Universitat Oberta de Catalunya

uoc.edu

Implementación de un sistema de detección de intrusos IDS mediante la inspección del tráfico a través de la red

Autor: **Antonio Suárez Bono**
Director: Joan Caparrós Ramírez
Trabajo Final de Máster – Junio 2023
Máster Universitario en Ciberseguridad y Privacidad

Índice

Introducción: Contexto

Aumento constante de incidentes de seguridad en Internet y sistemas informáticos.

La adopción masiva de IoT en los hogares ha llevado a un aumento de las ciberamenazas.

Riesgos que van desde la vigilancia hasta el control total de dispositivos inteligentes.

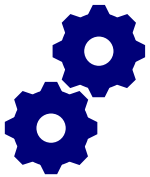
Importancia de considerar la seguridad desde el diseño.

Heterogeneidad de protocolos en dispositivos IoT como desafío principal.

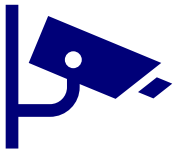
Introducción: Solución planteada

- Solución de bajo coste que permita detectar comportamientos anómalos o malintencionados.
- El análisis del tráfico debe realizarse a través de la red inalámbrica.
- Herramienta de análisis y visualización de eventos.

Introducción: Objetivos



Configuración del hardware para la implementación del sistema.

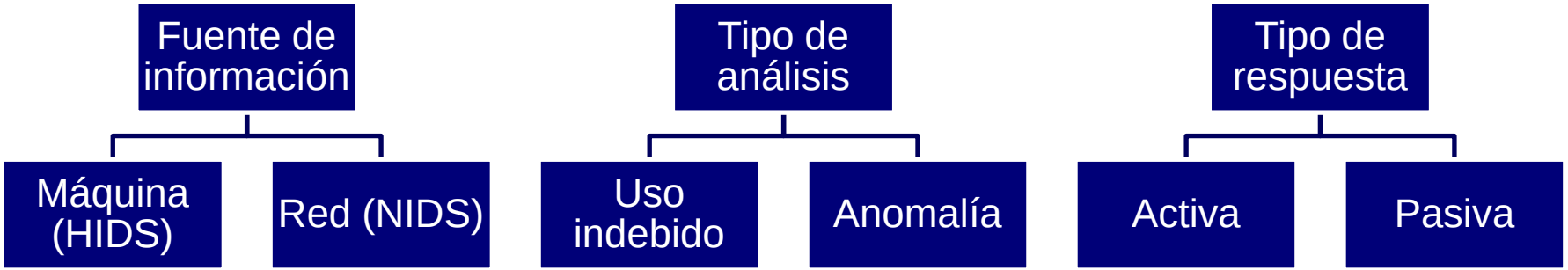


Instalación y configuración de un sistema de detección de intrusos.

Instalar y configurar la herramienta de análisis y visualización los datos.

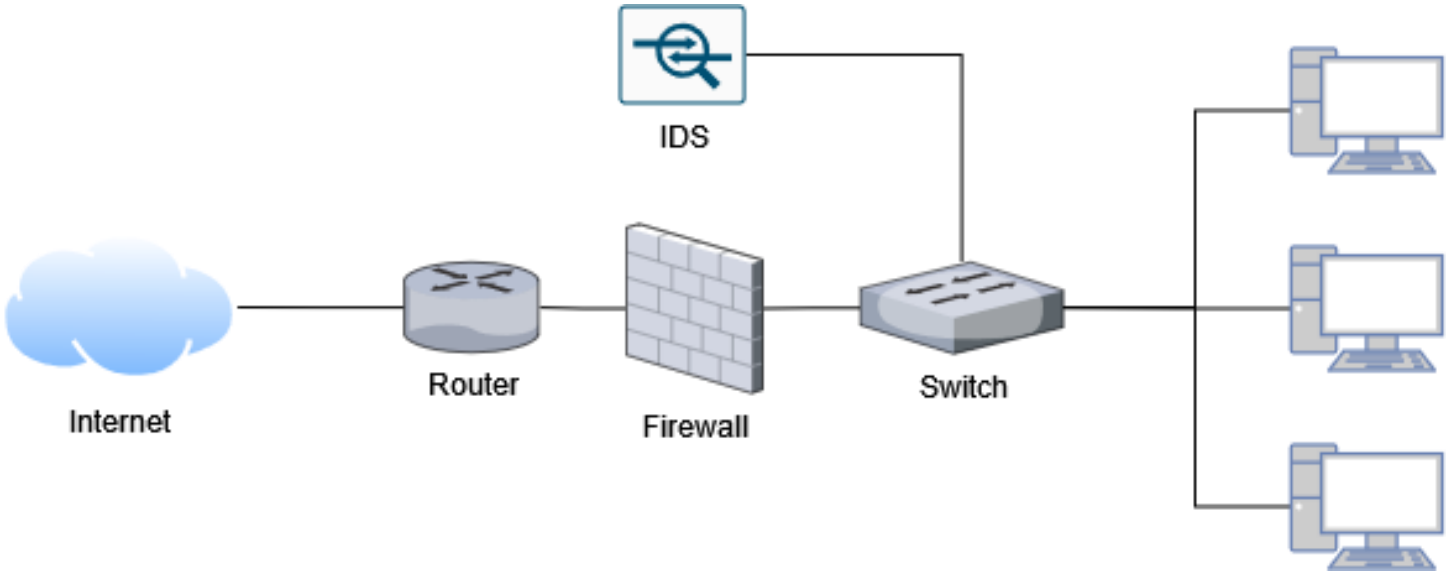
Investigación: Sistemas de Detección de Intrusos

