

SOC - ELK. Documentación, implementación y puesta en marcha de un servicio SOC

UOC

Felipe Bueno Carranza
Seguridad en aplicaciones web

Nombre Tutor/a de TF
Erik de Luis Gargallo

Profesor/a responsable de la asignatura
Erik de Luis Gargallo

Fecha Entrega
10/01/2024



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	SOC - ELK. Documentación, implementación y puesta en marcha de un servicio SOC
Nombre del autor:	Felipe Bueno Carranza
Nombre del consultor/a:	
Nombre del PRA:	Erik de Luis Gargallo
Fecha de entrega (mm/aaaa):	01/2024
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	Seguridad en Aplicaciones Web
Idioma del trabajo:	Castellano
Palabras clave	Elasticsearch, Logstash, Kibana

Resumen del Trabajo

En un panorama donde las amenazas cibernéticas son cada vez más complejas, la implementación de un Centro de Operaciones de Seguridad (SOC) efectivo se vuelve esencial para las organizaciones. Este trabajo se centra en la creación y operación de un SOC respaldado por la plataforma ELK (*Elasticsearch, Logstash, Kibana*), proporcionando una guía detallada para fortalecer la postura de seguridad cibernética. A través de una metodología que combina investigación, revisión de literatura y aplicación práctica, se documenta la importancia del SOC, se detalla la infraestructura y operaciones, y se implementa la plataforma ELK para el análisis de eventos de seguridad.

El trabajo abarca desde la comprensión del SOC hasta la implementación exitosa de ELK, documentando procesos clave y desarrollando *dashboards* y alertas para el análisis de seguridad. La implementación de un SOC respaldado por ELK mejora la seguridad cibernética, contribuyendo a una gestión más efectiva de eventos de seguridad.

Además, se destaca la importancia de considerar aspectos éticos, sostenibles y diversos en el ámbito de la ciberseguridad. En resumen, este trabajo promueve la seguridad cibernética y ofrece un recurso valioso para organizaciones que buscan fortalecer su postura en un entorno de amenazas cibernéticas en constante evolución.

Abstract

In a world where cyber threats are increasingly sophisticated and ubiquitous, the implementation of an effective Security Operations Center

(SOC) has become an unavoidable priority for organizations. This paper addresses the documentation, implementation, and operationalization of a SOC backed by the ELK platform (Elasticsearch, Logstash, Kibana). The main purpose is to provide a detailed guide enabling organizations to strengthen their cybersecurity posture. This is achieved through understanding the importance of a SOC, comprehensive documentation of SOC infrastructure and operations, effective implementation of the ELK platform for security event analysis, and the establishment of robust processes and procedures for continuous SOC operation.

A methodology combining thorough research, literature review, and practical implementation is employed. The ELK platform is used to collect and analyze security event data, facilitating data-driven decision-making. The paper provides a comprehensive guide from understanding the SOC's importance to the successful implementation of the ELK platform. Key processes and procedures are documented, and dashboards and alerts are developed for security analysis.

The implementation of an ELK-backed SOC strengthens organizations' cybersecurity. The proposed methodology and results contribute to more effective security event management. Additionally, the importance of considering ethical, sustainable, and diverse aspects in the cybersecurity context is emphasized. In summary, this work promotes cybersecurity and offers a valuable resource for organizations seeking to bolster their stance in an ever-evolving cyber threat environment.

Índice

1.	Introducción.....	6
1.1.	Contexto y justificación del Trabajo.....	6
1.2.	Objetivos del Trabajo	7
1.3.	Enfoque y método seguido.....	8
1.4.	Planificación del Trabajo	9
1.5.	Estado del arte	11
2.	Materiales y métodos	12
2.1.	Que es un SOC y cuáles son sus funciones	12
2.2.	Qué es un SIEM y cómo funciona	13
2.3.	Qué es un ELK y cómo se compone	14
2.4.	Ventajas y desafíos de usar un ELK en un SOC.....	15
2.5.	Eventos de seguridad de Windows	17
2.6.	Diseño e implementación del ELK	17
2.7.	Elección e implementación de <i>Beats</i>	18
2.8.	Reglas y <i>Dashboard</i> por defecto	18
2.9.	Creación de regla analítica y <i>dashboard</i> de ejemplo.....	20
2.10.	Requisitos funcionales y no funcionales	21
2.11.	Arquitectura y diseño del sistema montado	22
3.	Validación de resultados	23
3.1	Comprobación del estado de los servicios desplegados.....	23
3.2	Correcta visualización en Kibana	25
3.3	Ingesta y visualización de eventos de Windows	25
3.4	Funcionamiento apropiado de regla analítica.....	26
3.5	Visualización de <i>dashboard</i> de ejemplo	28
4	Conclusiones y trabajos futuros	29
4.1	Conclusiones del trabajo	29
4.2	Consecución de objetivos planteados	29
4.3	Seguimiento de la planificación y metodología a lo largo del producto.....	30
4.4	Posibles mejoras y líneas de trabajo futuro.....	30
5	Bibliografía	32
6	Anexos	35
A.	Guía de instalación de la pila ELK.....	35
B.	Guía de configuración de reglas y <i>dashboards</i>	43

Lista de figuras

Figura 1: Diagrama de Gantt	10
Figura 2: Arquitectura pila ELK [12]	15
Figura 3: Reglas predefinidas de Elastic	19
Figura 4: Dashboards por defecto de Winlogbeat	20
Figura 5: Dashboard de información de logins	20
Figura 6: Diseño del sistema montado	22
Figura 7: Validación despliegue Elasticsearch 1	23
Figura 8: Validación despliegue Elasticsearch 2	23
Figura 9: Validación despliegue Kibana	24
Figura 10: Validación despliegue <i>Logstash</i>	24
Figura 11: Validación despliegue Winlogbeat	25
Figura 12: Panel Discover en Kibana	25
Figura 13: Eventos en el visor de eventos de Windows	26
Figura 14: Eventos en Kibana	26
Figura 15: Enumeración de permisos de usuario (1)	26
Figura 16: Enumeración de permisos de usuario (2)	27
Figura 17: Pestaña Security-Alerts de <i>Kibana</i>	27
Figura 18: Regla de ejemplo disparada	28
Figura 19: <i>Dashboard</i> de ejemplo	28
Figura 20: Descarga de Java	35
Figura 21: Editar variables de entorno 1	35
Figura 22: Editar variables de entorno 2	36
Figura 23: Demostración ruta binario <i>javac</i>	36
Figura 24: Nueva variable de entorno SE_JAVA_HOME	36
Figura 25: Ejecución <i>elasticsearch.bat</i>	37
Figura 26: Password y token para Kibana	37
Figura 27: Carpeta "bin" de Kibana	38
Figura 28: Resultado de la ejecución de kibana.bat	38
Figura 29: Configuración de Kibana vía interfaz	38
Figura 30: Inicio de sesión en Kibana	39
Figura 31: Página inicial de Kibana	39
Figura 32: Fichero de configuración Logstash	40
Figura 33: Configuración eventos de Windows en Winlogbeat	41
Figura 34: Envío a Kibana desde Winlogbeat	41
Figura 35: Envío a Logstash desde Winlogbeat	42
Figura 36: Comando instalación Winlogbeat como servicio 1	42
Figura 37: Comando instalación Winlogbeat como servicio 2	42
Figura 38: Cargar dashboards de Winlogbeat	42
Figura 39: Solicitud de integración API Key	43
Figura 40: Panel principal de Reglas	43
Figura 41: Creación de regla 1	44
Figura 42: Definición de regla	44
Figura 43: Regla TFM-UOC-ejemplo	44
Figura 44: Pestaña Security-Dashboards	45
Figura 45: Creación de dashboard	45
Figura 46: Dashboard creado ejecutado en última semana	46

Lista de tablas

Tabla 1: Planificación temporal	9
Tabla 2: Tipos de <i>Beats</i> [13]	15
Tabla 3: Registros de seguridad de Windows [17]	17
Tabla 4: Eventos de Windows enviados por <i>winlogbeat</i>	18

1. Introducción

1.1. Contexto y justificación del Trabajo

Con el crecimiento constante de amenazas cibernéticas y la vulnerabilidad de las brechas de seguridad, las empresas se encuentran inmersas en un desafío permanente para proteger sus activos e información crítica. En este contexto, un pilar fundamental de la estrategia de ciberseguridad es la implementación de un Centro de Operaciones de Seguridad (SOC, por su acrónimo en inglés) eficaz. El SOC representa el corazón de la defensa cibernética de una organización, donde se lleva a cabo la supervisión en tiempo real, la detección y la respuesta ante las amenazas.

En el momento en que se inicia este proyecto, muchas organizaciones ya habían reconocido la necesidad de establecer un SOC, aunque a menudo enfrentaban desafíos relacionados con la documentación, la implementación eficiente y la puesta en funcionamiento efectiva de este servicio. Además, el análisis y correlación de datos de registros de eventos de seguridad se había vuelto especialmente complejo debido al volumen y la diversidad de estos datos.

