



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

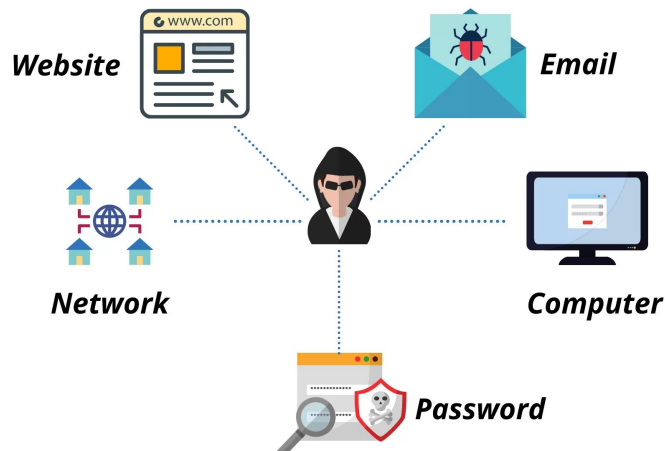
Resendiz Cruz Luis Fernando



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



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

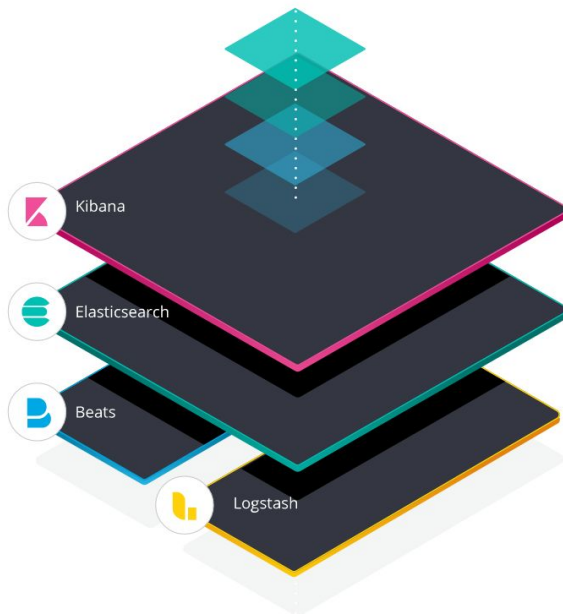




Descripción



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





Descripción

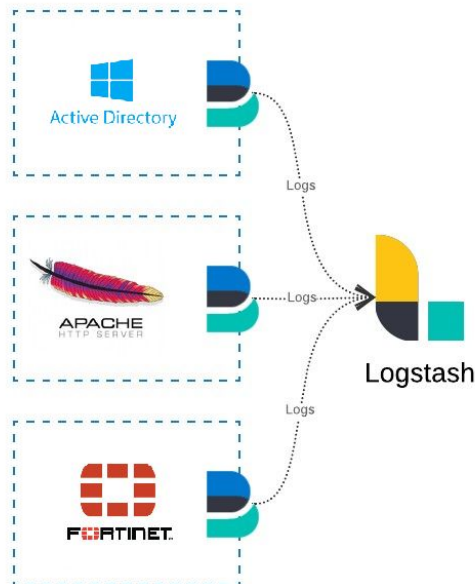
Beats: Agentes de datos de código abierto que se instalan sobre los servidores a monitorear.





Descripción

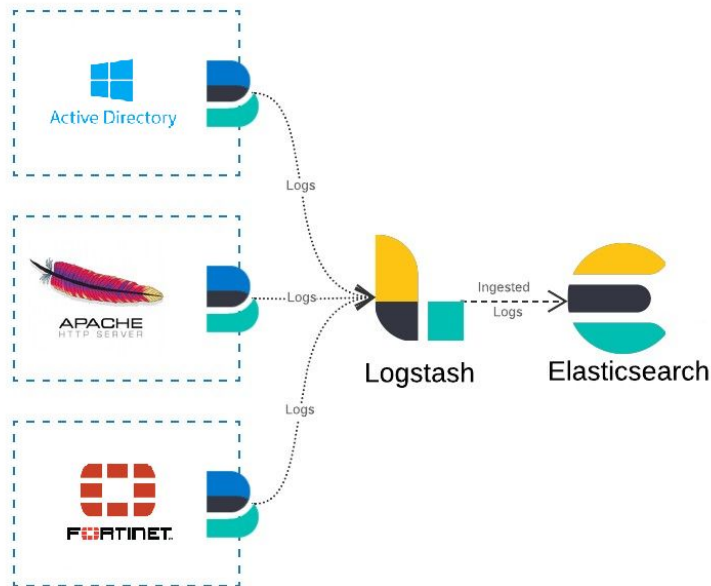
Logstash: Motor de recopilación de datos de código abierto que permite la unificación, normalización y enriquecimiento de estos.





