Monitoreo de Seguridad

WALC, 2022

Track de Ciberseguridad

Por: Sheyla Leacock

Sheyla Leacock

- Licenciada en Desarrollo de Software (UTP). Cursando un Máster en Ciberseguridad, Hacking Ético y Seguridad Ofensiva (UEMC-EIP).
- Líder de Women of Security (WoSEC) Panamá, Embajadora de la Fundación Comunidad Dojo y Community Builder de AWS.
- Oficial de Seguridad de la Transformación Digital e Instructora de cursos de Seguridad Informática.
- Ponente internacional en conferencias de Ciberseguridad y Tecnologías.
- Con certificaciones y especializaciones en AWS, ciberseguridad, redes (CCNA), administración de servidores Linux, entre otras.

shey.lck@gmail.com

https://www.linkedin.com/in/sheyla-leacock/

Contenido

- Monitoreo de Seguridad
- ¿Qué es un SOC?
- ¿Qué es un SIEM?
- Introducción a Wazuh
- Taller de implementación de Wazuh

Objetivos

- ➔ Conocer los conceptos de SOC y monitoreo de seguridad.
- ➔ Comprender el funcionamiento y arquitectura de un SIEM.
- ➔ Emplear técnicas de instalación y configuración de un SIEM.
- ➔ Inspeccionar los métodos de ingesta de logs en un SIEM.
- ➔ Identificar técnicas de monitoreo y análisis de logs.

Requerimientos para el taller

1.Tener instalado VirtualBox: https://www.virtualbox.org/wiki/Downloads

2. Tener una máquina virtual con Ubuntu y / o una máquina virtual con Windows 10

Máquinas Linux listas para importar en: https://www.osboxes.org/

Máquinas Windows listas para importar en: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

3. Descargar la OVA de Wazuh: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

Monitoreo de seguridad

Consiste en monitorear infraestructuras, usuarios y aplicaciones, con el objetivo de **identificar** posibles **amenazas** y **responder oportunamente** ante incidentes de ciberseguridad.

¿Qué es un SOC?

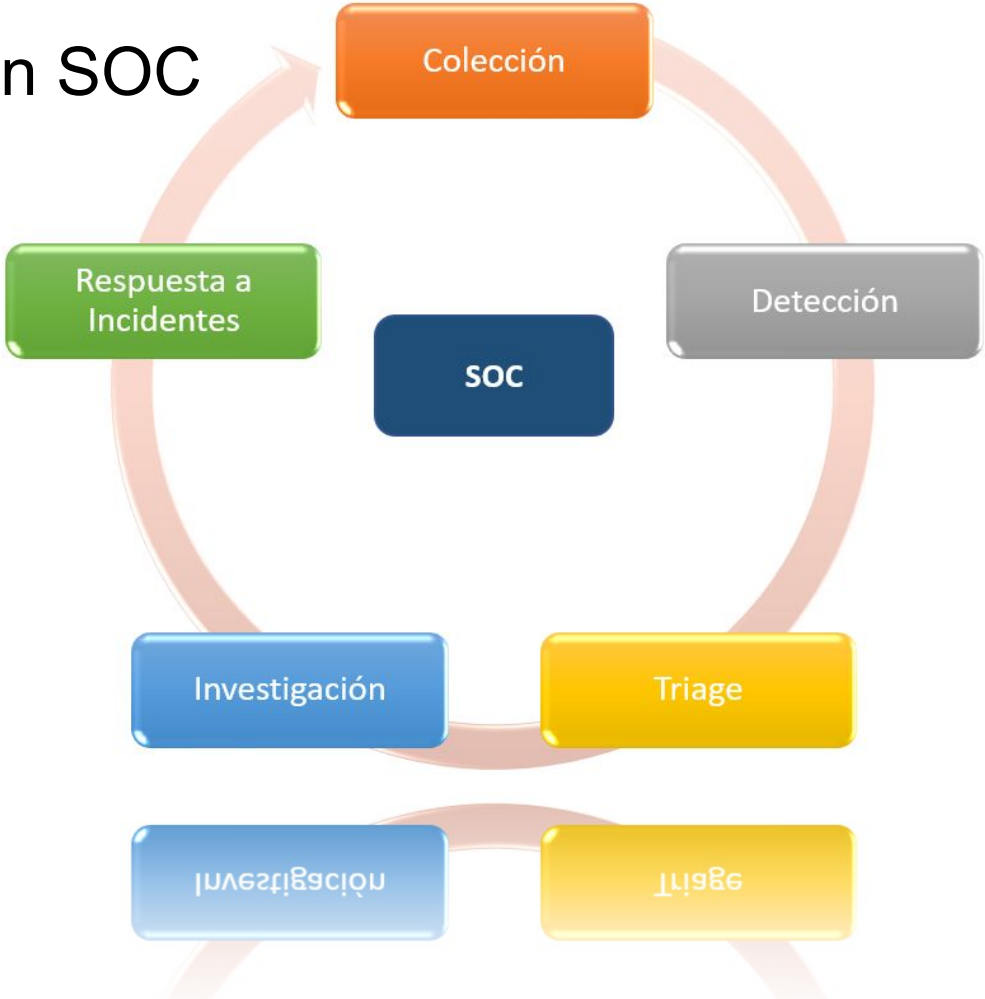
Un centro de operaciones de seguridad es el "eje" central, en el cual los equipos internos de TI y ciberseguridad de una organización participan en la **detección**, el **análisis** y la respuesta de amenazas. Un SOC inteligente permite a los equipos de seguridad:

