DGTIC

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Identificar patrones anómalos en la infraestructura de una organización

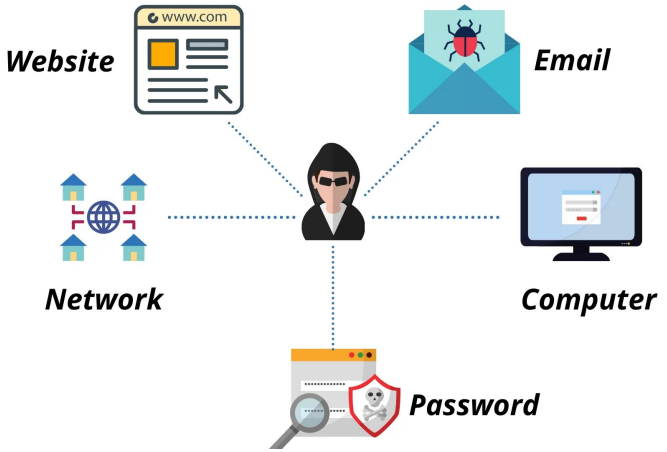
Ponente:
Fernández Martínez Abisinia Ivey
Luna Castañeda Abraham Iván
López Matías Alexis Brayan
Resendiz Cruz Luis Fernando

Descripción

- Capaz de analizar bitácoras y eventos de múltiples servicios, dispositivos y sistemas operativos.
- Generar reportes manuales y automáticos.
- Visualizar informes, tablas, gráficos y métricas.

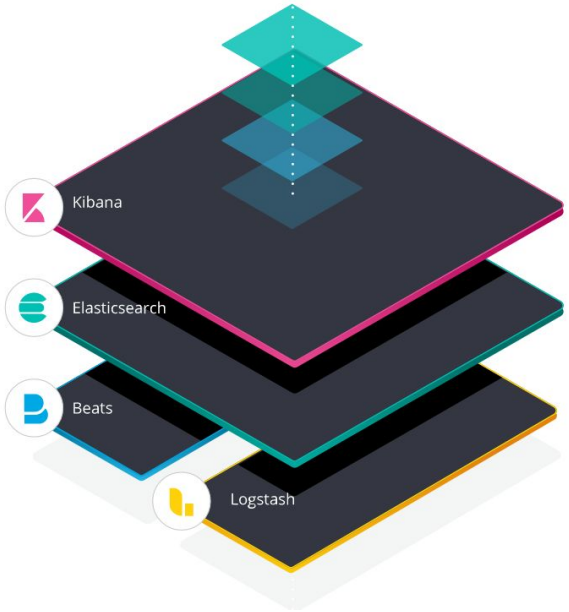
Descripción

- Identificar patrones anómalos:
  - Ataques de Open Relay
  - Escaneo de directorios
  - Ataques de fuerza bruta
  - Inyección SQL
  - Enumeración de usuarios



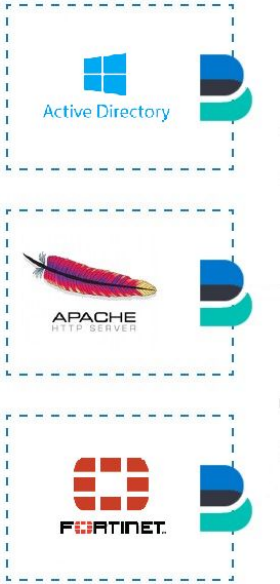
Descripción

Infraestructura compuesta por BELK Stack (Beats, Elasticsearch, Logstash, Kibana).



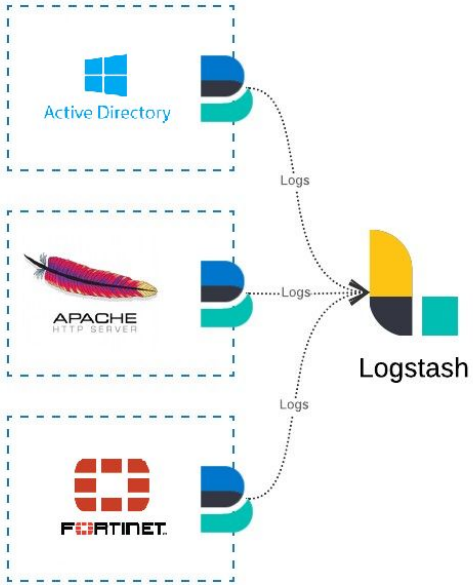
Descripción

Beats: Agentes de datos de código abierto que se instalan sobre los servidores a monitorear.