El propósito central de este trabajo es ofrecer una guía minuciosa para la documentación, la implementación y la puesta en marcha de un servicio SOC efectivo, aprovechando la plataforma ELK (Elasticsearch, Logstash, Kibana). ELK, una pila de código abierto, proporciona capacidades de búsqueda y análisis de registros a gran escala, lo que lo convierte en una opción ideal para la gestión de eventos de seguridad en un SOC.

La contribución de este proyecto radica en la creación de un recurso integral destinado a:

- Fomentar la comprensión de la importancia de un SOC en el ámbito de la seguridad cibernética.
- Facilitar la documentación de todos los elementos críticos de la infraestructura y operaciones del SOC.
- Implementar eficazmente la plataforma ELK para el análisis y correlación de eventos de seguridad.
- Establecer procesos y procedimientos sólidos que respalden la puesta en marcha y el funcionamiento continuo del SOC.

En resumen, este trabajo busca enriquecer la seguridad cibernética al proporcionar una guía práctica y detallada para la creación y operación de un SOC respaldado por la plataforma ELK, lo que permitirá a las organizaciones afrontar con mayor solidez las amenazas cibernéticas en el entorno actual.

1.2. Objetivos del Trabajo

Objetivo General:

Diseñar, documentar, implementar y poner en marcha un servicio SOC utilizando la plataforma ELK (Elasticsearch, Logstash, Kibana) como herramienta principal para la gestión de eventos de seguridad.

Objetivos Específicos:

- Seleccionar y configurar adecuadamente las herramientas de la pila ELK (Elasticsearch, Logstash, Kibana) para la recopilación, el almacenamiento y el análisis de registros de eventos de seguridad.
- Exponer la valía de la solución propuesta mediante el uso de dashboards que muestren de manera compacta la información recogida.
- Evaluar la efectividad del SOC implementado a través de pruebas de detección de amenazas y la capacidad de respuesta a incidentes.
- Presentar un informe detallado que incluya la documentación completa del SOC y las recomendaciones para mejoras futuras.

1.3. Enfoque y método seguido

El enfoque para este trabajo ha abarcado diversas etapas. En primer lugar, se ha recopilado exhaustivamente información relacionada con Centros de Operaciones de Seguridad (SOC), Sistemas de Gestión de Información y Eventos de Seguridad (SIEM), así como con la pila ELK (*Elasticsearch*, *Logstash*, *Kibana*).

En la fase de recopilación de información, se ha investigado a fondo la documentación actual para comprender la naturaleza y funcionalidad de los SOC, SIEM. Esto implica identificar mejores prácticas, desafíos comunes y tendencias actuales en el ámbito de la seguridad cibernética.

Tras esto, se ha analizado la documentación existente de la pila ELK. Se han examinado manuales de instalación, configuración y casos de uso. Esta investigación ha incluido la revisión de recursos en línea, documentos técnicos y material oficial para obtener una comprensión completa de las capacidades y configuraciones posibles.

Posteriormente, se ha procedido a la implementación de la pila ELK. Esto implica la configuración precisa de *Elasticsearch* para el almacenamiento eficiente de datos, *Logstash* para la transformación y enriquecimiento de registros, y *Kibana* para la visualización interactiva. Se han seguido las mejores prácticas y directrices de seguridad durante esta fase. Además, se ha instalado el agente *winlogbeat* para el envío de logs hacia la pila.

En la etapa de análisis de datos, se ha utilizado activamente la pila ELK para la recopilación y análisis de datos de eventos de seguridad enviados con *winlogbeat*. Se han explorado las capacidades de búsqueda y recuperación de *Elasticsearch*, así como la transformación de datos crudos mediante *Logstash* para su posterior análisis.

Como parte integral de la implementación, se han desarrollado *dashboards* personalizados en *Kibana* para facilitar la visualización intuitiva de datos. Se han configurado alertas para notificar de inmediato sobre eventos de seguridad críticos, contribuyendo así a la respuesta temprana ante posibles amenazas.

En la fase final, se han analizado los resultados obtenidos a través de la implementación y el uso práctico de la pila ELK. Se han extraído conclusiones significativas sobre la eficacia del SOC respaldado por ELK, destacando áreas de mejora y lecciones aprendidas. Este análisis ha proporcionado una visión valiosa para la gestión continua y la optimización del entorno de seguridad.

1.4. Planificación del Trabajo

Tarea	Inicio	Fin	Duración (días)	Duración (horas)
Introducción	01-oct-23	11-oct-23	10	2
Objetivos del Trabajo	01-oct-23	12-oct-23	11	1
Enfoque y método seguido	03-oct-23	12-oct-23	9	3
Planificación del Trabajo	04-oct-23	12-oct-23	8	2
Estado del arte	04-oct-23	14-oct-23	10	1
PEC1	01-oct-23	14-oct-23	13	9
Conceptos básicos sobre seguridad informática	30-oct-23	11-nov-23	12	2
Qué es un SOC y cuáles son sus funciones	30-oct-23	12-nov-23	13	1
Qué es un ELK y cómo se compone	01-nov-23	11-nov-23	10	1
Ventajas y desafíos de usar un ELK en un SOC	01-nov-23	12-nov-23	11	2
Diseño e implementación del ELK	05-nov-23	12-nov-23	7	4
Requisitos funcionales y no funcionales	05-nov-23	12-nov-23	7	1
Arquitectura y componentes del ELK	05-nov-23	12-nov-23	7	1
PEC2: 13 noviembre 2023	30-oct-23	12-nov-23	13	21
Proceso de instalación y configuración del ELK	15-nov-23	13-dic-23	28	8
Integración con las fuentes de datos del SOC	15-nov-23	13-dic-23	28	4
Desarrollo de dashboards y alertas para el análisis de seguridad	08-dic-23	13-dic-23	5	2
Documentación del ELK	08-dic-23	13-dic-23	5	1
PEC3: 15 diciembre 2023	15-nov-23	13-dic-23	28	15
Manual de usuario	26-dic-23	07-ene-24	12	2
Manual técnico	26-dic-23	07-ene-24	12	2
Manual de mantenimiento y actualización	26-dic-23	07-ene-24	12	2
Memoria final	07-ene-24	08-ene-24	1	4
PEC4: 10 enero 2024	26-dic-23	08-ene-24	13	10