- Construir una arquitectura SIEM adaptativa
- Aprovechar la analítica de seguridad avanzada
- Detectar amenazas en tiempo real
- Explorar la inteligencia de amenazas integrada
- Automatizar las respuestas a incidentes
- Investigar y visualizar amenazas y aportar soluciones

Funciones CORE de un SOC

Un SOC tiene una serie de funciones divididas a su vez en etapas; donde cada etapa depende del éxito de la etapa anterior.

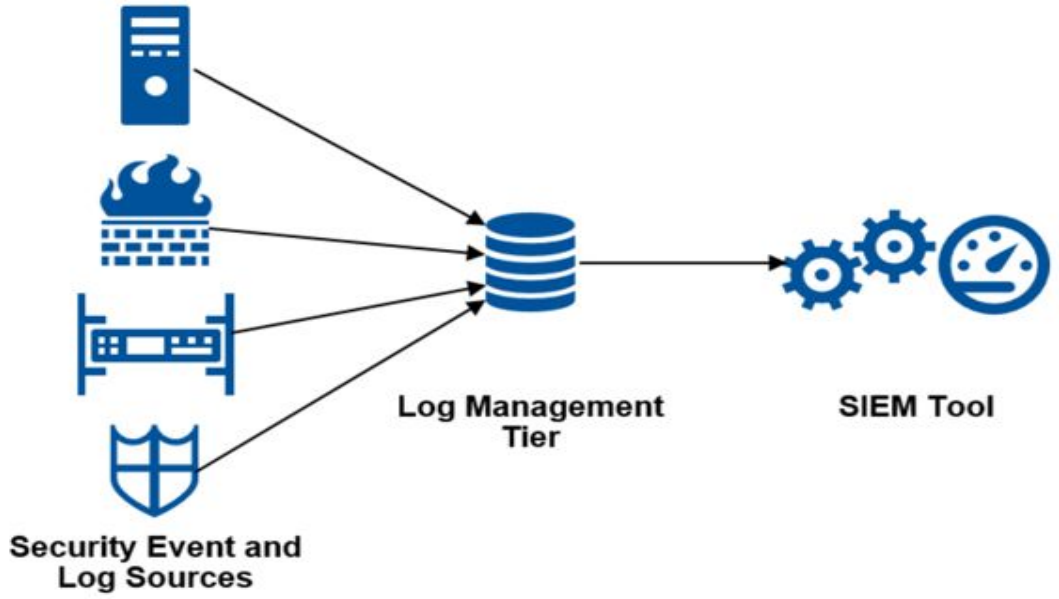
A la derecha observamos las 5 funciones principales de un SOC



¿Qué es un SIEM?