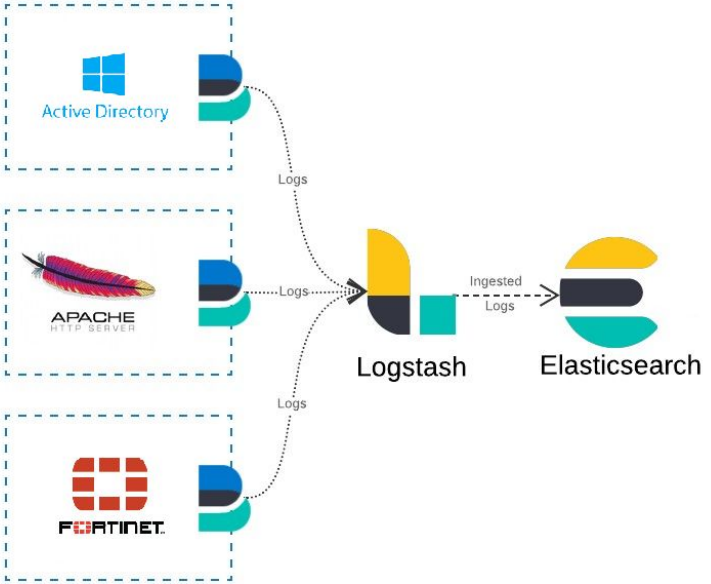
Descripción

Logstash: Motor de recopilación de datos de código abierto que permite la unificación, normalización y enriquecimiento de estos.



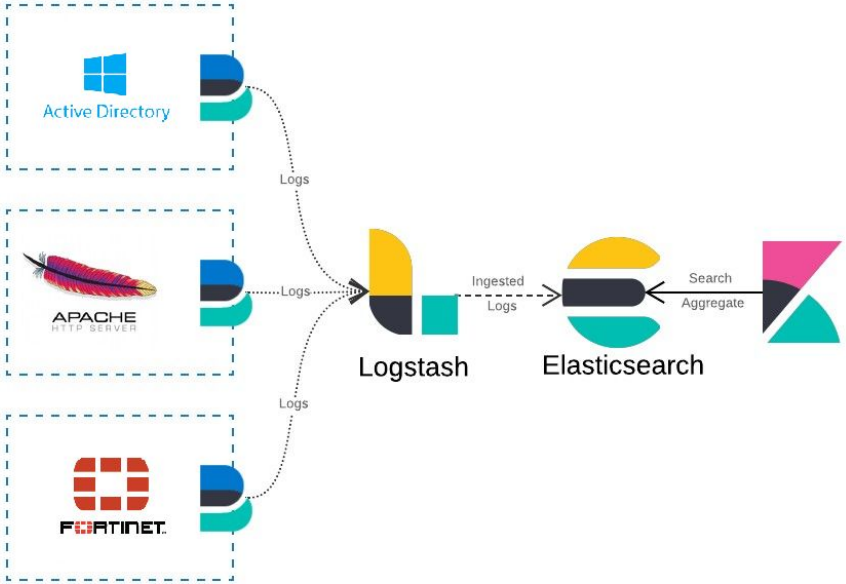
Descripción

Elasticsearch: Motor de análisis, búsqueda y almacenamiento distribuido en tiempo real.



Descripción

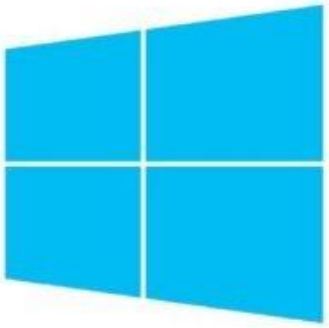
Kibana: Plataforma de análisis, visualización y administración de código abierto.