Tabla 1: Planificación temporal

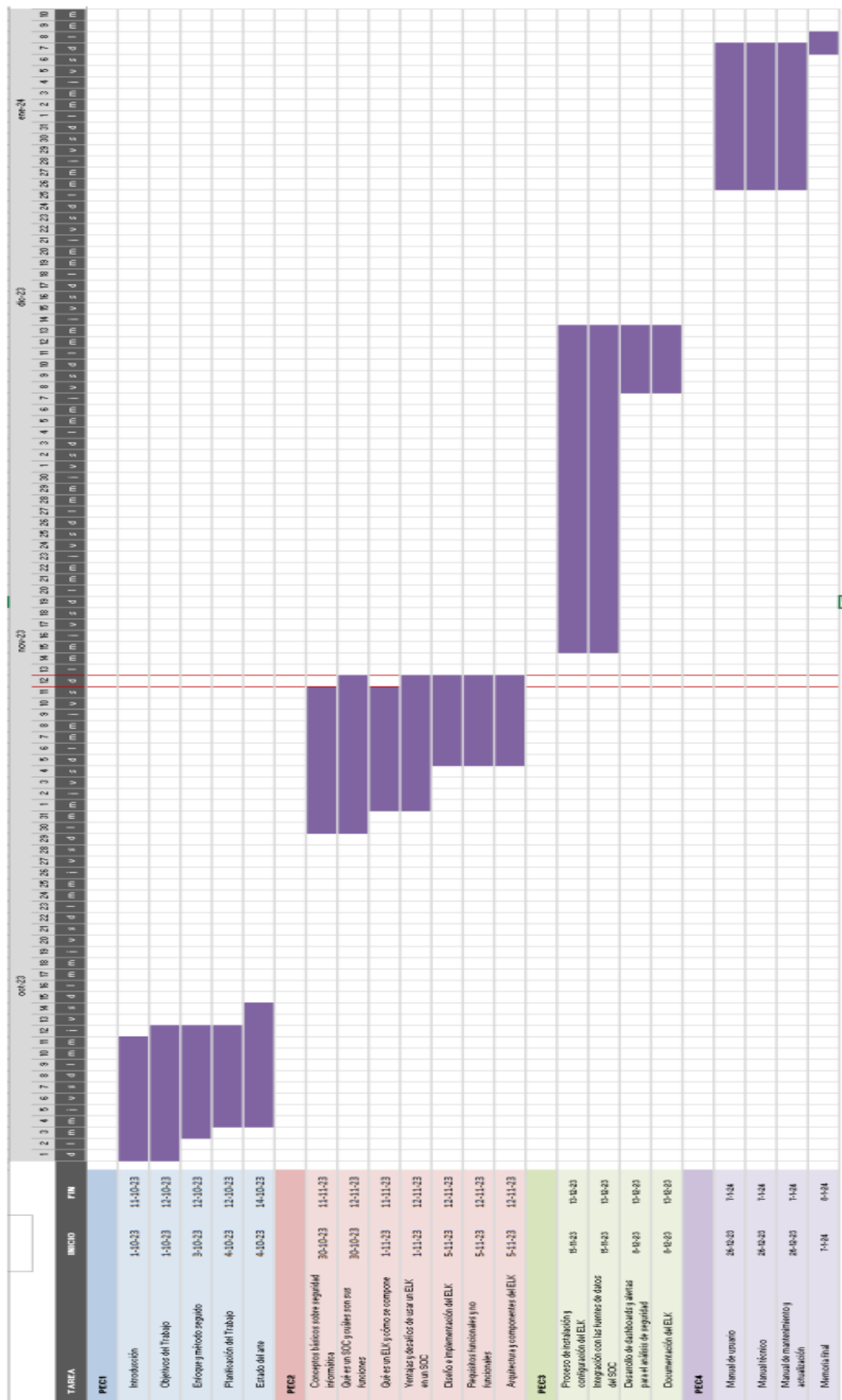


Figura 1: Diagrama de Gantt

1.5. Estado del arte

El análisis del estado actual de la investigación y las prácticas en el ámbito de la ciberseguridad y la implementación de Centros de Operaciones de Seguridad (SOC) respaldados por tecnologías como ELK (*Elasticsearch*, *Logstash*, *Kibana*) es fundamental para comprender las tendencias y los avances en este campo en constante evolución.

En las últimas décadas, se ha observado una progresión constante en la sofisticación y diversificación de las amenazas cibernéticas. Ataques como el *ransomware*, el phishing y las intrusiones dirigidas han adquirido notoriedad, lo que ha impulsado la necesidad de implementar SOC efectivos. La ciberseguridad se ha convertido en una prioridad en un mundo digital interconectado [1].

Los SOC han experimentado una transformación significativa en sus funciones y roles. Han evolucionado de ser entidades reactivas que solo respondían a incidentes a ser proactivos en la prevención de amenazas. Las responsabilidades en un SOC incluyen la supervisión en tiempo real, la detección y respuesta a incidentes, la gestión de vulnerabilidades y la evaluación de riesgos. Los roles clave en un SOC abarcan desde analistas de seguridad hasta ingenieros de seguridad y directores de SOC [2].

ELK, junto con otras soluciones de análisis de datos, ha ganado prominencia en la gestión de eventos de seguridad. La capacidad de ELK para recolectar, almacenar, analizar y visualizar datos de seguridad ha hecho que sea una elección atractiva para organizaciones de diversos sectores. Además, otras soluciones como *Splunk* también se utilizan ampliamente en SOC [3].

La gestión de eventos de seguridad presenta desafíos significativos, incluyendo la identificación temprana de amenazas, la correlación precisa de eventos, la reducción de falsos positivos y la respuesta eficaz a incidentes. Las técnicas de aprendizaje automático y el análisis de comportamiento se han vuelto elementos esenciales para la detección de amenazas, permitiendo una mayor precisión en la identificación y respuesta a incidentes [4].

2. Materiales y métodos

2.1. Que es un SOC y cuáles son sus funciones

SOC, por sus siglas en inglés, se refiere a *Security Operations Center* o "Centro de Operaciones de Seguridad". Un SOC es un componente fundamental en la estrategia de seguridad de una organización y sirve como un centro de comando centralizado para monitorear, detectar, responder y mitigar amenazas de seguridad cibernética [5].

Las principales funciones y propósitos de un SOC incluyen:

- **Monitoreo de Seguridad:**
 - Supervisar continuamente la infraestructura de TI y las redes en busca de actividades sospechosas o anómalas.
- **Detección de Amenazas:**
 - Utilizar herramientas y tecnologías, como SIEM (*Security Information and Event Management*), para detectar patrones de actividad que podrían indicar posibles amenazas o violaciones de seguridad.
- **Análisis de Incidentes:**
 - Analizar los eventos de seguridad identificados para determinar la gravedad y la naturaleza de las posibles amenazas.
- **Respuesta a Incidentes:**
 - Desarrollar y ejecutar planes de respuesta a incidentes para contener y mitigar amenazas tan pronto como se detectan.
- **Investigación Forense:**
 - Llevar a cabo investigaciones forenses para comprender la causa y el alcance de los incidentes de seguridad.
- **Integración de Herramientas de Seguridad:**
 - Implementar y administrar herramientas de seguridad, como firewalls, sistemas de detección y prevención de intrusiones, y antivirus, para fortalecer la postura de seguridad.
- **Generación de Informes y Cumplimiento:**
 - Crear informes periódicos sobre la actividad de seguridad, proporcionando análisis detallados y métricas clave para la toma de decisiones y el cumplimiento normativo.
- **Colaboración y Coordinación:**
 - Colaborar con otras áreas de la organización, como el equipo de TI, para compartir información y coordinar respuestas a incidentes de seguridad.

Un SOC juega un papel crucial en la defensa proactiva contra las amenazas cibernéticas, permitiendo a las organizaciones identificar y abordar rápidamente los incidentes de seguridad. Además, ayuda a mejorar la postura de seguridad general mediante la implementación de controles preventivos y la adaptación continua a las evoluciones en las tácticas de los ciberdelincuentes. [6]

2.2. Qué es un SIEM y cómo funciona

Un SIEM (*Security Information and Event Management*) es una solución integral diseñada para proporcionar visibilidad y control sobre la seguridad de la información en una organización. Este sistema se encarga de recopilar, correlacionar, analizar y presentar datos de seguridad provenientes de diversos recursos dentro de una red [7].

Una plataforma SIEM opera al recopilar datos de registros y eventos generados por diversas tecnologías en el entorno de una organización, brindando a los analistas de seguridad una visión integral de la infraestructura de TI. Un SIEM eficaz automatiza la mitigación de amenazas conocidas y, al mismo tiempo, destaca situaciones más complejas, permitiendo a los analistas determinar si se requiere una investigación y acción adicionales [8].

En el día a día de una organización, dispositivos, redes, servidores, aplicaciones y sistemas generan una gran cantidad de datos operativos. Estos datos contienen información valiosa que puede contribuir a la seguridad del entorno. Es en este contexto que la SIEM desempeña un papel crucial.

De manera general, las funciones de un SIEM son [9] [10]:

- **Recopilación de Datos:**
 - Un SIEM recopila datos de eventos y registros de seguridad de una variedad de fuentes, como sistemas operativos, aplicaciones, dispositivos de red y sistemas de seguridad.
- **Normalización y Correlación:**
 - Normaliza los datos para que tengan un formato consistente y los correlaciona para identificar patrones o relaciones que podrían indicar actividades maliciosas.
- **Análisis de Amenazas:**
 - Utiliza reglas predefinidas y algoritmos para analizar la información recopilada y detectar posibles amenazas de seguridad.
- **Generación de Alertas:**
 - Genera alertas en tiempo real cuando se detecta una actividad sospechosa o un patrón de comportamiento anómalo. Estas alertas pueden variar en gravedad y ayudan a los equipos de seguridad a priorizar respuestas.
- **Dashboards e Informes:**
 - Proporciona *dashboards* e informes que resumen la actividad de seguridad, permitiendo a los analistas y administradores obtener una visión general y detallada del estado de la seguridad.
- **Almacenamiento a Largo Plazo:**
 - Almacena datos a largo plazo para permitir la investigación forense, cumplimiento de normativas y análisis histórico.
- **Integración con Herramientas de Seguridad:**

- Se integra con otras herramientas de seguridad, como firewalls, sistemas de detección y prevención de intrusiones, antivirus, entre otras, para mejorar la capacidad de respuesta.
- **Respuesta a Incidentes:**
 - Facilita la respuesta a incidentes al proporcionar información detallada sobre amenazas, lo que permite a los equipos de seguridad tomar medidas correctivas de manera eficiente.