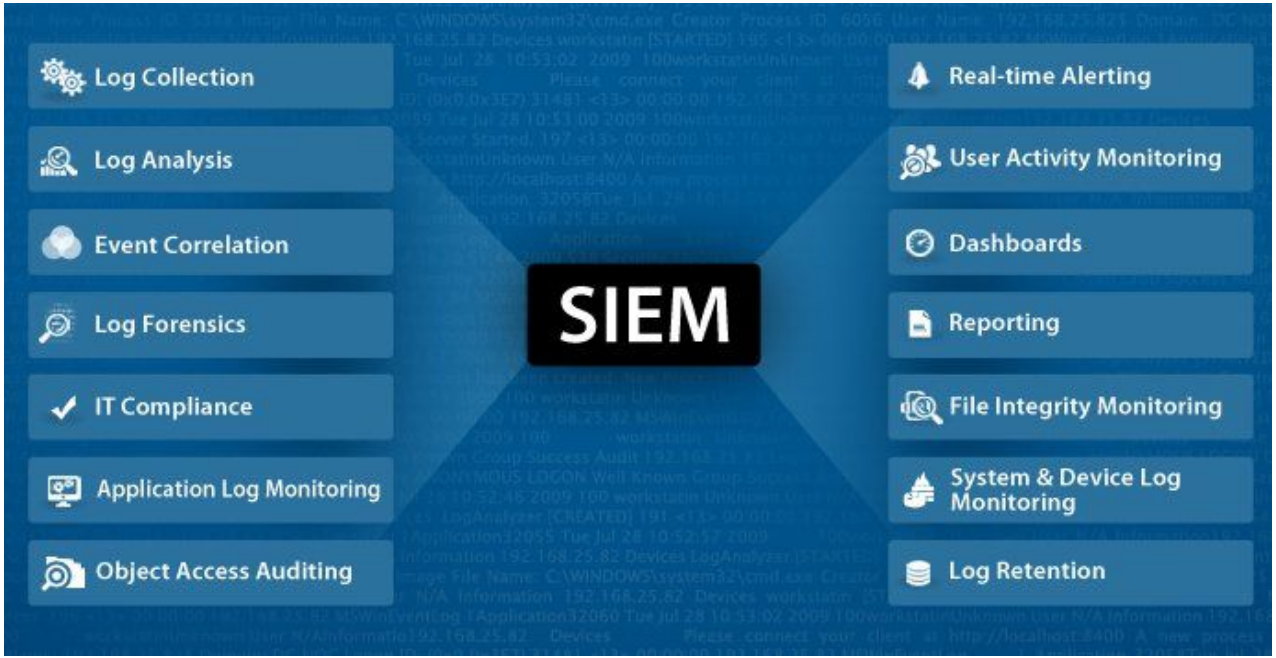
- ★ SIEM - ***S***ecurity ***I***nformation ***E***vent ***M***anagement (Gestión de eventos de información de seguridad)
- ★ Registro y agregación de eventos de diversas fuentes:
  - ○ Network (router,switch,firewall,etc)
  - ○ System (Server,workstation,etc)
  - ○ Application (Web, DB)
- ★ Motor de correlación de eventos
  - ○ Generación de alarmas ante múltiples eventos relacionados

¿Cómo funciona un SIEM?