Taxonomía



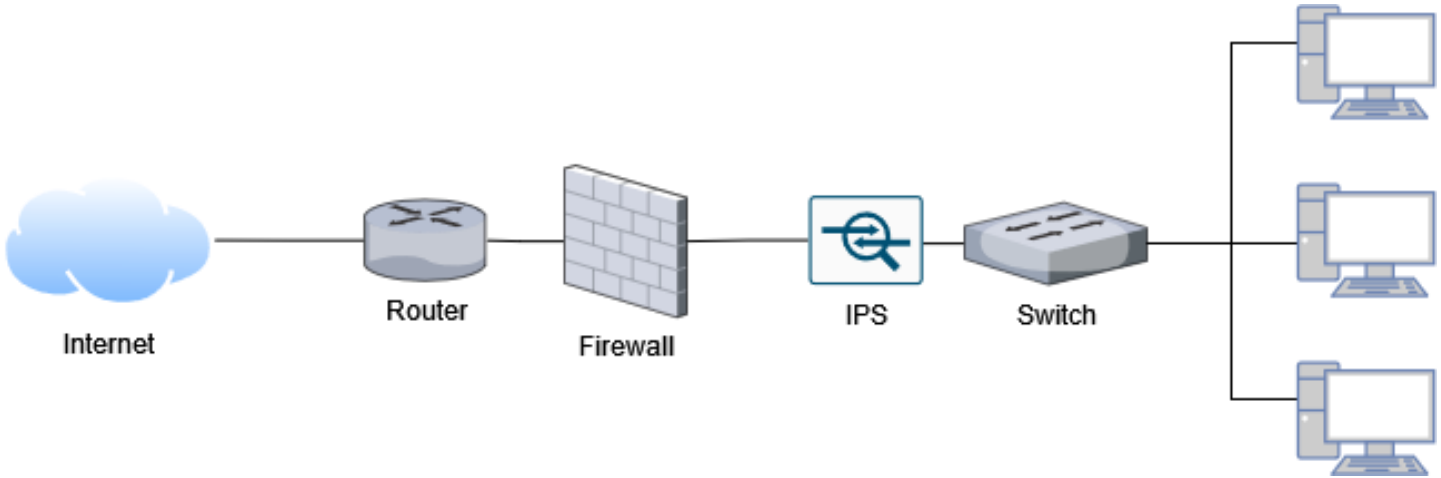
Investigación: Sistemas de Detección de Intrusos