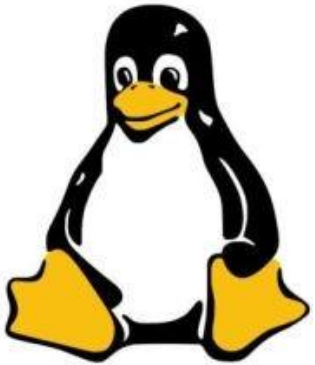


Objetivos

Desarrollo de una infraestructura capaz de:

- Detectar eventos anómalos sobre múltiples servicios.
- Alertar sobre situaciones de riesgo en cada uno de los servicios monitoreados.
- Analizar bitácoras y eventos de servicios sobre plataformas Windows y Linux.



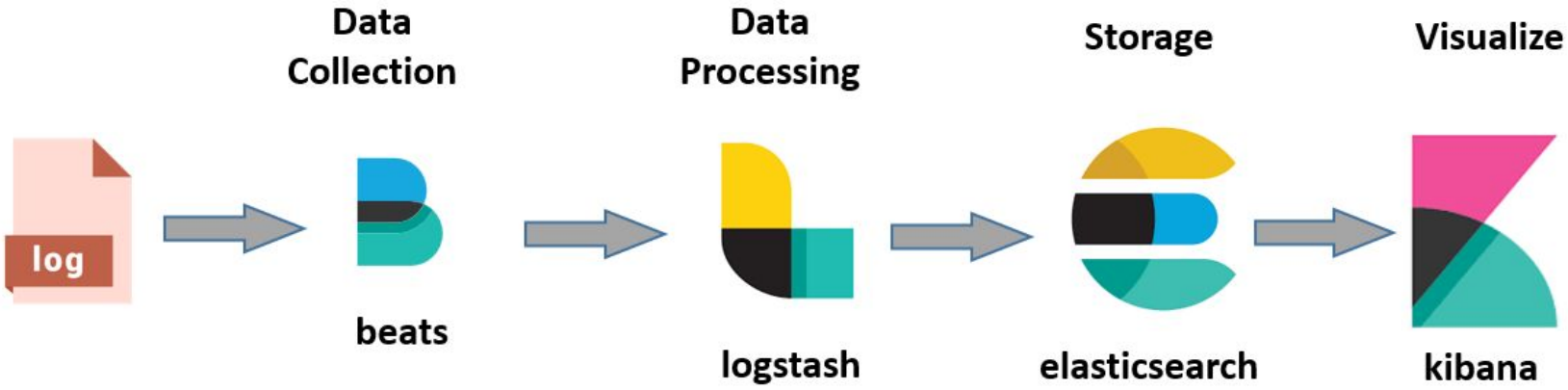


Objetivos

- Generar informes de forma manual y automatizada.
- Permitir la visualización gráfica y numérica de los datos analizados.
- Proveer una forma centralizada de monitoreo y detección de eventos.

Herramientas utilizadas

- Logstash
- Kibana
- Beats
- Elasticsearch



Herramientas utilizadas

- Git
- Bash
- NMap

Herramientas utilizadas

- VMware Workstation
- GNS3
- Discord

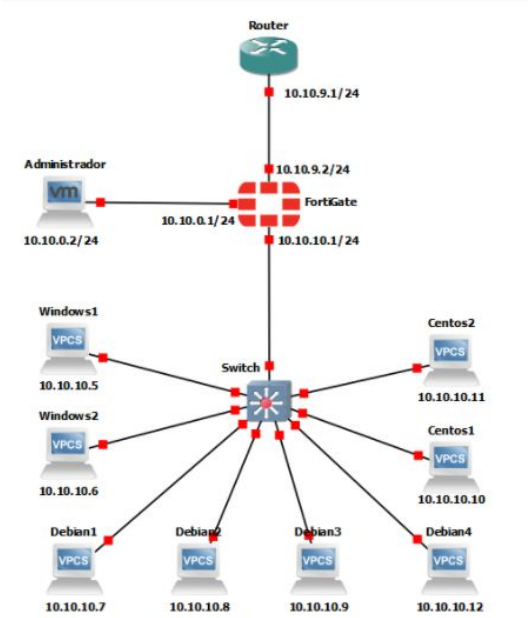
Metodología de desarrollo

5 entregables a lo largo de 8 semanas.