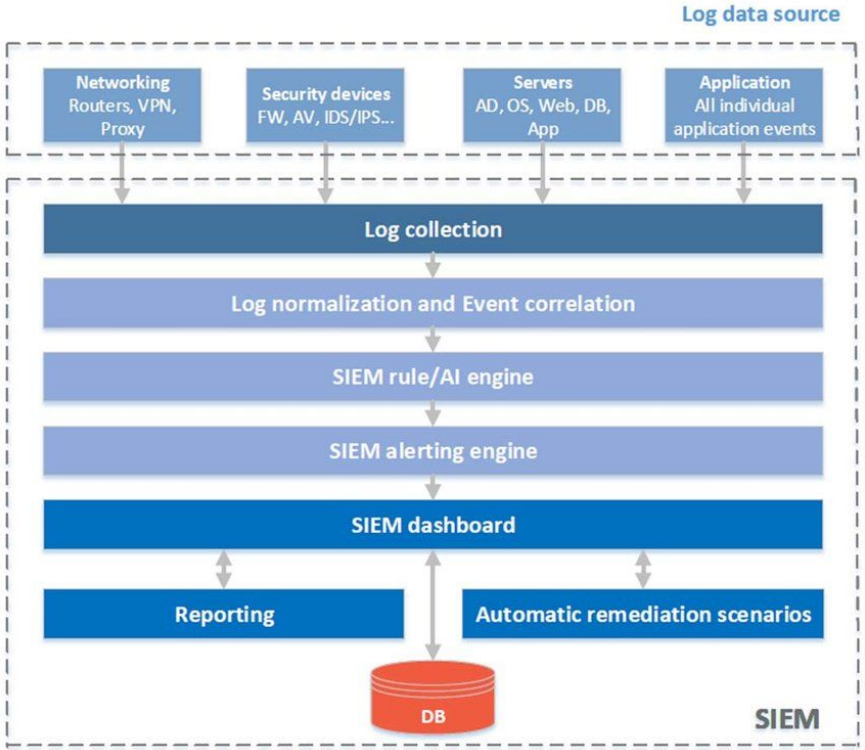


Source: Gartner (October 2016)

Ventajas de un SIEM



Arquitectura de un SIEM



Aspectos importantes

- Fuentes de logs
  - Definir las fuentes
  - Habilitar y configurar los logs en las fuentes
- Recolección de logs
  - Agentes de logs (Opensource, propietarios, agentless)
  - Protocolos (Syslog, SNMP, HTTPS/API, WMI, SMB/CIFS, FTP)
  - En línea o batch
- Generación de valor
  - Definición de casos de uso
  - Eliminación de ruido (filtrado de eventos)

Aspectos importantes (continuación)

- Transporte de logs
  - Cifrado en tránsito
  - Compresión de archivos
  - Caché
  - Banda ancha
- Enriquecimiento
  - Automatización
  - Auditorías
  - Categorización y etiquetado

SIEMs líderes en el mercado

Figure 1: Magic Quadrant for Security Information and Event Management

Source: Gartner (June 2021)