Descripción

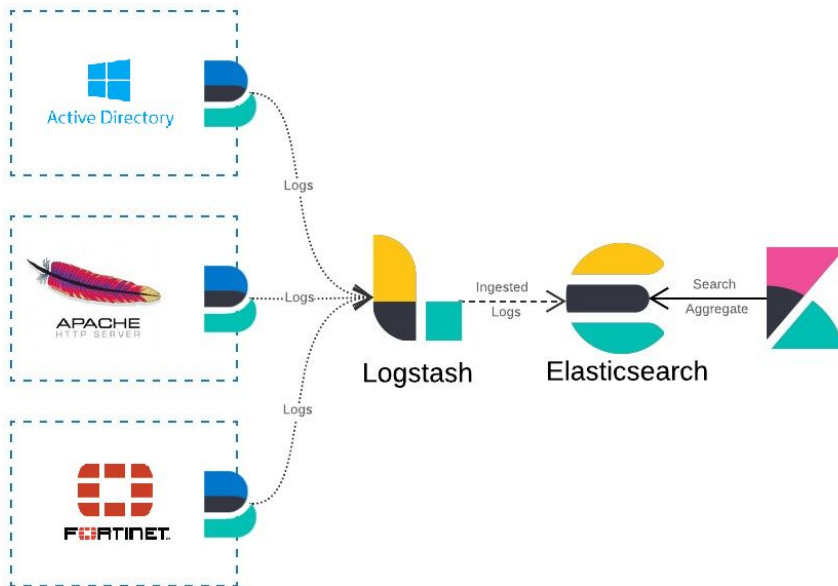
Elasticsearch: Motor de análisis, búsqueda y almacenamiento distribuido en tiempo real.





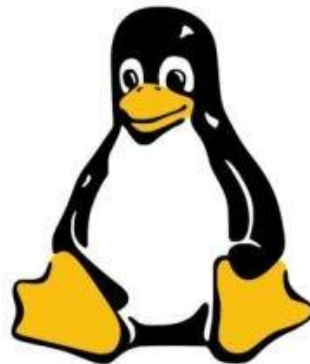
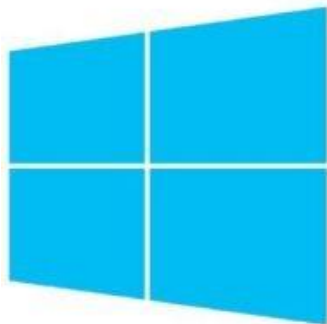
Descripción

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



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.

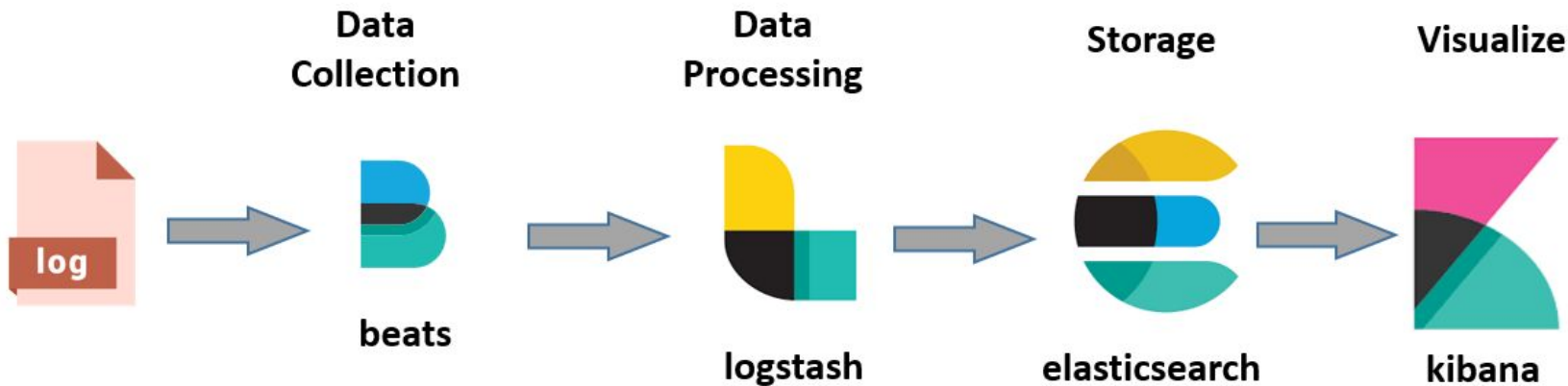


- Generar informes de forma manual y automatizada.
- Permitir la visualización gráfica y numérica de los datos analizados.
- Proveer una forma centralizada de monitoreo y detección de eventos.