2.3. Qué es un ELK y cómo se compone

ELK hace referencia a un conjunto de herramientas de gran potencial de código abierto que se combinan para crear una herramienta de administración de registros permitiendo la monitorización, consolidación y análisis de logs generados en múltiples servidores, estas herramientas son [11] [12]:

- **Elasticsearch:** Es un motor de búsqueda y análisis distribuido y de código abierto. Se utiliza para almacenar y buscar datos. En el contexto de ELK, *Elasticsearch* almacena los datos de registros y eventos, lo que facilita la búsqueda y recuperación eficientes.
- **Logstash:** Es un procesador de datos que ingiere, procesa y envía datos a *Elasticsearch*. *Logstash* se encarga de la recopilación de datos desde múltiples fuentes, la transformación de esos datos según sea necesario y el envío de los datos procesados a *Elasticsearch* para su indexación.
- **Kibana:** Es una interfaz de usuario web que permite visualizar y explorar los datos almacenados en *Elasticsearch*. *Kibana* proporciona un entorno gráfico para realizar consultas y crear visualizaciones interactivas basadas en los datos almacenados en *Elasticsearch*. Permite a los usuarios analizar y entender fácilmente los registros y eventos.
- **Beats:** Agente de cliente a cargo de empujar cualquier archivo nuevo o modificación de la fuente de datos. Actualmente, los *Beats* oficiales de *Elasticsearch* son los siguientes:

Beat	Descripción
<i>Auditbeat</i>	Lee datos del <i>framework</i> de auditoría de Linux (auditd) y controla la integridad de los archivos.
<i>Metricbeat</i>	Extrae métricas de sistema y aplicaciones. Se integra de forma nativa con infinidad de tecnologías gracias a los módulos preexistentes.
<i>Filebeat</i>	Recolecta logs de sistema y aplicaciones. Se integra de forma nativa con infinidad de tecnologías gracias a los módulos preexistentes.
<i>Winlogbeat</i>	Misma funcionalidad que <i>Filebeat</i> para leer los eventos de los sistemas Windows.
<i>Packetbeat</i>	Monitoriza el tráfico de red de tu infraestructura y consigue métricas como latencia y errores, tiempos de respuesta, patrones y tendencias de comportamiento de usuarios.
<i>Heartbeat</i>	Mide el tiempo de disponibilidad de un sistema o aplicación de forma activa con sondas de monitorización.

Tabla 2: Tipos de *Beats* [13]

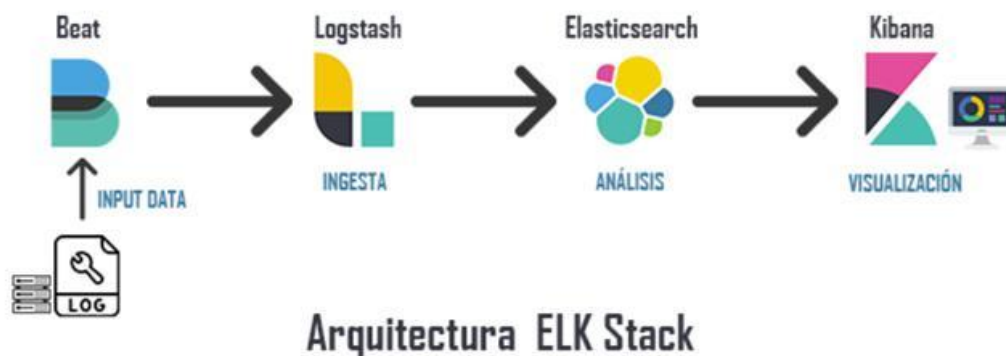


Figura 2: Arquitectura pila ELK [12]

2.4. Ventajas y desafíos de usar un ELK en un SOC

Una de las principales fortalezas de implementar la pila ELK radica en su capacidad para recopilar y analizar registros de manera efectiva. A través de *Logstash*, un agente de recolección de datos, se recopilan registros de diversas fuentes, se filtran y se envían a *Elasticsearch* para su almacenamiento y análisis. *Elasticsearch*, una base de datos de búsqueda distribuida facilita el almacenamiento y búsqueda en tiempo real de grandes cantidades de datos. *Kibana*, una plataforma de análisis y visualización permite a los usuarios crear paneles personalizados para analizar y visualizar los datos de registros de manera intuitiva.

Otro punto a favor de contar con ELK es su capacidad para monitorear el rendimiento del sistema en tiempo real y detectar problemas de forma

proactiva. Utilizando *Logstash* para recopilar y enviar registros a *Elasticsearch*, los usuarios pueden identificar rápidamente problemas y tomar medidas correctivas antes de que escalen. *Kibana* ofrece una variedad de paneles y gráficos personalizables que posibilitan el monitoreo continuo del rendimiento del sistema en tiempo real.

La pila ELK destaca por su alta flexibilidad y su capacidad para adaptarse a las necesidades y requisitos específicos de cada empresa. *Elasticsearch* es altamente escalable, capaz de manejar grandes volúmenes de datos. *Logstash*, por su parte, es altamente personalizable, permitiendo filtrar y transformar registros según las necesidades particulares del usuario. *Kibana* ofrece una configuración extensa y opciones diversas para visualización y análisis de datos, proporcionando una solución adaptable a diferentes contextos empresariales [14].

Por último, cabe señalar su facilidad de integración con otros sistemas y herramientas de monitoreo y análisis de datos. *Elasticsearch* se integra de manera fluida con otras bases de datos y sistemas de monitoreo, posibilitando a los usuarios consolidar y analizar datos provenientes de diversas fuentes. *Logstash* se enlaza con diversas fuentes de datos y herramientas de análisis de datos, brindando a los usuarios la capacidad de personalizar su solución de monitoreo y análisis de datos de acuerdo con sus necesidades específicas.

En resumen, la adopción de la pila ELK puede ser altamente ventajosa para la monitorización debido a su capacidad integral para recopilar y almacenar datos, herramientas avanzadas de visualización y análisis, funciones de búsqueda de texto completo, alertas y notificaciones, así como su escalabilidad y la facilidad de integración con otras herramientas de monitorización. Al implementar una pila ELK, las organizaciones pueden potenciar la capacidad de sus equipos de operaciones e infraestructura para supervisar el entorno y abordar rápidamente cualquier problema, lo que puede resultar en una mejora significativa en la eficiencia y la reducción del tiempo de inactividad [15].

2.5. Eventos de seguridad de Windows

Los eventos de Windows o eventos del sistema Windows guardan información de lo que está ocurriendo en el equipo. Se almacenan eventos de Windows de una aplicación o del sistema operativo como tal [16].

Tipo de registro	Descripción
ADAM	Registra los eventos registrados por el repositorio de ADAM.
Aplicación	Registra los eventos registrados por una aplicación en el equipo, como el inicio o un error de un servicio.
Servicio de directorio	Registra eventos relacionados con los controladores de dominio que mantienen la base de datos de seguridad.
Servicio de réplica de archivos	Registra eventos relacionados con los servicios de réplica de archivos proporcionados por el sistema operativo.
Seguridad	Registra eventos que incluyen intentos de entrada a la sesión, acceso a archivos y directorios, y cambios en la directiva de seguridad que se basan en las opciones de la directiva de auditoría.
Sistema	Registra los eventos registrados por los componentes del sistema de Windows, como el error de un controlador o servicios que se inician y se detienen.

Tabla 3: Registros de seguridad de Windows [17]

2.6. Diseño e implementación del ELK

En este trabajo, la pila ELK ha sido instalada en un ordenador personal con el sistema operativo Windows 10.

Todos los elementos de la pila han sido descargados desde el repositorio oficial de *Elastic* [18] en su última versión disponible (8.11.2) a 7 de diciembre de 2023.

Ha sido necesaria la descarga e instalación de Java en su versión 17.0.9 desde el repositorio oficial de Oracle [19] para la correcta puesta en funcionamiento de la pila. Además, también se ha requerido definir la variable de entorno *SE_JAVA_HOME*.

El agente *Elasticsearch* ha sido configurado para escuchar conexiones en la máquina local (*localhost*) en el puerto 9200, con el usuario “elastic” y una contraseña. Por su parte, *Kibana* ha sido configurado para desplegarse en el puerto 5601, también en la máquina local, y comunicarse con *Elasticsearch*.

Por su parte, *Logstash* ha sido configurado para la recepción de logs por el puerto 5044 de la dirección IP local de la subred (192.168.1.48), obviando las configuraciones de encriptación SSL, ya que no es objeto en este trabajo.

Toda la configuración de los elementos de la pila se detalla en el [Anexo A: Guía de instalación de la pila ELK](#).

2.7. Elección e implementación de *Beats*

La extensión *beat* elegida para el envío de logs a la pila ha sido *winlogbeat*, debido a su diseño específico para Windows, facilidad de configuración, bajo consumo de recursos e integración nativa con la pila ELK.

Winlogbeat ha sido descargada, en su versión 8.11.3, también desde el repositorio oficial [18] e instalada en la misma máquina que la pila (por facilidad de configuración), para disponer de eventos de seguridad de Windows en la solución ELK.

Se ha instalado *winlogbeat* como servicio de Windows, para enviar logs al puerto 5044 de la dirección IP 192.168.1.48 (dirección y puerto de escucha de *Logstash*) y enviar eventos de seguridad generados en el propio sistema operativo Windows donde se ha instalado *winlogbeat*.

Los eventos de seguridad de Windows para los que se ha configurado el envío a *Logstash* son aquellos que venían por defecto en el fichero de configuración *winlogbeat.yml*, que se disponen en la siguiente tabla.