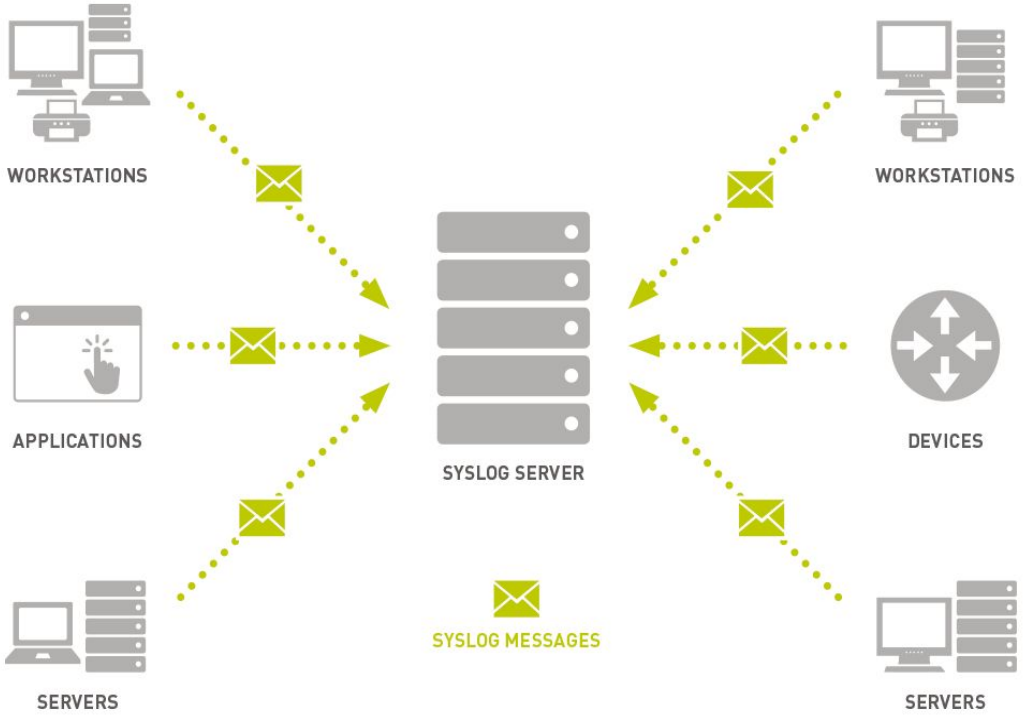
SIEMs Opensource

Introducción a Syslog

Syslog

Syslog (***Sys***tem ***Log***ging Protocol) es un protocolo estándar utilizado para enviar logs del sistema o mensajes de eventos a un servidor específico (Syslog Server).

Su función principal es recolectar logs de diversos dispositivos y máquinas hacia un lugar centralizado para su revisión y monitoreo.



Introducción a Wazuh

¿Qué es Wazuh?

Wazuh es una solución de seguridad Open source del tipo all-in-one, que integra las capacidades de un SIEM y XDR.

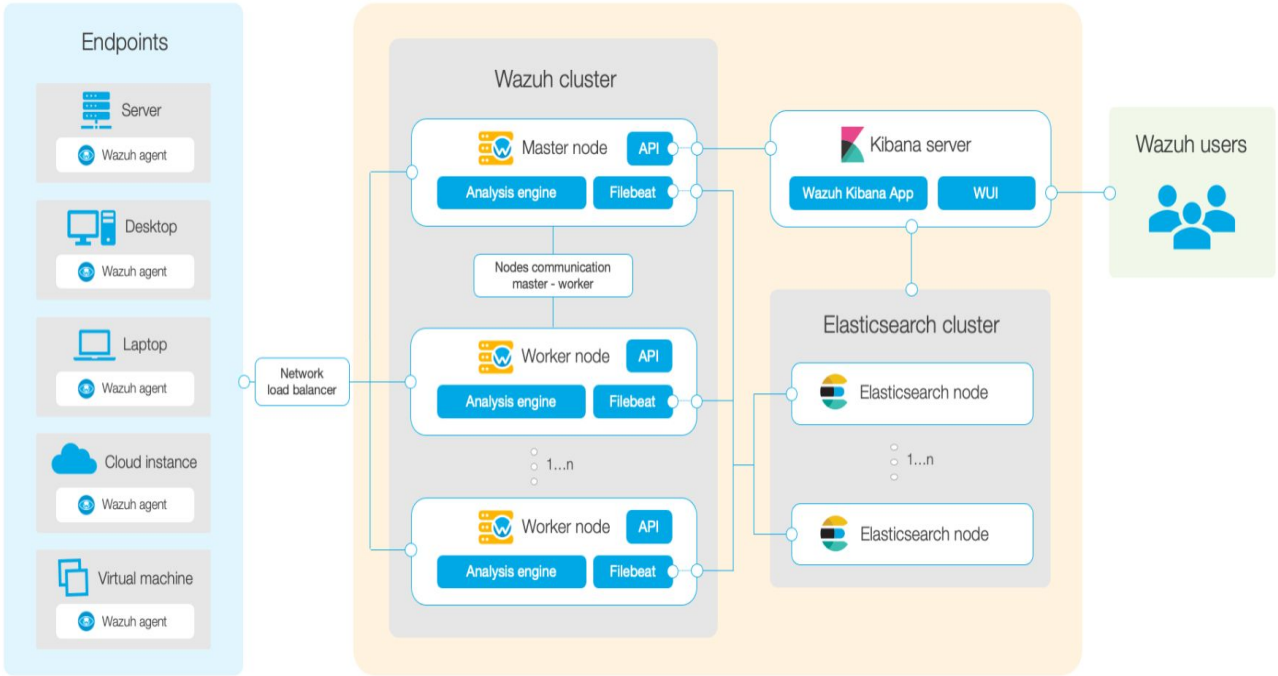
Puede proteger cargas de trabajo en premisas, entornos de nube, entornos contenerizados y entornos virtualizados.