Modelo de arquitectura fuera de línea



Investigación: Sistemas de Detección de Intrusos

Modelo de arquitectura en línea

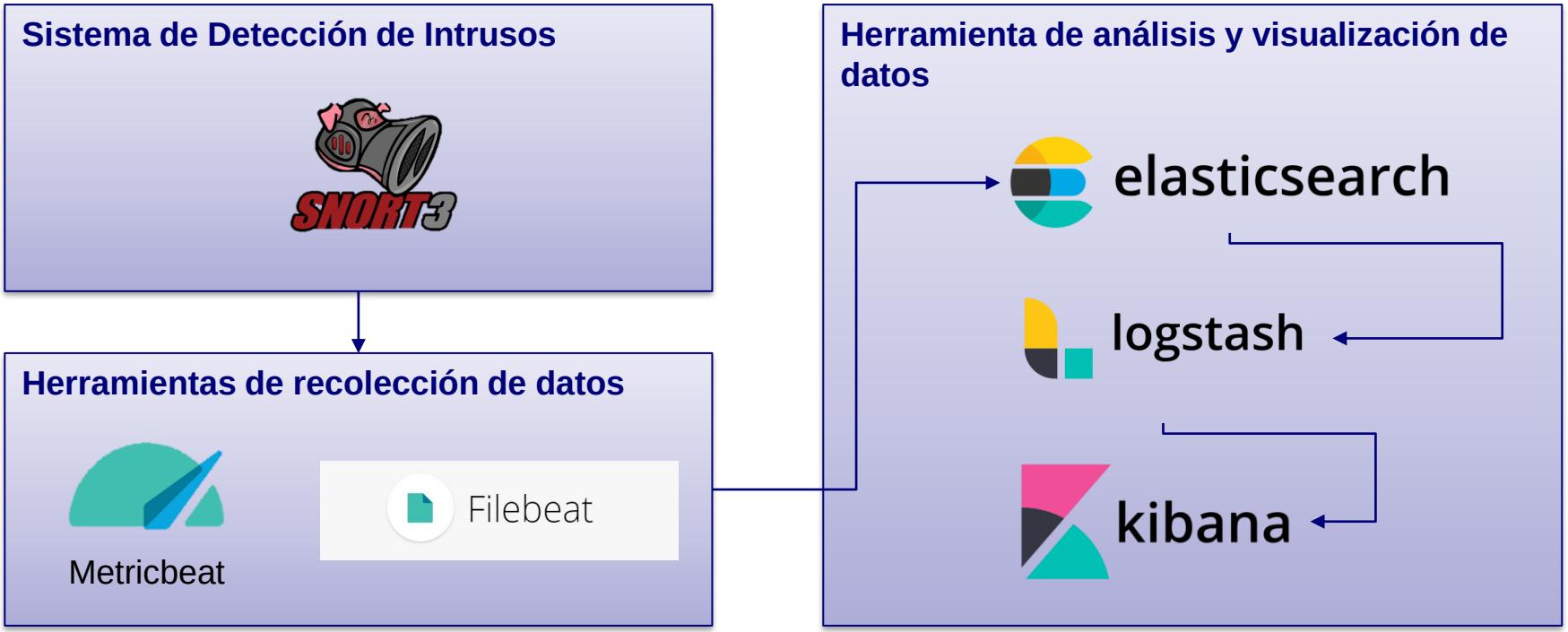


Investigación: Análisis y Visualización de Datos

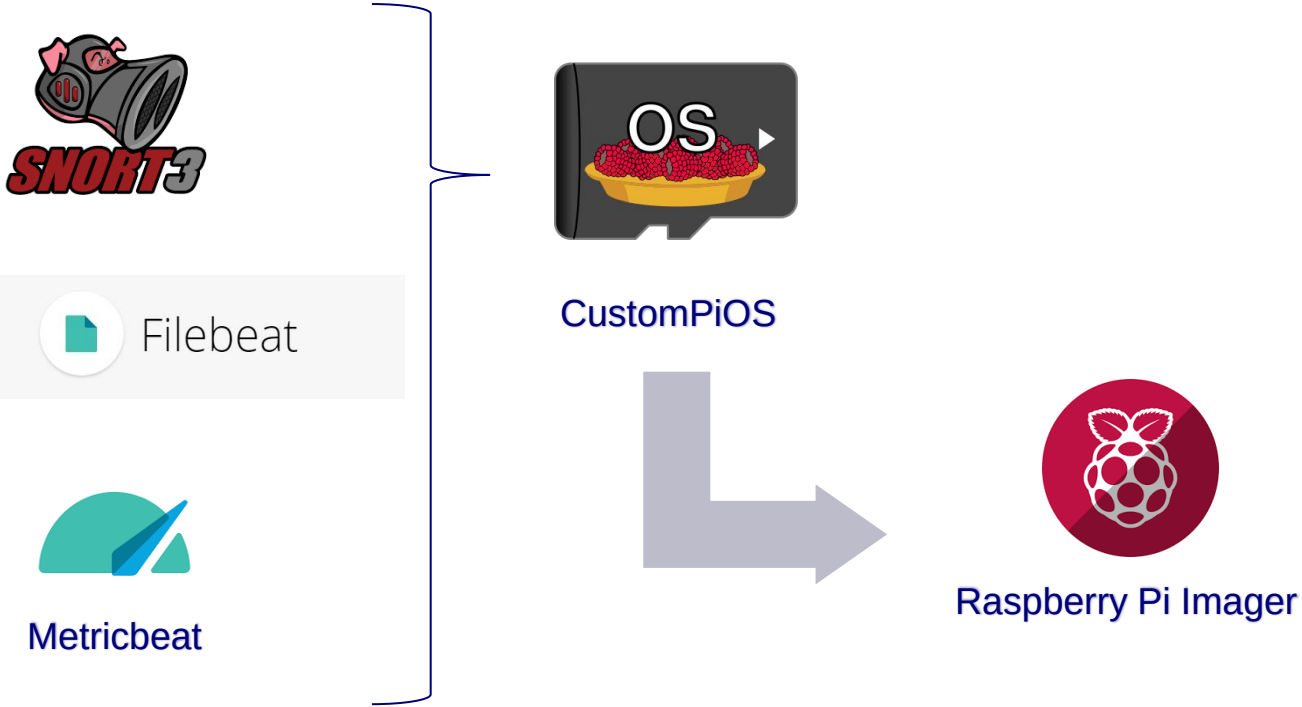