Herramientas utilizadas

- Logstash
- Beats
- Elasticsearch
- Kibana

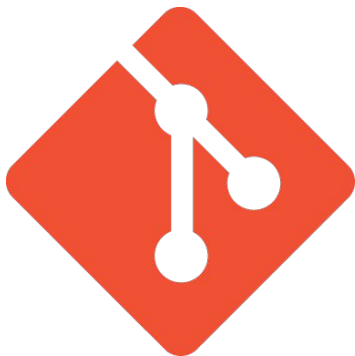




Herramientas utilizadas



- Git
- Bash
- NMap





Herramientas utilizadas



- VMware Workstation
- GNS3
- Discord





Metodología de desarrollo



5 entregables a lo largo de 8 semanas.

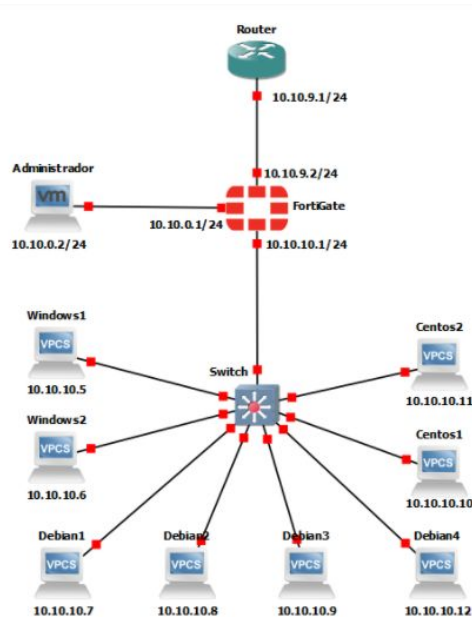




Metodología de desarrollo

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



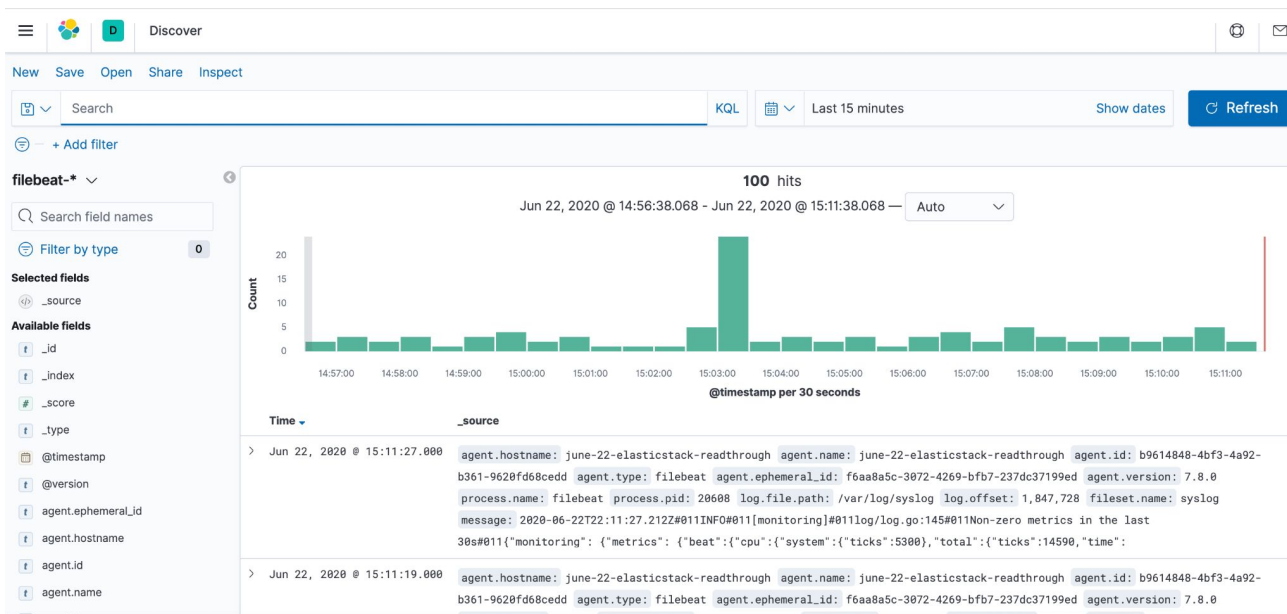
Generación de scripts de hardening para los servicios del entregable 1. [Semanas 2 y 3] (Aseguramiento de los servicios)

```
1 echo "  
2 _____  
3 Cuentas por defecto  
4 _____  
5 "  
6 ./HardeningUserAccounts.sh  
7  
8 echo "  
9 _____  
10 POLÍTICA DE CONTRASEÑAS  
11 _____  
12 "  
13 ./password.sh  
14  
15 echo "  
16 _____  
17 Usuarios y privilegios  
18 _____  
19 "  
20 ./usuarios.sh
```