wazuh.

Características de Wazuh

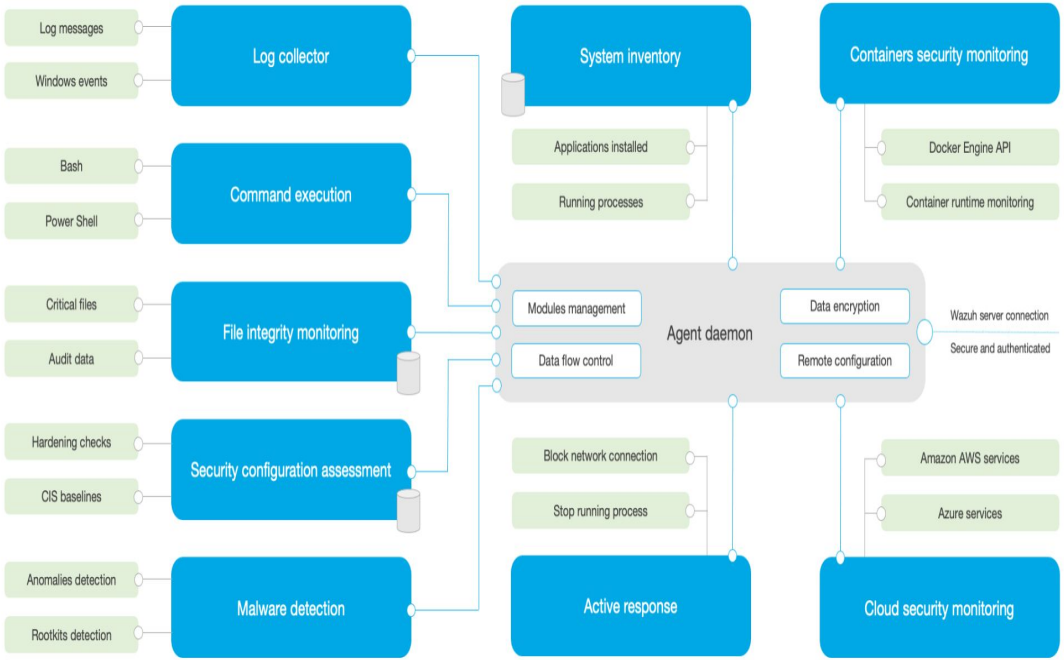
- ★ Análisis y recolección de logs
- ★ Monitoreo de integridad de archivos y configuraciones de red
- ★ Detección de Malware e intrusos
- ★ Inventario de procesos y aplicaciones
- ★ Gestión centralizada de agentes
- ★ Evaluación de configuraciones
- ★ Detección de vulnerabilidades
- ★ Cumplimiento regulatorio
- ★ Fácil integración con otras herramientas (Elastic Stack, Splunk, etc).