Metodología de desarrollo

Entregable 1

Instalación de servicios en ambientes Windows, GNU/Linux y dispositivos de red. [Semana 1] (Proveer bitácoras y eventos)



Metodología de desarrollo

Entregable 2

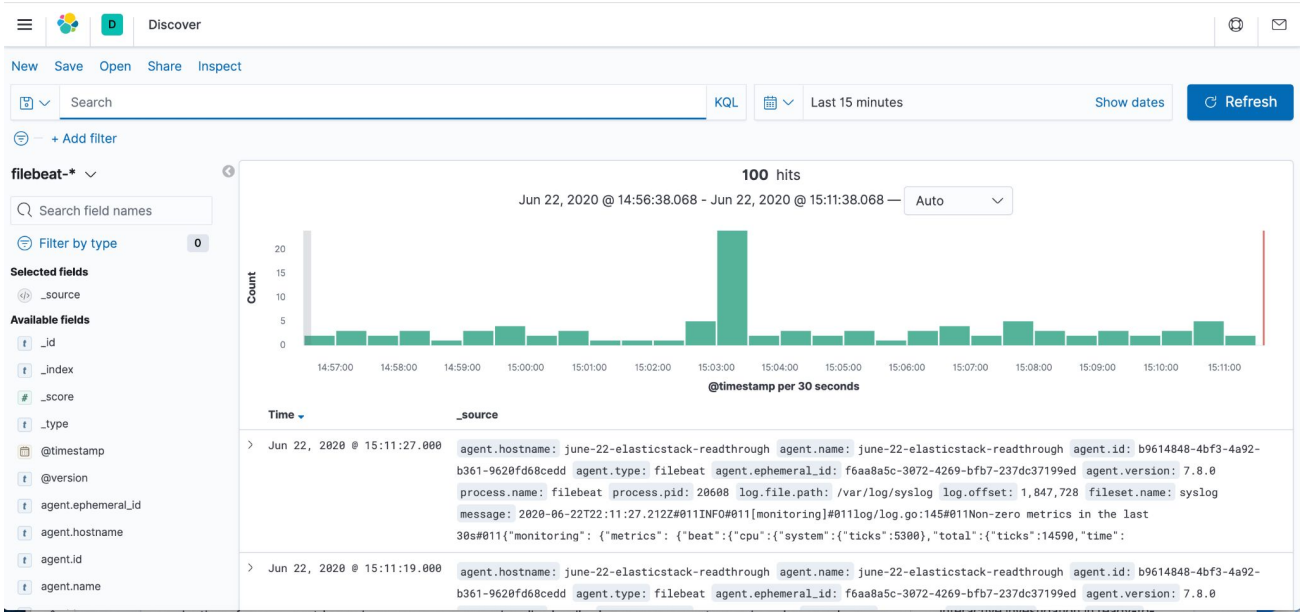
Generación de scripts de hardening para los servicios del entregable 1. [Semanas 2 y 3] (Aseguramiento de los servicios)

```
echo "
------------------------------------------------------------
                        CUENTAS POR DEFECTO
------------------------------------------------------------
"
./HardeningUserAccounts.sh

echo "
------------------------------------------------------------
                        POLÍTICA DE CONTRASEÑAS
------------------------------------------------------------
"
./password.sh

echo "
------------------------------------------------------------
                        USUARIOS Y PRIVILEGIOS
------------------------------------------------------------
"
./usuarios.sh
```