Metodología de desarrollo

Entregable 3

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

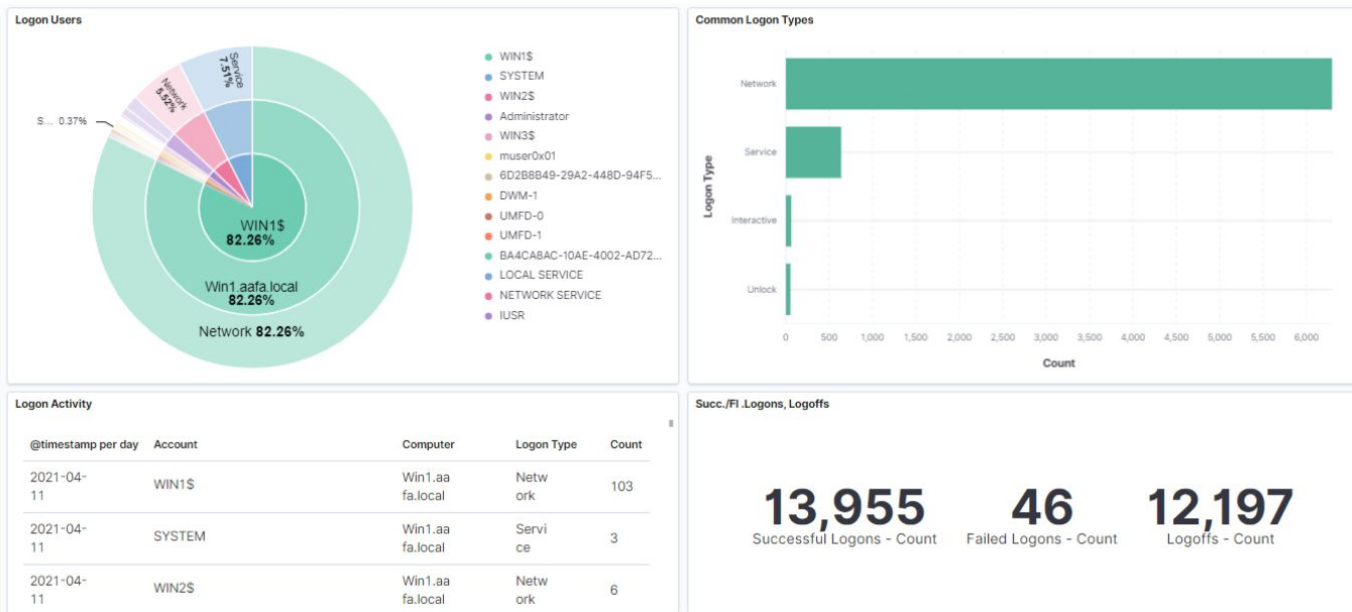




Metodología de desarrollo

Entregable 4

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



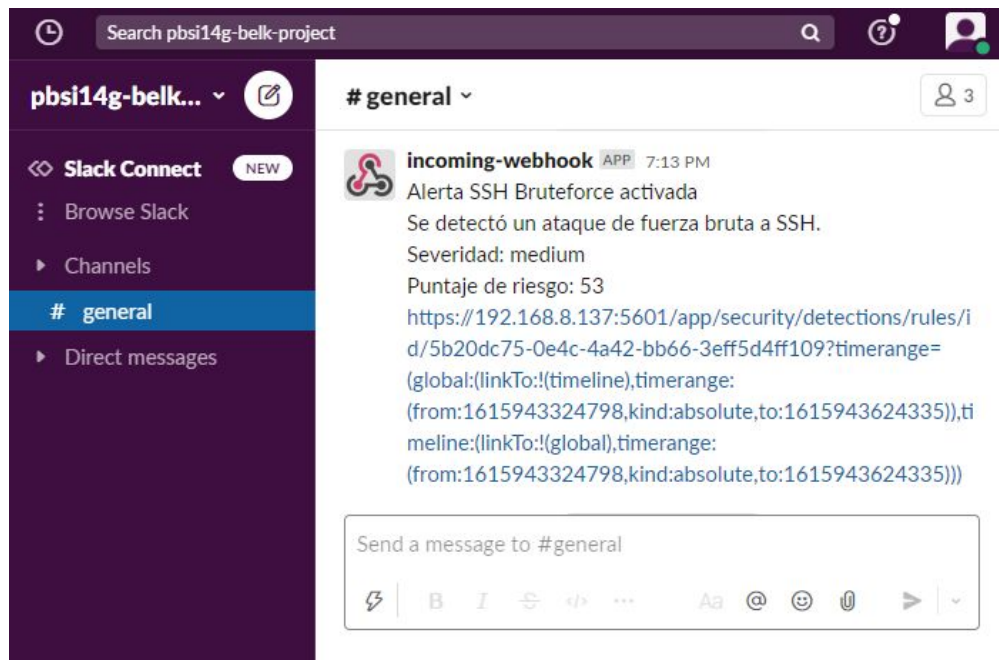


Metodología de desarrollo

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]

Detection alerts

Last alert: 2 days ago

[Manage detection rules](#)

Trend

Showing: 65 alerts

Stack by signal.rule.name





Metodología de desarrollo

Semanas 7 y 8

coloquio de proyectos
de Becarios en Seguridad Informática
7

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

Kibana / 10.10.10.30

[Back to Hosts](#) [Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Vulnerabilities 23

Filter Search Vulnerabilities 23 Vulnerabilities

Sev	Name	Family	Count	
MIXED	SSL (Multiple Issues)	General	5	
INFO	Service Detection	Service detection	4	
INFO	HTTP (Multiple Issues)	Web Servers	3	
INFO	Nessus SYN scanner	Port scanners	3	