Arquitectura de Wazuh



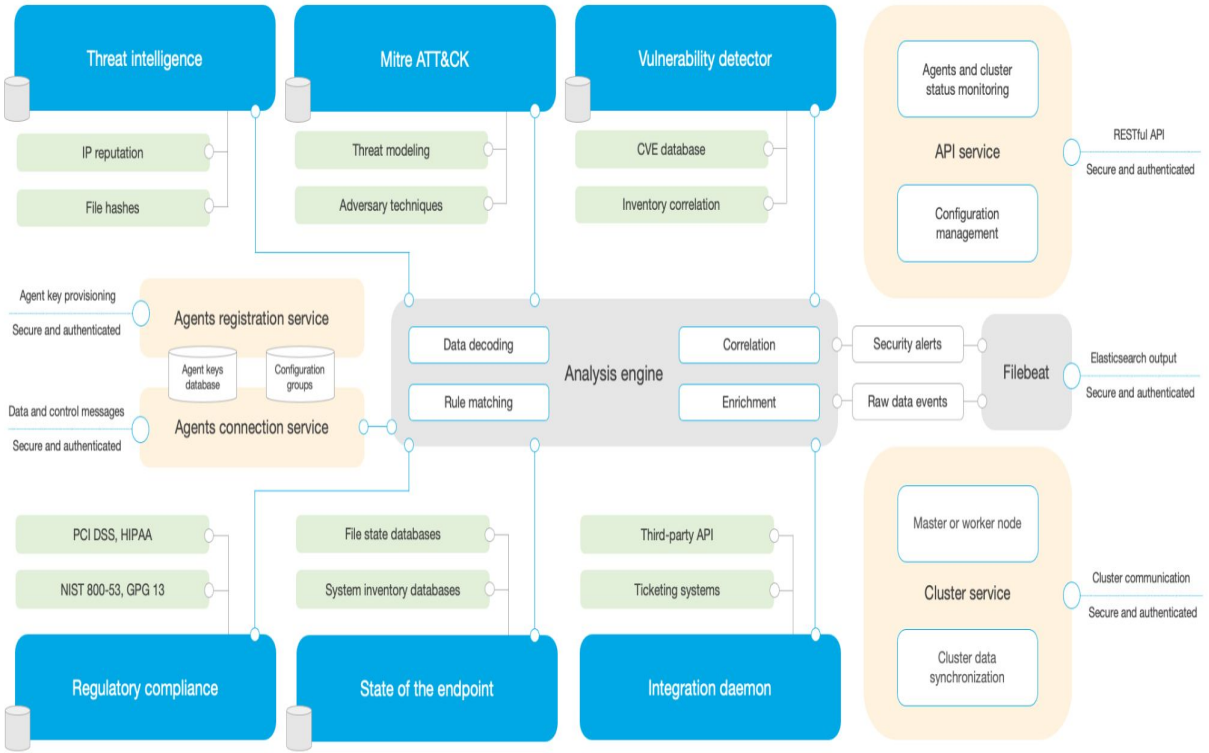
Componentes de Wazuh - Agente

- Se instala en los endpoints para brindar capacidades de detección, prevención y respuesta.
- Arquitectura modular donde cada componente se encarga de sus propias tareas.
- Arquitectura adaptable que permite habilitar o deshabilitar los módulos del agente según cada caso de uso particular.



