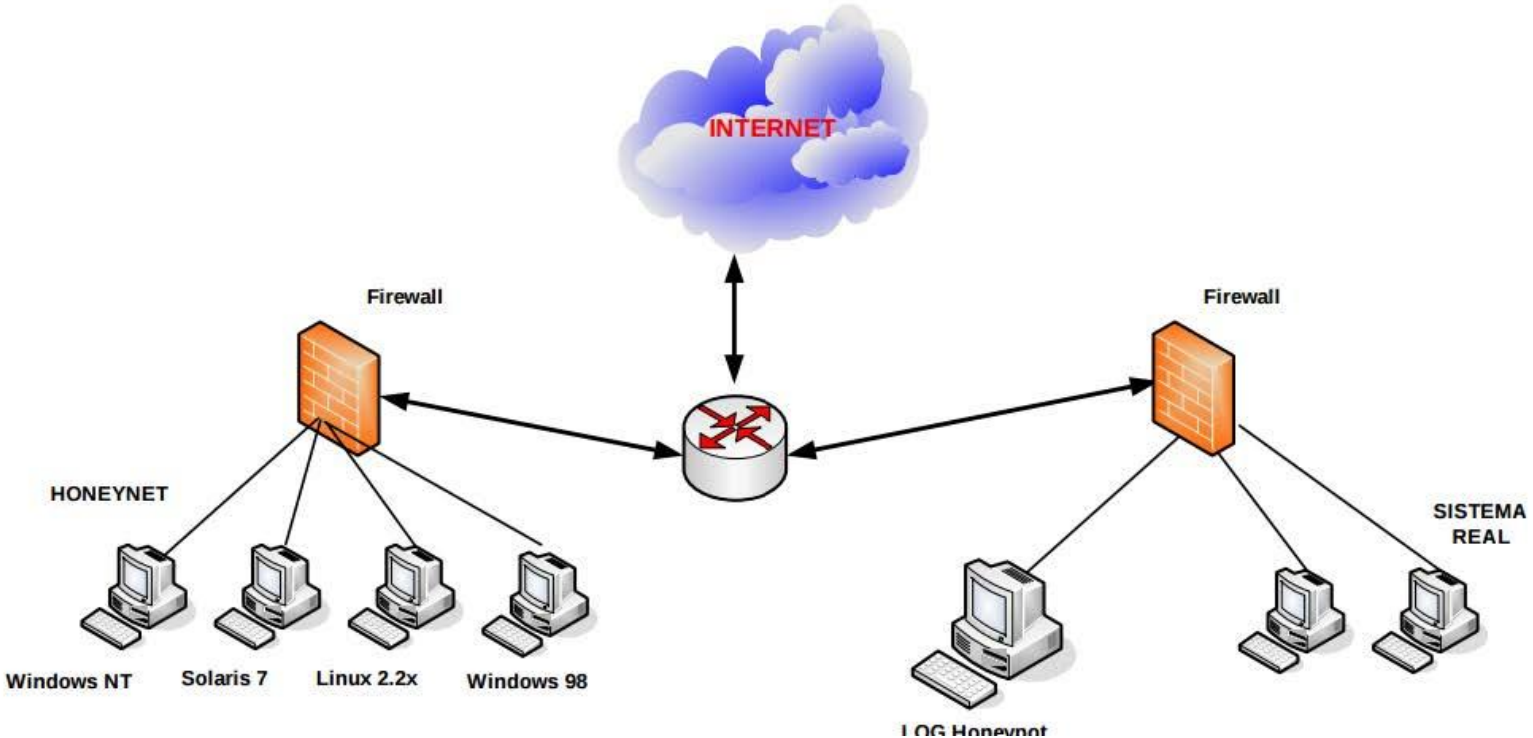
HoneyPots

Ubicación



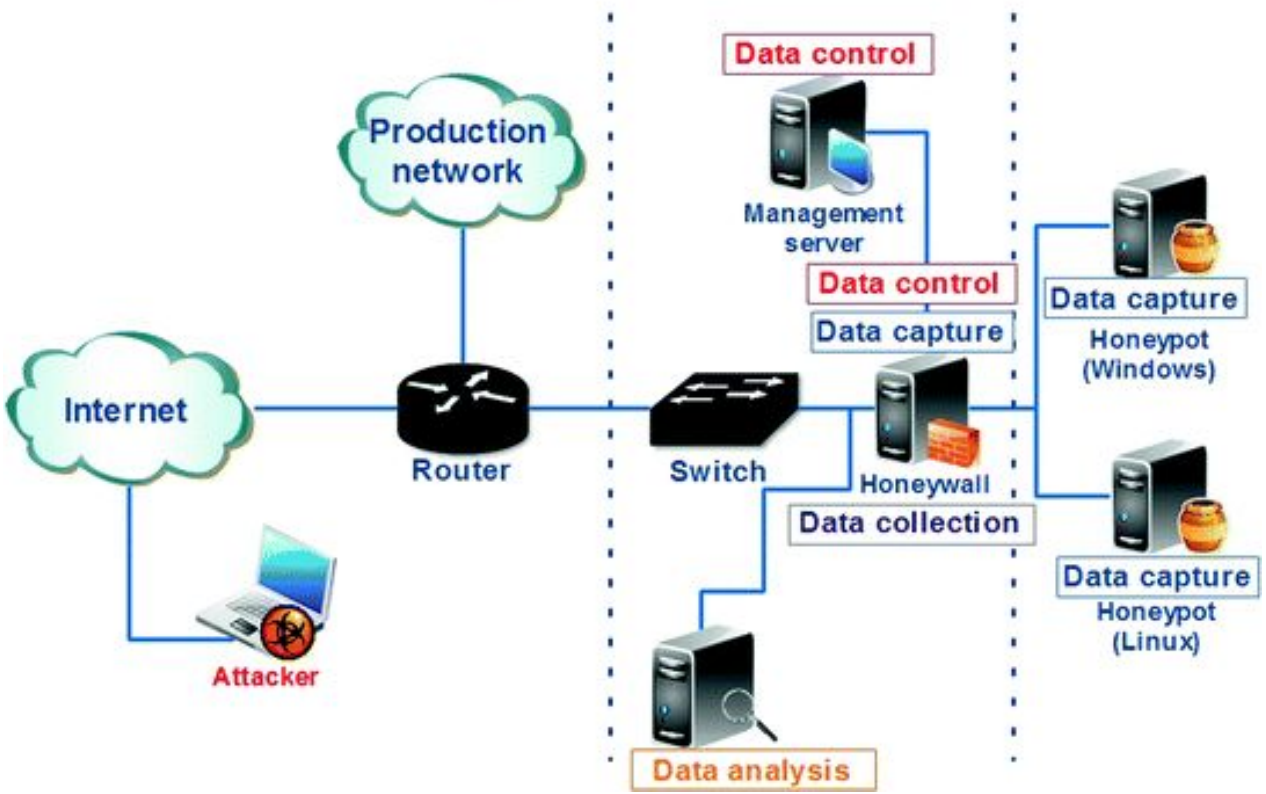
HoneyPots

HoneyNet



HoneyPots

HoneyNet



HoneyPots

Ventajas

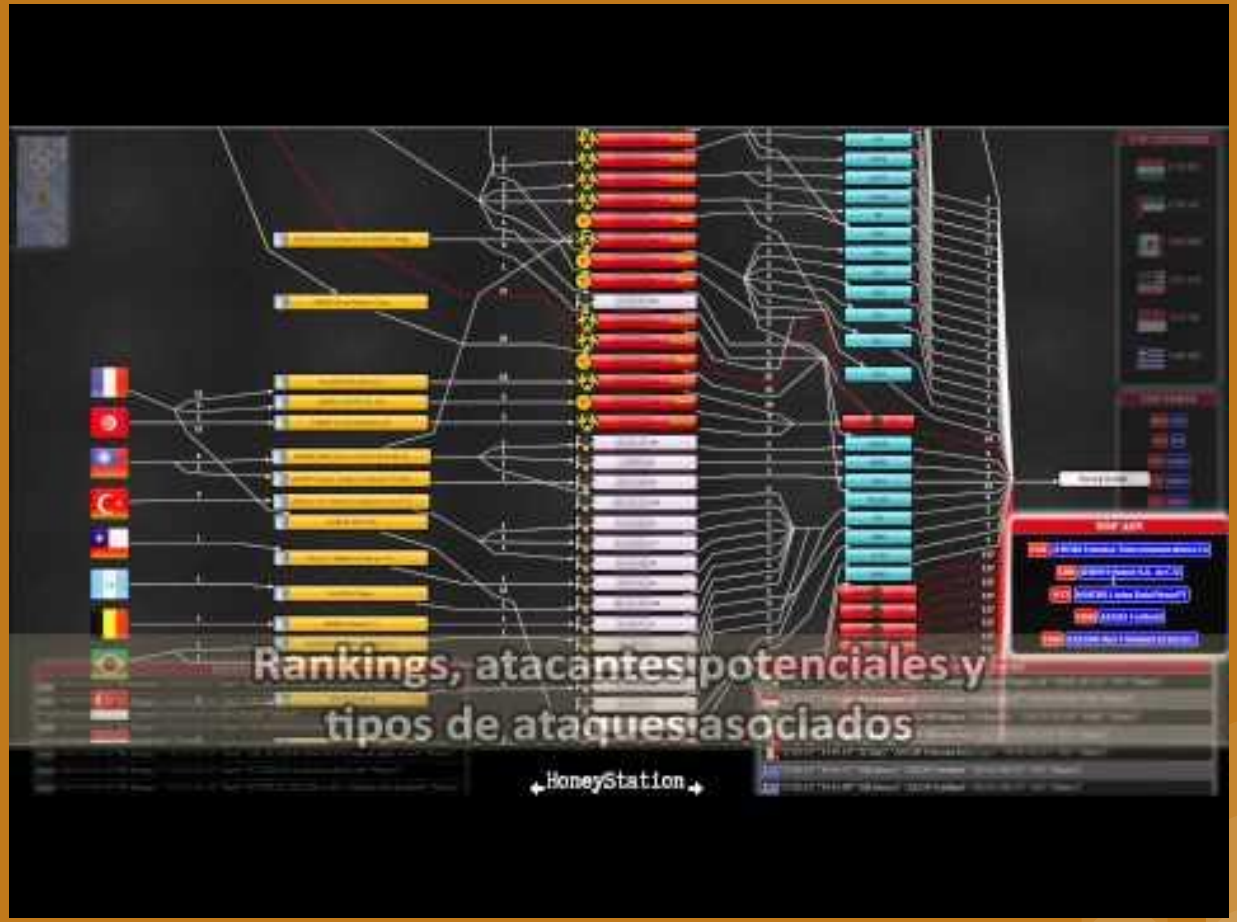
- Generan un volumen pequeño de datos, frente a los sistemas clásicos de seguridad, y datos de alto valor.
- Evade los falsos positivos.
- Se necesita recursos mínimos.
- Detecta tanto atacantes internos como externos.

Desventajas

- Son elementos totalmente pasivos, por lo que necesitan ser atacados para cumplir con su función.
- Son fuentes potenciales de riesgo para nuestra red.
- Consumen una dirección IP como mínimo.

Honeystation

Honeypot desarrollada en INCIBE


Rankings, atacantes potenciales y
tipos de ataques asociados
HoneyStation

Conclusiones

- Los Honeypots tienen un limitado carácter preventivo.
- Tienen un alto grado de detección.
- La reacción es otro de los valores que añade el uso de Honeypots.

¿Preguntas?