Metodología de desarrollo

Entregable 3

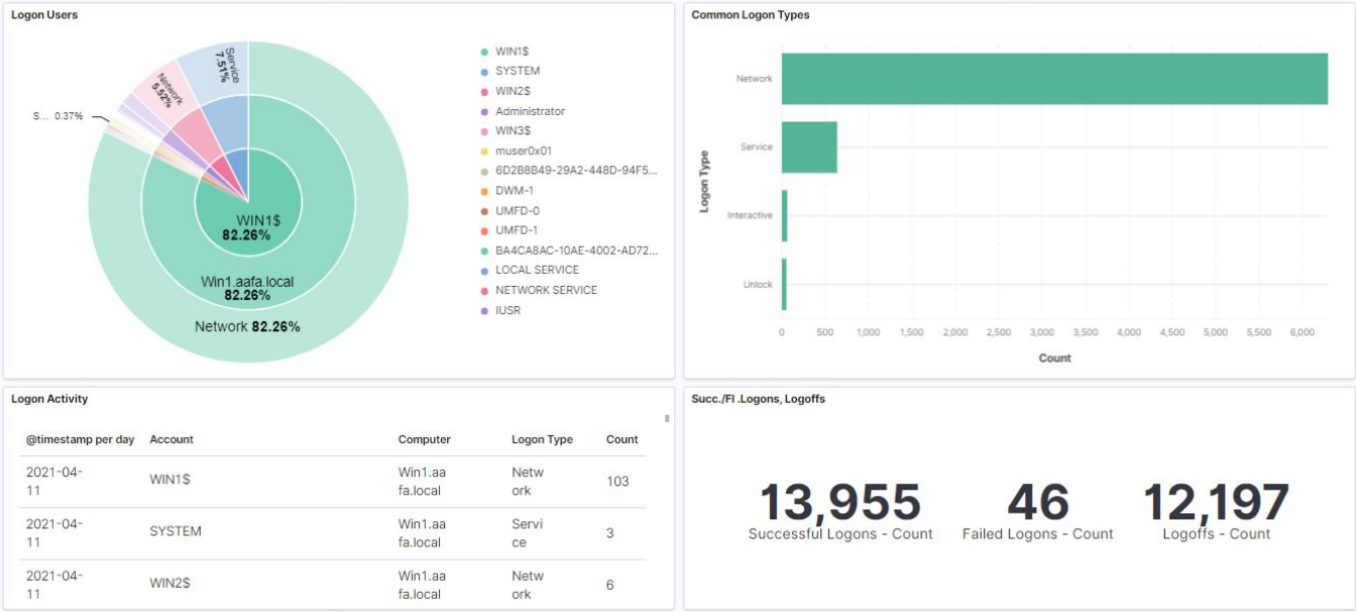
Implementación de la infraestructura BELK. [Semana 3] (Recepción de bitácoras y eventos)



Metodología de desarrollo

Entregable 4

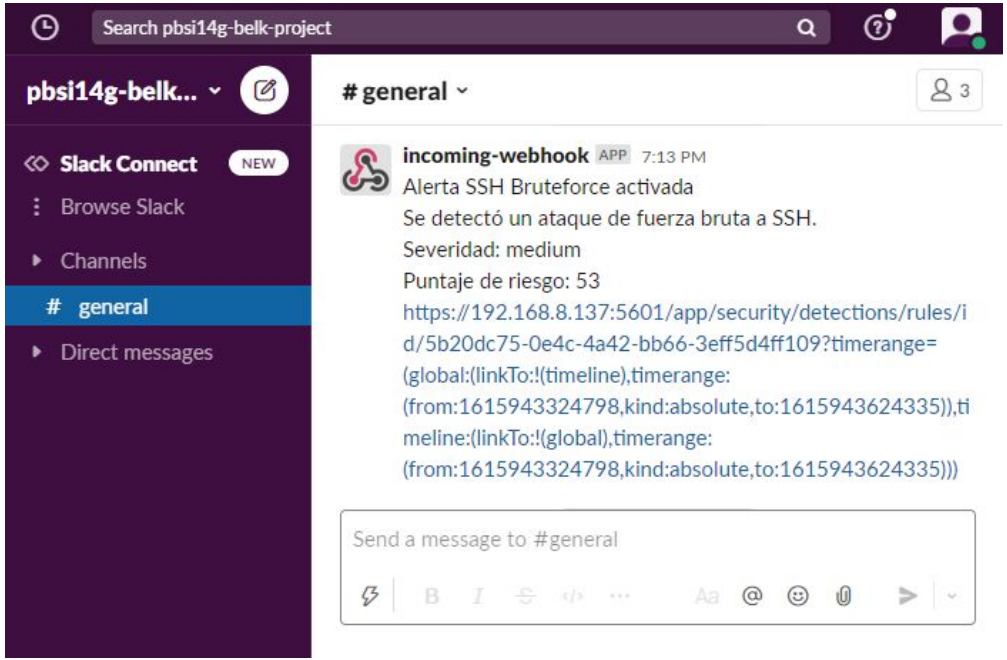
Visualización de gráficas, emisión de alertas y generación de reportes. [Semanas 4 y 5]