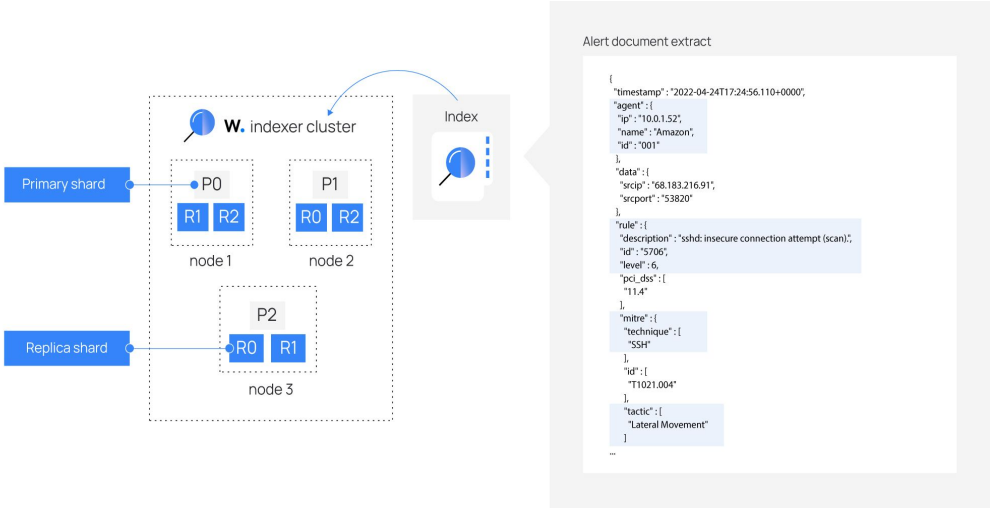
Componentes de Wazuh - Servidor

- Analiza la data recibida por los agentes y la procesa mediante reglas, decodificadores e inteligencia de amenazas.
- Gestiona los agentes de forma remota (configuraciones y actualizaciones) y genera alertas ante amenazas o anomalías.
- Usualmente se ejecuta en una máquina stand-alone física, virtual, contenedor de docker o instancia cloud.



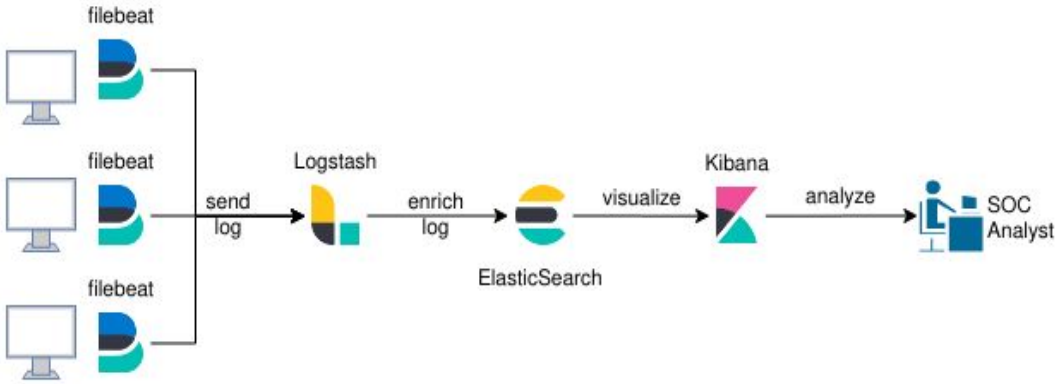
Componentes de Wazuh - Indexador

- Indexa y almacena las alertas generadas por el servidor de Wazuh y provee capacidades de búsqueda y analítica.
- Se puede configurar como un único nodo o clúster multi nodo para proporcionar escalabilidad y alta disponibilidad.
- Almacena los datos como documentos JSON.
- Wazuh utiliza cuatro índices diferentes para almacenar diferentes tipos de eventos:
    - Wazuh-alerts
    - Wazuh-archives
    - Wazuh-monitoring
    - Wazuh-statistics.



Componentes de Wazuh - Dashboard

- Es una interface web para analizar y visualizar eventos de seguridad y alertas. También se utiliza para la gestión y monitoreo de la plataforma de Wazuh.
- Wazuh se integra con herramientas del Elastic Stack como Filebeat, Elasticsearch y Kibana.
-



Recursos de valor

Guía del taller:

https://github.com/Sheynnie05/WALC2022

SIEM:

https://wazuh.com/

Muestras de logs:

https://www.secrepo.com/maccdc2012/ftp.log.gz

https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES/tree/master/AutomatedTestingTools

http://www.almhuette-raith.at/apache-log/

¡Gracias!


https://www.linkedin.com/in/sheyla-leacock/


shey.lck@gmail.com


@sheynnie_mcr


https://github.com/Sheynnie05/


https://www.wosecpanama.com/

https://comunidaddojo.org/

https://backtrackacademy.com/@Sheyla_Leacock/cursos