Nombre	Eventos
Application	Generados en las últimas 72h
System	Todos
Security	Todos
Microsoft-Windows-Sysmon/Operational	Todos
Windows Powershell	400, 403, 600, 800
Microsoft-Windows-Powershell/Operational	4103, 4104, 4105, 4106
ForwardedEvents	Tags: [forwarded]

Tabla 4: Eventos de Windows enviados por *winlogbeat*

Todos los pasos seguidos para la configuración del servicio se detallan en el [Anexo A: Guía de instalación de la pila ELK](#).

2.8. Reglas y *Dashboard* por defecto

En un entorno ELK, de manera opcional, se dispone de un conjunto de reglas de correlación ya desarrolladas para instalar en el sistema y aplicar a los eventos entrantes que correspondan.

Con estas reglas, es posible sentar las bases del SIEM para conseguir una monitorización de las vulnerabilidades más comunes en diferentes entornos IT,

tales como AWS (Amazon Web Services), Kubernetes, LSAASS, Windows, Linux, Microsoft365, etc.

En la documentación oficial se dispone del listado completo de reglas predefinidas de Elastic [20]

Add Elastic Rules

See what's new in Prebuilt Security Detection Rules

Search by rule name

Tags 87

<input type="checkbox"/>	Rule	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 6	Risk score	Severity	
<input type="checkbox"/>	Linux Restricted Shell Breakout via Linux Binary(s)	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 6	47	Medium	Install rule
<input type="checkbox"/>	Suspicious File Creation in /etc for Persistence	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 8	47	Medium	Install rule
<input type="checkbox"/>	Unusual File Creation - Alternate Data Stream	<input type="checkbox"/> 0/2 integrations	<input type="checkbox"/> 6	47	Medium	Install rule
<input type="checkbox"/>	Potentially Successful MFA Bombing via Push Notifications	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 3	73	High	Install rule
<input type="checkbox"/>	Abnormal Process ID or Lock File Created	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 7	47	Medium	Install rule
<input type="checkbox"/>	Potential Persistence Through Run Control Detected	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 7	47	Medium	Install rule
<input type="checkbox"/>	PowerShell Script with Token Impersonation Capabilities	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 5	47	Medium	Install rule
<input type="checkbox"/>	New Systemd Service Created by Previously Unknown Process	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 7	47	Medium	Install rule
<input type="checkbox"/>	Suspicious File Changes Activity Detected	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 5	47	Medium	Install rule
<input type="checkbox"/>	Suspicious Process Access via Direct System Call	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 7	73	High	Install rule
<input type="checkbox"/>	Potential Persistence Through init.d Detected	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 7	47	Medium	Install rule
<input type="checkbox"/>	Suspicious Process Spawned from MOTD Detected	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 7	73	High	Install rule
<input type="checkbox"/>	FirstTime Seen Account Performing DCSync	<input type="checkbox"/> 0/1 integrations	<input type="checkbox"/> 8	73	High	Install rule

Figura 3: Reglas predefinidas de Elastic

Además, con el *plugin* de *Winlogbeat*, es posible cargar una serie de dashboards por defecto que muestran de manera visual la ingesta de eventos de Windows, según diferentes patrones.

Estos dashboards, de manera combinada junto a las reglas mencionadas anteriormente, en este caso las aplicables a Windows, conformarían un punto de partida óptimo para monitorizar un entorno Windows.

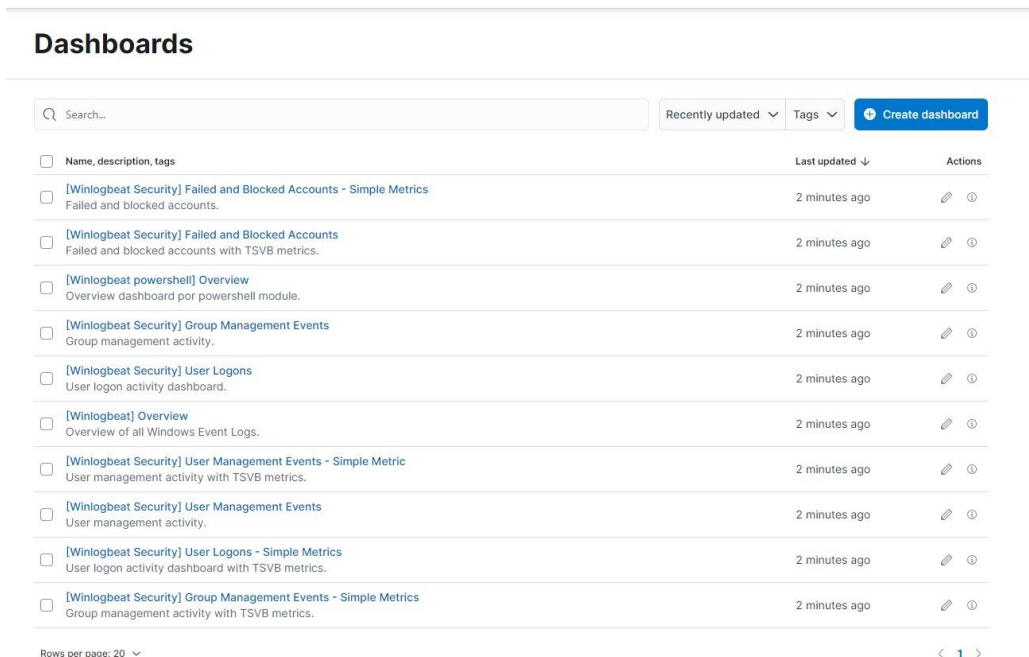


Figura 4: Dashboards por defecto de Winlogbeat

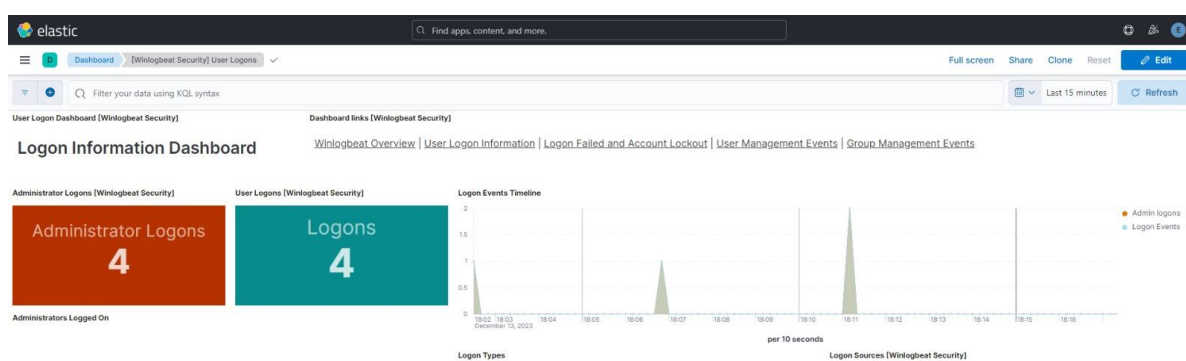


Figura 5: Dashboard de información de logins

En este trabajo no se ha ahondado en el uso y aplicación de estos elementos disponibles, tan solo se pretende mostrar al usuario la practicidad y utilidad de lo expuesto.

2.9. Creación de regla analítica y *dashboard* de ejemplo

Con intención de mostrar de manera explícita la utilidad del ELK en un entorno SOC funcionando como SIEM, se ha pretendido elaborar una regla analítica de correlación de un evento de Windows, así como un *dashboard* sencillo de visualización del evento.

La regla elaborada genera una alerta de severidad baja cada vez que se ingesta un evento con id de Windows “4798” [21] y el usuario destino es “Felipe”.

Por su parte, el *dashboard* generado muestra la distribución a lo largo del tiempo de usuarios destino de los diferentes eventos, según los distintos id de Windows recibidos.

Los pasos detallados de ambos procesos están disponibles en el [Anexo B: Guía de configuración de reglas y dashboards](#).

2.10. Requisitos funcionales y no funcionales

Los requisitos funcionales y no funcionales son dos categorías distintas de especificaciones que se utilizan en el desarrollo de software para definir lo que debe hacer el sistema y cómo debe hacerlo.

Los requisitos funcionales describen las funciones específicas que el sistema debe realizar. Los requisitos funcionales de este trabajo son:

- **Ingestión de Datos:** El sistema ELK debe ser capaz de recopilar y procesar datos de diversas fuentes, como registros de aplicaciones, eventos de red, etc.
- **Indexación Eficiente:** *Elasticsearch* debe realizar la indexación de datos de manera rápida y eficiente para facilitar la búsqueda y recuperación.
- **Transformación de Registros:** *Logstash* debe ser capaz de transformar registros según las necesidades específicas del usuario antes de enviarlos a *Elasticsearch*.
- **Búsqueda Avanzada:** *Elasticsearch* debe proporcionar capacidades avanzadas de búsqueda, incluyendo búsqueda de texto completo, filtrado y consultas complejas.
- **Visualización Interactiva:** *Kibana* debe ofrecer una interfaz de usuario intuitiva para crear *dashboards* interactivos y visualizar datos almacenados en *Elasticsearch*.
- **Alertas y Notificaciones:** El sistema debe permitir la configuración de alertas basadas en ciertos criterios para notificar a los usuarios sobre eventos críticos.