¿Que se busca?:

- Recopilación de datos.
- Almacenamiento y búsqueda de datos.
- Análisis y agregación de datos.
- Visualización de datos.
- Monitorización y alertas.

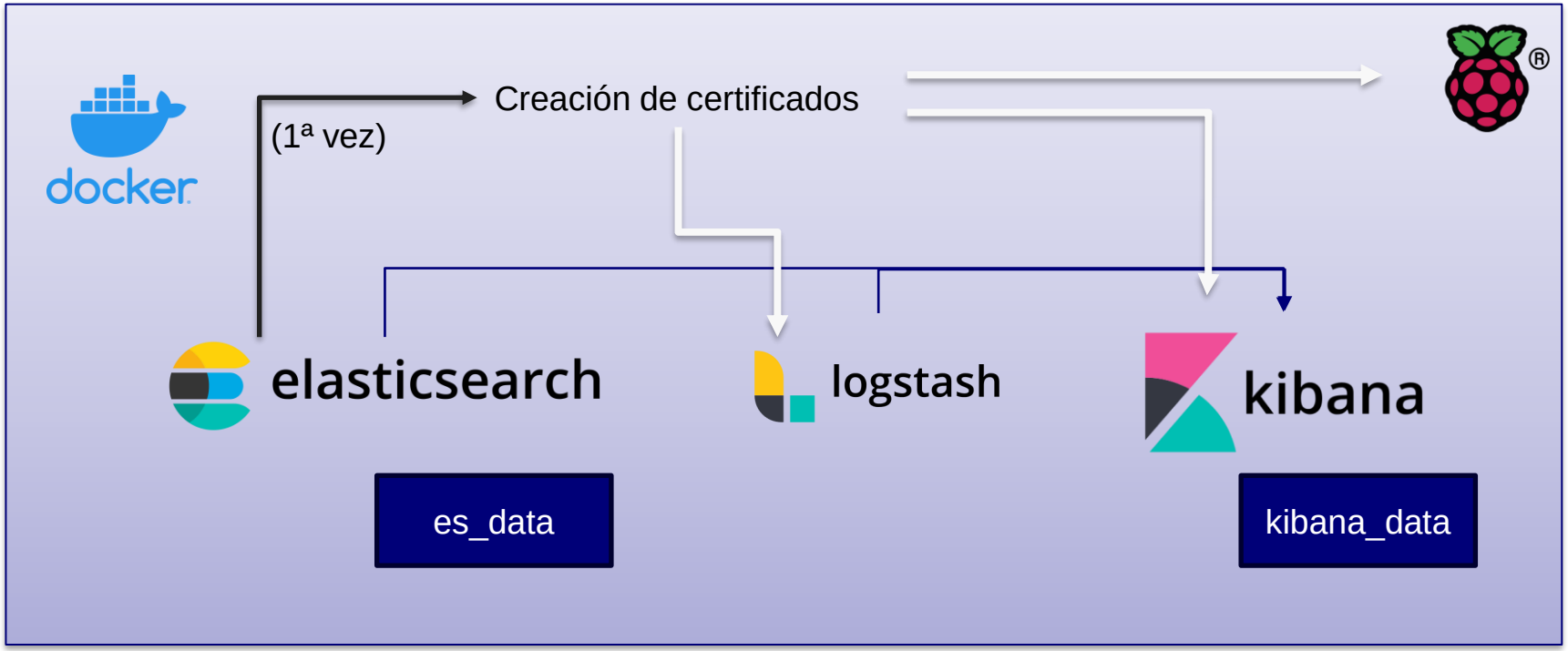
Investigación: Tecnologías seleccionadas