INFO	TLS (Multiple Issues)	Service detection	2	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Device Type	General	1	
INFO	Ethernet Card Manufacturer Detection	Misc.	1	
INFO	Ethernet MAC Addresses	General	1	
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1	
INFO	Kibana Detection	CGI abuses	1	

Host Details

IP: 10.10.10.30
MAC: 00:0C:29:0F:54:99
OS: Linux Kernel 2.6
Start: Today at 11:04 AM
End: Today at 11:08 AM
Elapsed: 4 minutes
KB: [Download](#)

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Plugin ID: 117896

Demostración





Obstáculos



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



elastic stack

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



Obstáculos

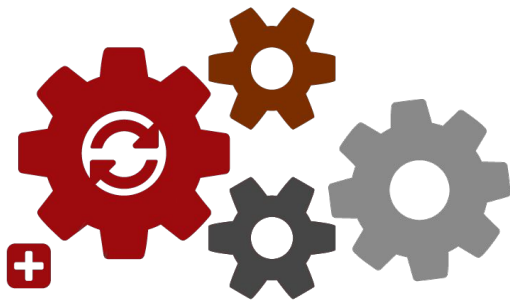


- Depuración de errores en Logstash.
- Configuración de HTTPS.
- Versiones en producción.

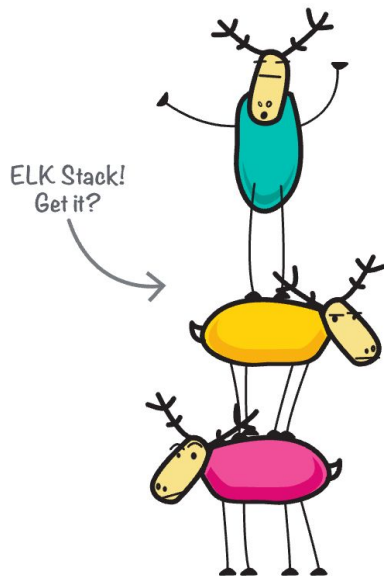
\$ apt-get



- 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.



- 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?