Los requisitos no funcionales son aspectos del sistema que no describen funciones específicas, pero que son igualmente críticos para su éxito y eficiencia. Los requisitos no funcionales de este trabajo son:

- **Seguridad:** Se deben implementar medidas de seguridad robustas, como cifrado de datos, autenticación segura y control de acceso, para proteger la integridad de la información.
- **Facilidad de Implementación y Configuración:** El proceso de implementación y configuración de la pila ELK debe ser claro y fácil de seguir, facilitando su adopción por parte de los usuarios.
- **Mantenibilidad:** La pila ELK debe ser fácil de mantener y actualizar, permitiendo la incorporación de nuevas características y corrección de errores de manera eficiente.

2.11. Arquitectura y diseño del sistema montado

En este apartado se pretende mostrar el esquema de red de la pila ELK montada en este trabajo.

De esta manera, se pretende conseguir una comprensión visual de la forma en la que han sido instalados los diferentes servicios que se implementan en este trabajo, y cuál es el flujo de la comunicación entre estos.

En la correspondiente figura, se muestran los diferentes servicios desplegados, con los puertos en los que escuchan, y sus relaciones con los servicios hacia los que tienen comunicación.

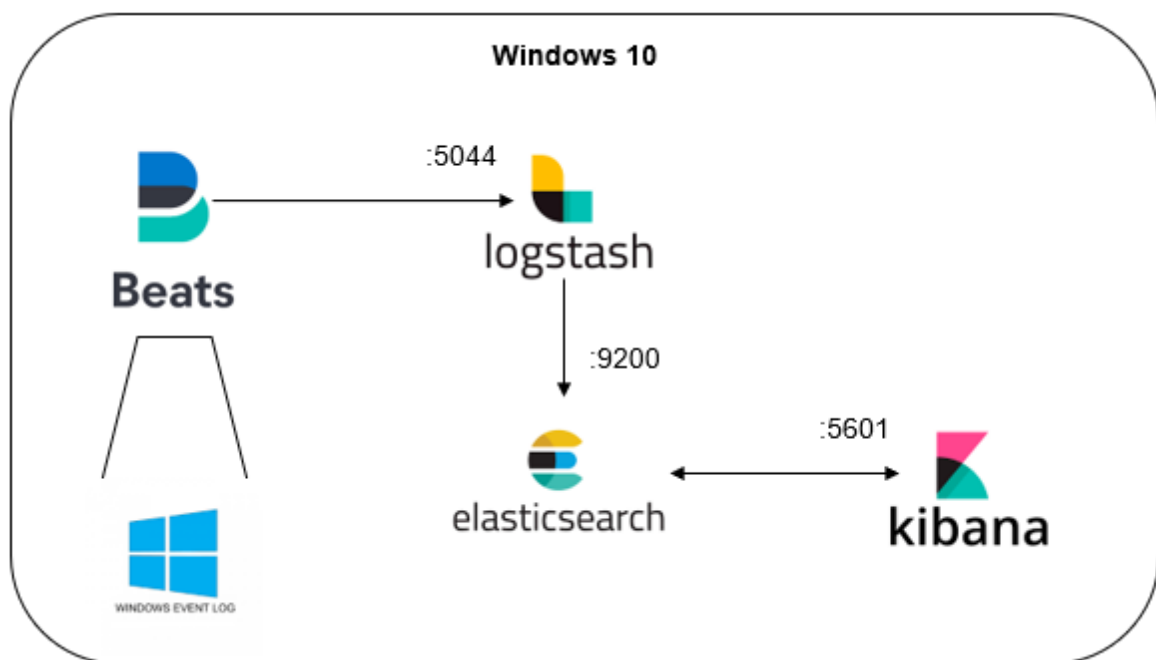


Figura 6: Diseño del sistema montado

3. Validación de resultados

En este apartado se pretende comprobar el correcto funcionamiento al completo de cada uno de los elementos instalados o elaborados en el apartado anterior.

3.1 Comprobación del estado de los servicios desplegados

Para validar la instalación de *Elasticsearch*, se ha abierto el navegador de Chrome [22] y se ha realizado una consulta al puerto 9200 de la máquina *localhost*, donde ha sido instalado el servicio.

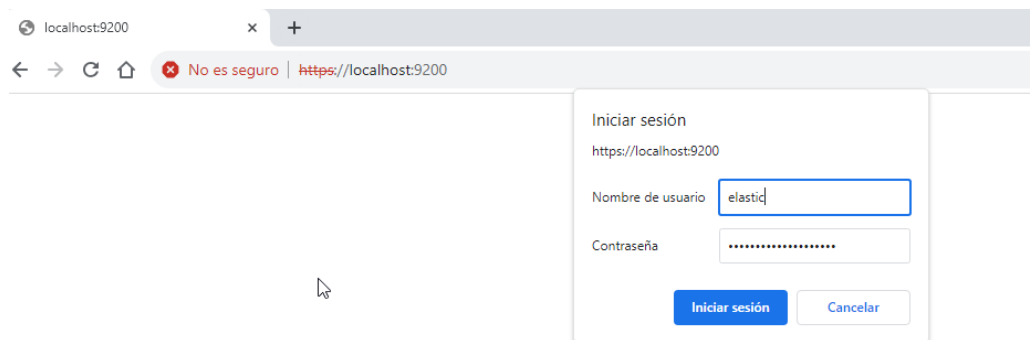


Figura 7: Validación despliegue Elasticsearch 1

Tras introducir las credenciales que se indicaron a la hora de poner en marcha el servicio, se comprueba que Elasticsearch está desplegado de manera correcta según la documentación oficial [23].

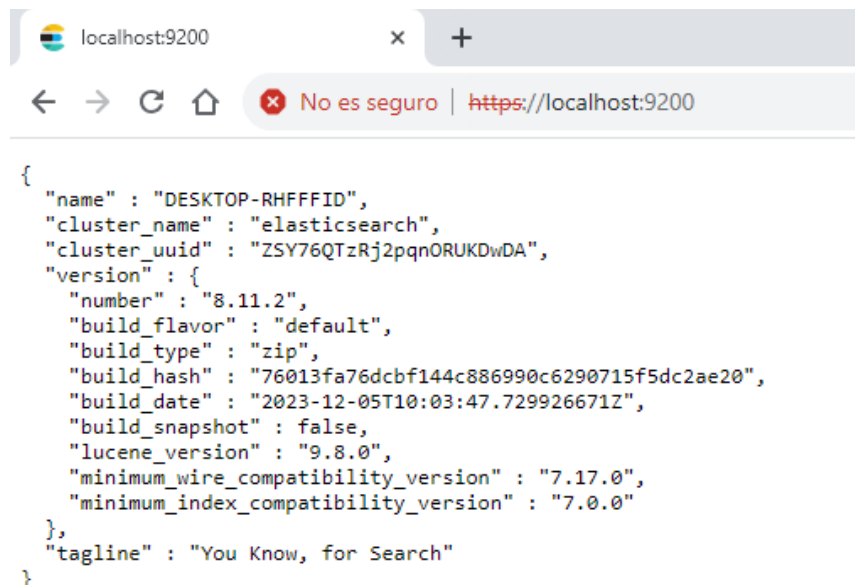


Figura 8: Validación despliegue Elasticsearch 2

En el caso de *Kibana*, simplemente ha sido necesario acceder al puerto 5601 de la máquina *localhost*, de nuevo desde chrome, para visualizar el panel inicial.

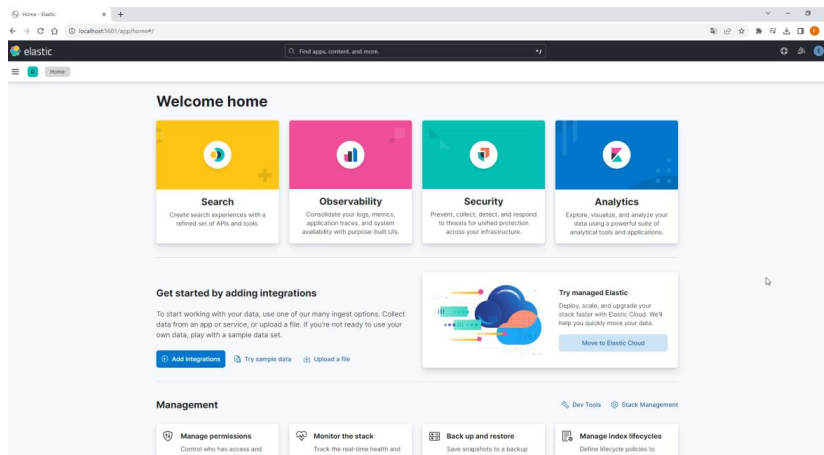


Figura 9: Validación despliegue Kibana

Para *Logstash*, simplemente es necesario fijarse en la salida de comandos a la hora de ejecutar el servicio desde la terminal.