Implementación: Configuración del Raspberry Pi



Implementación: Pila de aplicaciones ELK



Implementación: Problemas encontrados

- Crisis de los semiconductores
- Instalación costosa a nivel de hardware
- Recursos necesarios para ejecutar la pila de aplicaciones ELK
- Configuración de certificados para Elasticsearch
- Imposibilidad de implementar un IDS fuera de línea

Optimización y Pruebas: Reglas de Snort

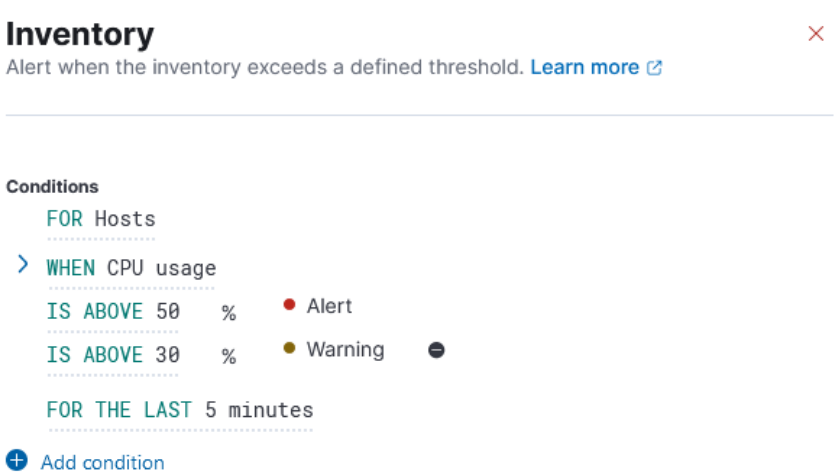
Escaneo de red

- Peticiones ICMP de tipo ECO
- Escaneo de puertos TCP
- Escaneo de puertos TCP FIN

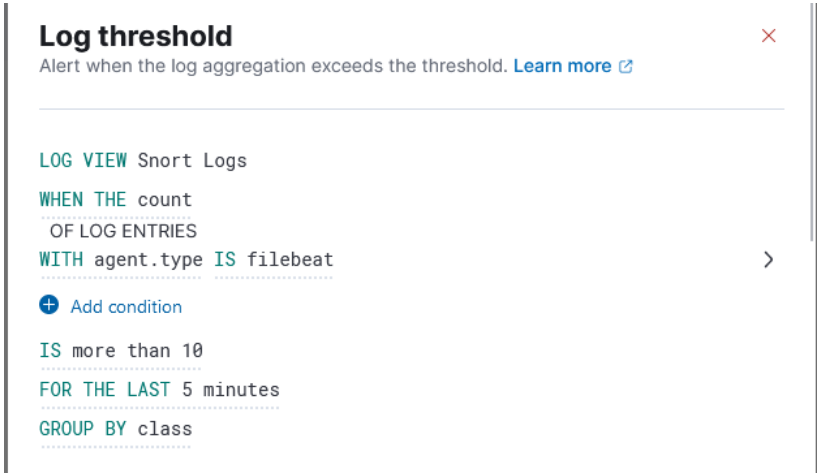
Detección de información de identificación personal