Metodología de desarrollo

Entregable 4

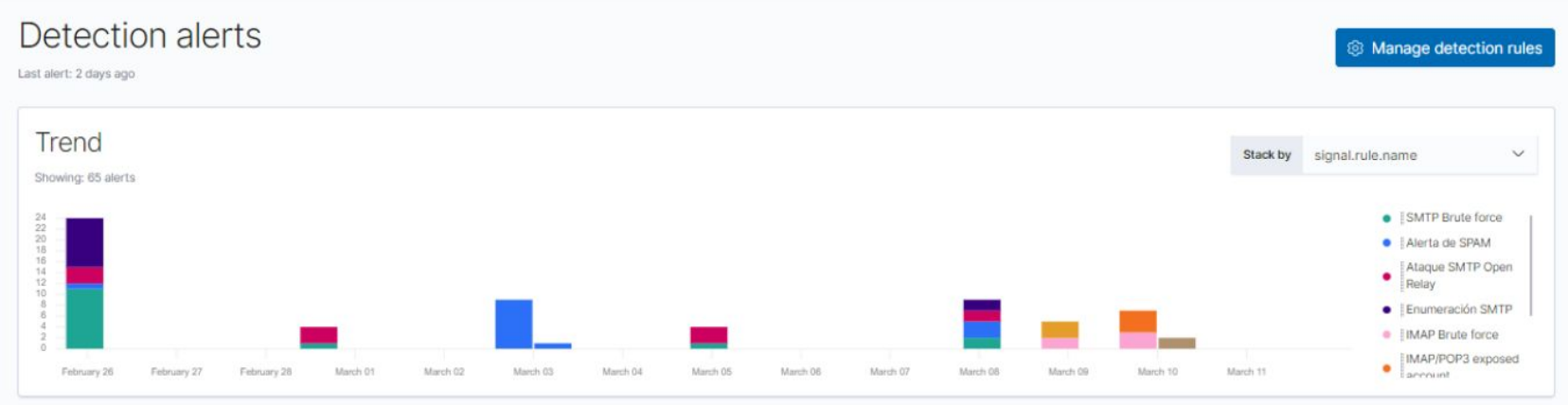
Visualización de gráficas, emisión de alertas y generación de reportes. [Semanas 4 y 5]



Metodología de desarrollo

Entregable 5

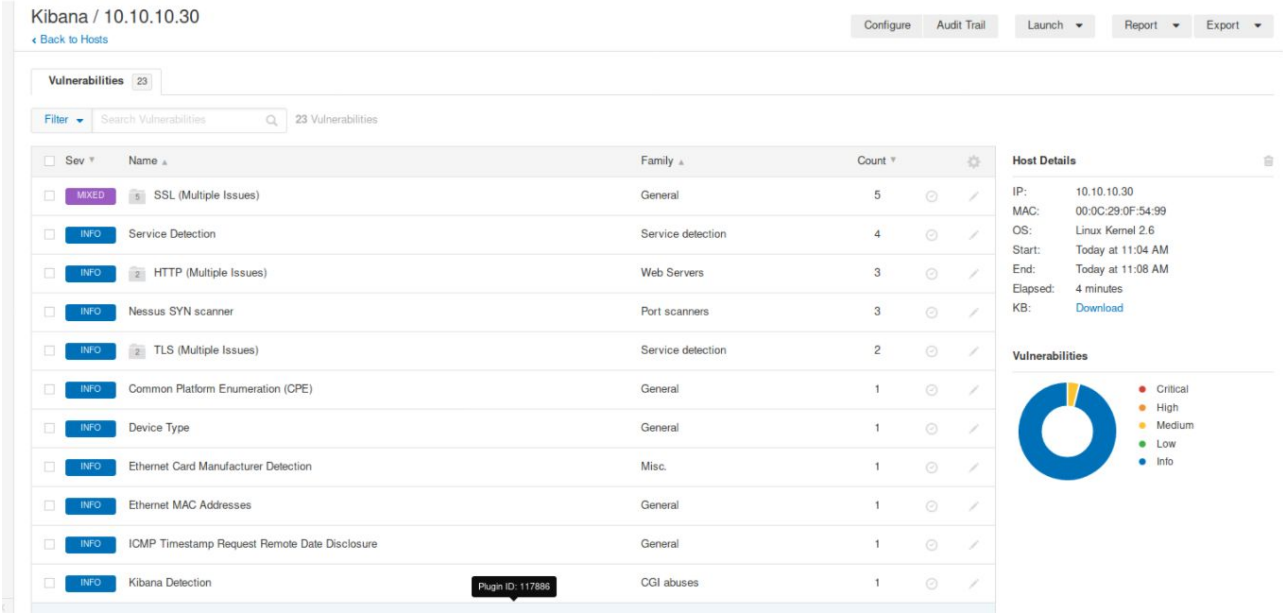
Correlación de eventos. [Semanas 5 y 6]