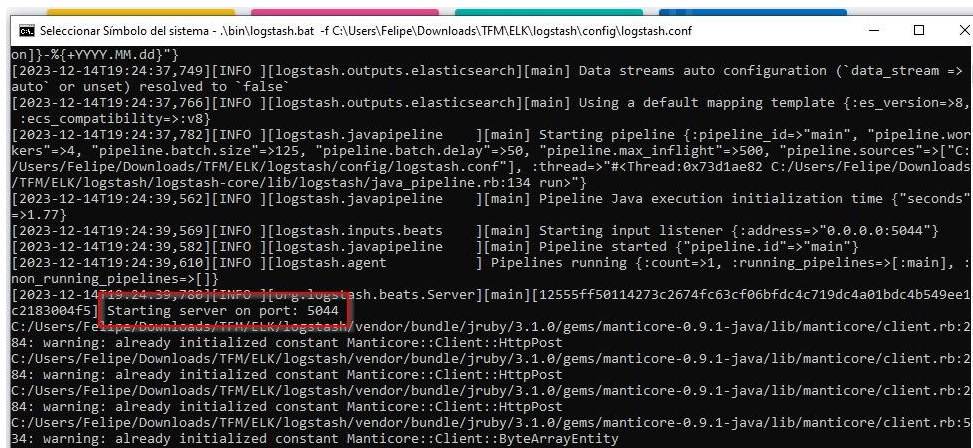


Figura 10: Validación despliegue Logstash

Por último, para comprobar *Winlogbeat*, al haber sido instalado como servicio de Windows, ha sido posible validarlo desde el aplicativo "Servicios" del propio sistema operativo Windows.

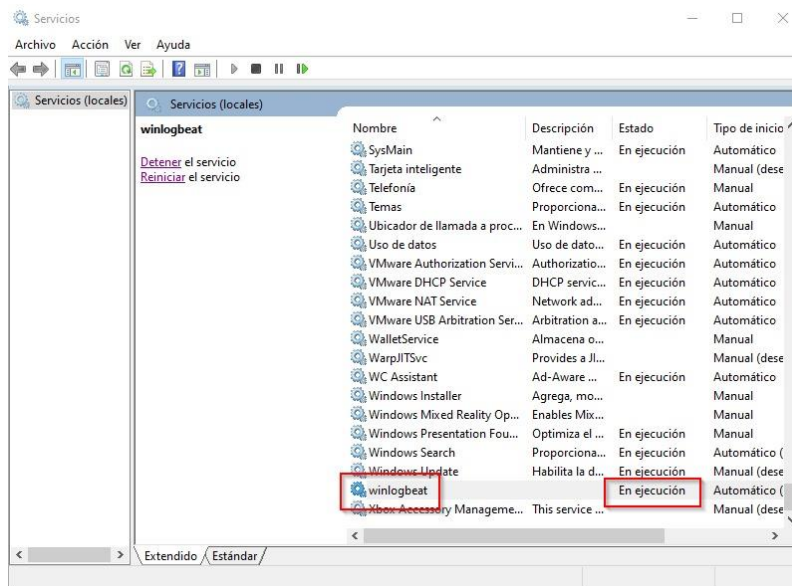


Figura 11: Validación despliegue Winlogbeat

3.2 Correcta visualización en Kibana

Una vez comprobada la satisfactoria instalación de los servicios, es necesario corroborar la visualización correcta en Kibana, para ello ha sido necesario navegar por los diferentes paneles de la interfaz y comprobar su funcionamiento al completo.

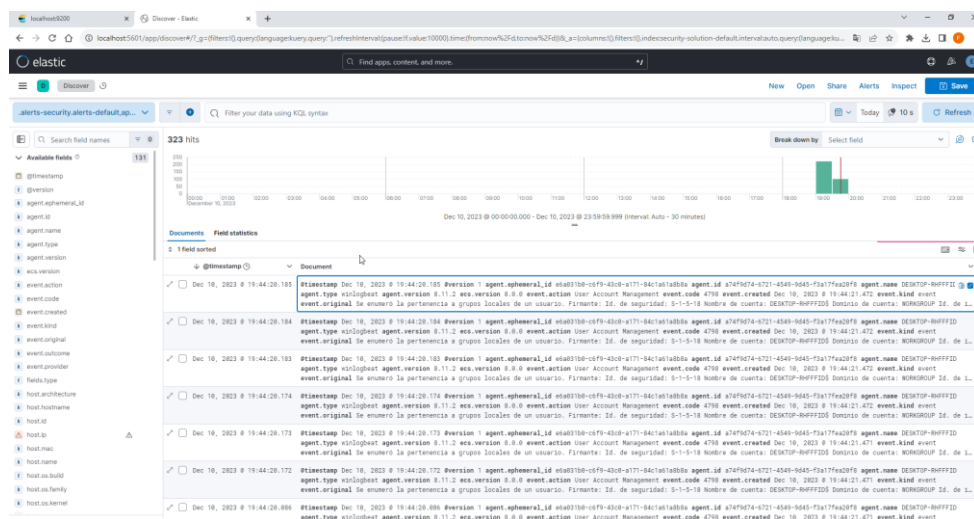


Figura 12: Panel Discover en Kibana

3.3 Ingesta y visualización de eventos de Windows

Es necesario comprobar que los eventos de Windows que se están generando en el sistema están siendo enviados de manera apropiada por Winlogbeat, así como recibidos por Logstash y son visibles en Kibana.

Para ello, se han observado de manera paralela eventos en el visor de eventos de Windows y en Kibana, ratificando lo anterior

Palabras clave	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
Auditoría correcta	13/12/2023 18:26:28	Microsoft Windows security a...	4672	Special Logon
Auditoría correcta	13/12/2023 18:26:28	Microsoft Windows security a...	4624	Logon
Auditoría correcta	13/12/2023 18:26:28	Microsoft Windows security a...	4672	Special Logon
Auditoría correcta	13/12/2023 18:26:28	Microsoft Windows security a...	4624	Logon

Figura 13: Eventos en el visor de eventos de Windows

Timestamp	Document
Dec 13, 2023 @ 18:26:28.643	@timestamp Dec 13, 2023 @ 18:26:28.643 @version 1 agent.ephemeral_id 4fbee7c0-1f0a-4fdd-b383-07f019fcd326 agent.id a74f9d74-6721-4549-9d45-f3a17fea20f8 agent.name DESKTOP-RHFFID agent.type winlogbeat agent.version 8.11.2 ecs.version 8.0.0 event.action Special Logon event.code 4672 event.created Dec 13, 2023 @ 18:26:31.069 event.kind event event.original Se asignaron privilegios especiales a un nuevo inicio de sesión. Sujeto: Id. de seguridad: S-1-5-18 Nombre de cuenta: SYSTEM Dominio de cuenta: NT AUTHORITY Id. de inicio de sesión: 0x3...
Dec 13, 2023 @ 18:26:28.643	@timestamp Dec 13, 2023 @ 18:26:28.643 @version 1 agent.ephemeral_id 4fbee7c0-1f0a-4fdd-b383-07f019fcd326 agent.id a74f9d74-6721-4549-9d45-f3a17fea20f8 agent.name DESKTOP-RHFFID agent.type winlogbeat agent.version 8.11.2 ecs.version 8.0.0 event.action Logon event.code 4624 event.created Dec 13, 2023 @ 18:26:31.069 event.kind event event.original Se inició sesión correctamente en una cuenta. Firmante: Id. de seguridad: S-1-5-18 Nombre de cuenta: DESKTOP-RHFFID Dominio de cuenta: WORKGROUP Id. de inicio de sesión: 0x3E7 Información de ...
Dec 13, 2023 @ 18:26:28.610	@timestamp Dec 13, 2023 @ 18:26:28.610 @version 1 agent.ephemeral_id 4fbee7c0-1f0a-4fdd-b383-07f019fcd326 agent.id a74f9d74-6721-4549-9d45-f3a17fea20f8 agent.name DESKTOP-RHFFID agent.type winlogbeat agent.version 8.11.2 ecs.version 8.0.0 event.action Special Logon event.code 4672 event.created Dec 13, 2023 @ 18:26:31.069 event.kind event event.original Se asignaron privilegios especiales a un nuevo inicio de sesión. Sujeto: Id. de seguridad: S-1-5-18 Nombre de cuenta: SYSTEM Dominio de cuenta: NT AUTHORITY Id. de inicio de sesión: 0x3...
Dec 13, 2023 @ 18:26:28.610	@timestamp Dec 13, 2023 @ 18:26:28.610 @version 1 agent.ephemeral_id 4fbee7c0-1f0a-4fdd-b383-07f019fcd326 agent.id a74f9d74-6721-4549-9d45-f3a17fea20f8 agent.name DESKTOP-RHFFID agent.type winlogbeat agent.version 8.11.2 ecs.version 8.0.0 event.action Logon event.code 4624 event.created Dec 13, 2023 @ 18:26:30.682 event.kind event event.original Se inició sesión correctamente en una cuenta. Firmante: Id. de seguridad: S-1-5-18 Nombre de cuenta: DESKTOP-RHFFID Dominio de cuenta: WORKGROUP Id. de inicio de sesión: 0x3E7 Información de ...