- Documento Nacional de Identidad
- Código Internacional de Cuenta Bancaria
- Fechas en formato DD/MM/YYYY
- Direcciones de correo electrónico

Optimización y Pruebas: Alertas de Kibana

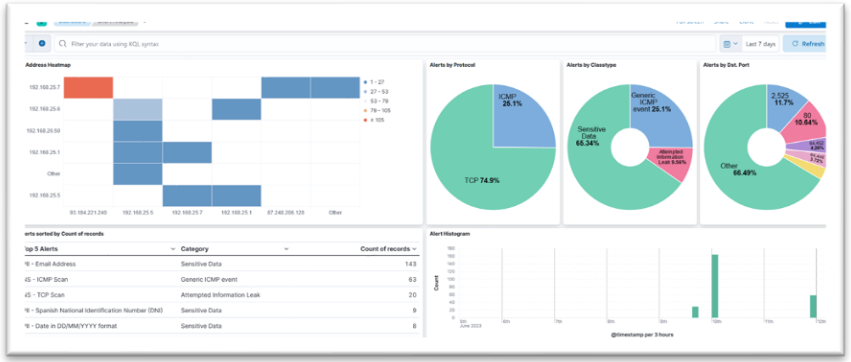


CPU Usage Alert

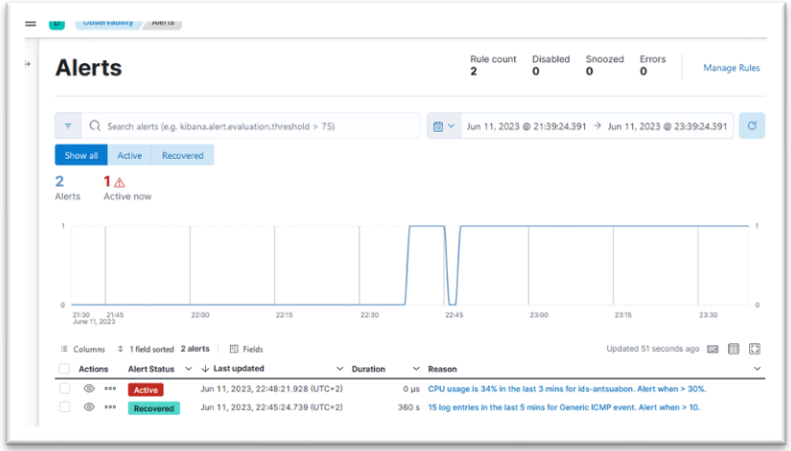


Snort Alert by Class Threshold

Demostración



Dahboard de Kibana



Alertas de Kibana

Conclusiones

- Investigación herramientas que facilitan la instalación en dispositivos con recursos limitados.

- Desarrollo de un conjunto de reglas de prueba para Snort, que permiten detectar:
  - Escaneos de red.
  - Patrones de información de identificación personal.

- Desarrollo de un conjunto de alertas para que Kibana notifique a los usuarios cuando se encuentre una determinada condición en:
  - Registro de alertas de Snort.
  - Métricas del dispositivo Raspberry Pi.

- Se ha logrado conectar Kibana a un conectar de correo electronico para el envío de notificaciones.

Conclusiones

- No ha sido necesario el uso de Logstash debido a que Snort 3 es capaz de generar salidas en formato JSON.

- La pila de herramienta ELK consume demasiados recursos como para ser instalada en el dispositivo Raspberry Pi junto al Sistema de Detección de Intrusos.

- Flexibilidad de la herramiente de visualización y análisis de datos:
  - Diagramas de sectores.
  - Histogramas.
  - Tablas.
  - Etc.

Trabajos futuros

- Profundizar en la creación de reglas para Snort:
  - Extender la detección de información de identificación personal.
  - Detección de huellas malware conocidas.
  - Detección de ataques de denegación de servicios.
- Explorar alternativas hardware con mejores recursos y velocidad de procesamiento.
- Buscar sistemas de detección de intrusos compatibles con la captura de datos en redes inalámbricas, es decir, con arquitectura fuera de línea.
- Vías alternativas para enviar las alertas de Kibana:
  - Telegram, SMS, WhatsApp, etc.

Universitat Oberta de Catalunya

uoc.edu

¡Muchas gracias!

Antonio Suárez Bono

Trabajo Final de Máster

Máster Universitario en Ciberseguridad y Privacidad