Metodología de desarrollo

Semanas 7 y 8

Afinamiento, aseguramiento, pruebas de penetración e implementación en producción.



Demostración

Obstáculos

- Aprendizaje de una infraestructura totalmente nueva (BELK Stack).
- Procesamiento de bitácoras mediante Regex.
- Registros duplicados.

elastic stack

```
AMAVIS \(%{DATA:amavis_id}\) %{WORD:amavis_action}
```

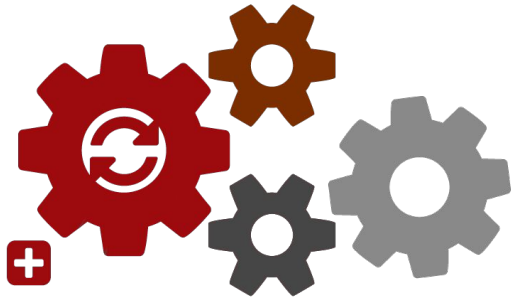
Obstáculos

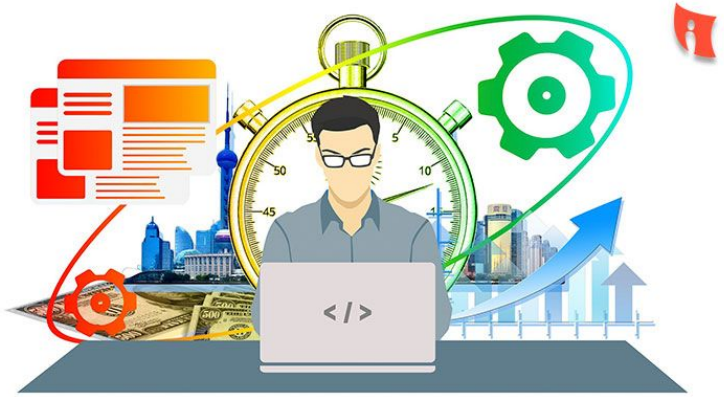
- Depuración de errores en Logstash.
- Configuración de HTTPS.
- Versiones en producción.

$ apt-get

Conclusiones

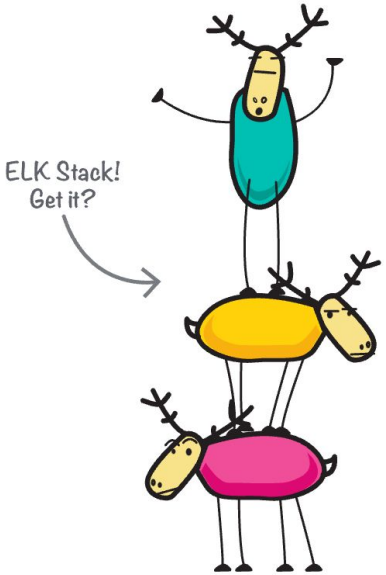
- Sistema modular permite escalabilidad y mantenimiento asequible.
- Automatización mejora el desempeño de una organización y posibilita la notificación oportuna.
- Administración centralizada facilita el monitoreo y reduce tiempos de respuesta.





Conclusiones

- Detección de anomalías es más sencilla mediante gráficas.
- Elastic Stack es una gran opción para el desarrollo de un SIEM.



E Elasticsearch

L Logstash

K Kibana

¿Preguntas?