Figura 14: Eventos en Kibana

3.4 Funcionamiento apropiado de regla analítica

La regla de correlación elaborada ha sido testeada generando un evento de Windows que la dispare, por tanto, se han enumerado desde el usuario "Felipe" los permisos de este mismo documento que se está redactando, lo cuál ha generado una serie de eventos 4798.

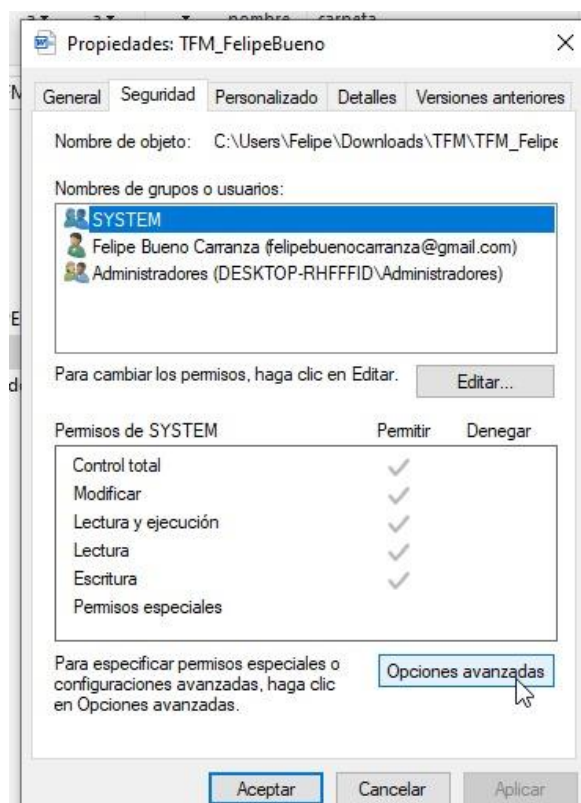


Figura 15: Enumeración de permisos de usuario (1)

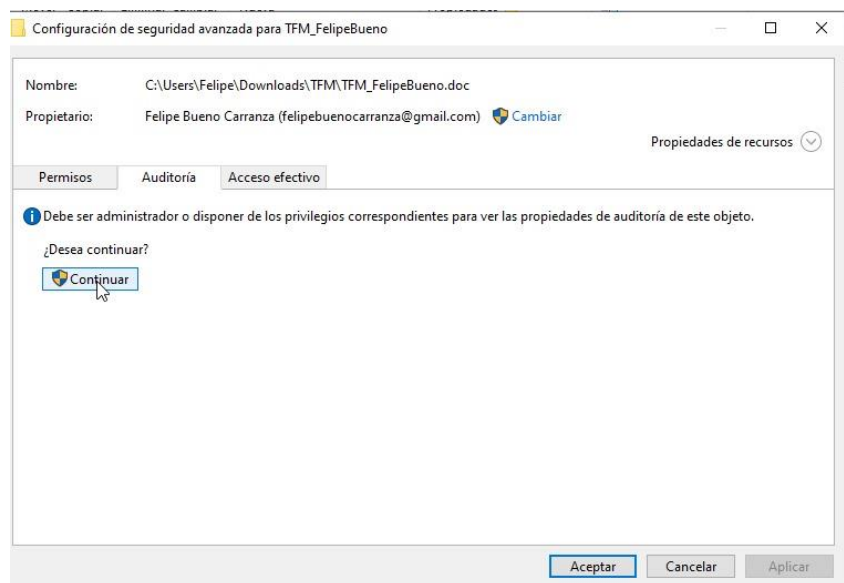


Figura 16: Enumeración de permisos de usuario (2)

Posteriormente, se ha visitado la pestaña Security-Alerts disponible en Kibana, donde aparece la regla de ejemplo elaborada disparada en 26 ocasiones, ratificando el correcto funcionamiento de esta.

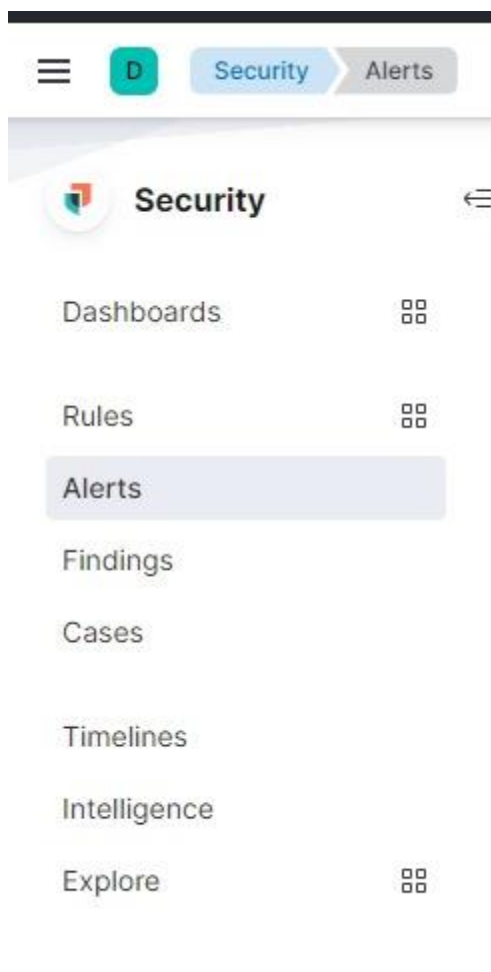


Figura 17: Pestaña Security-Alerts de Kibana

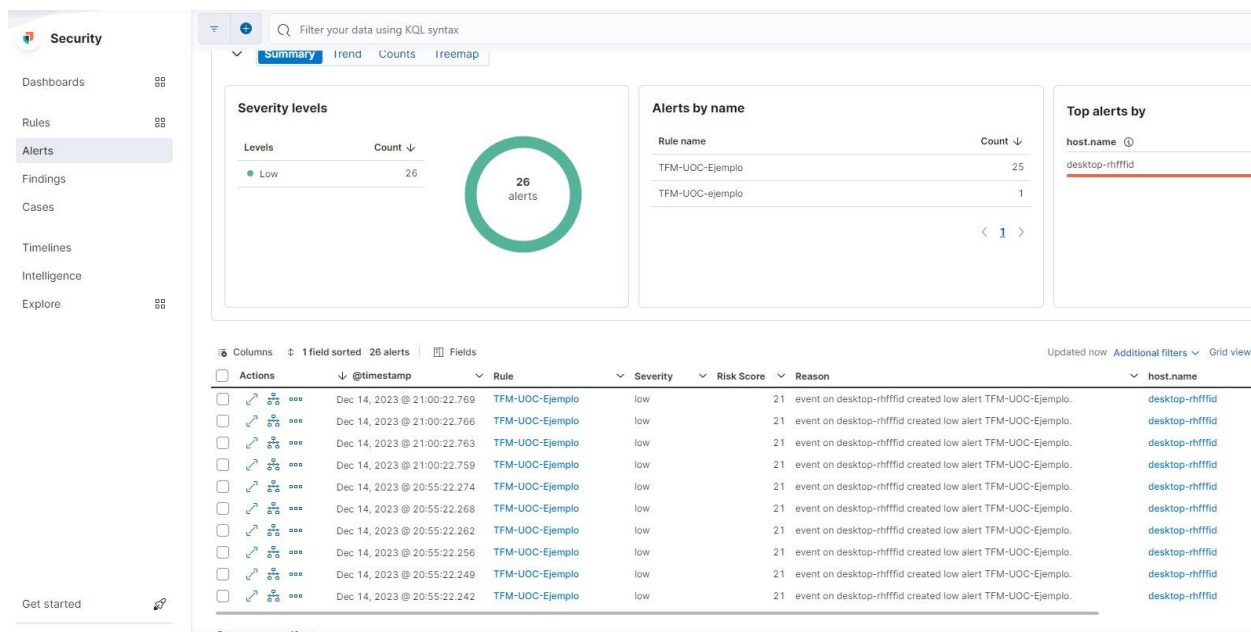


Figura 18: Regla de ejemplo disparada

3.5 Visualización de *dashboard* de ejemplo

El exitoso funcionamiento del *dashboard* implementado puede comprobarse visualizando y navegando por este, disponible en la pestaña Security-Dashboards.

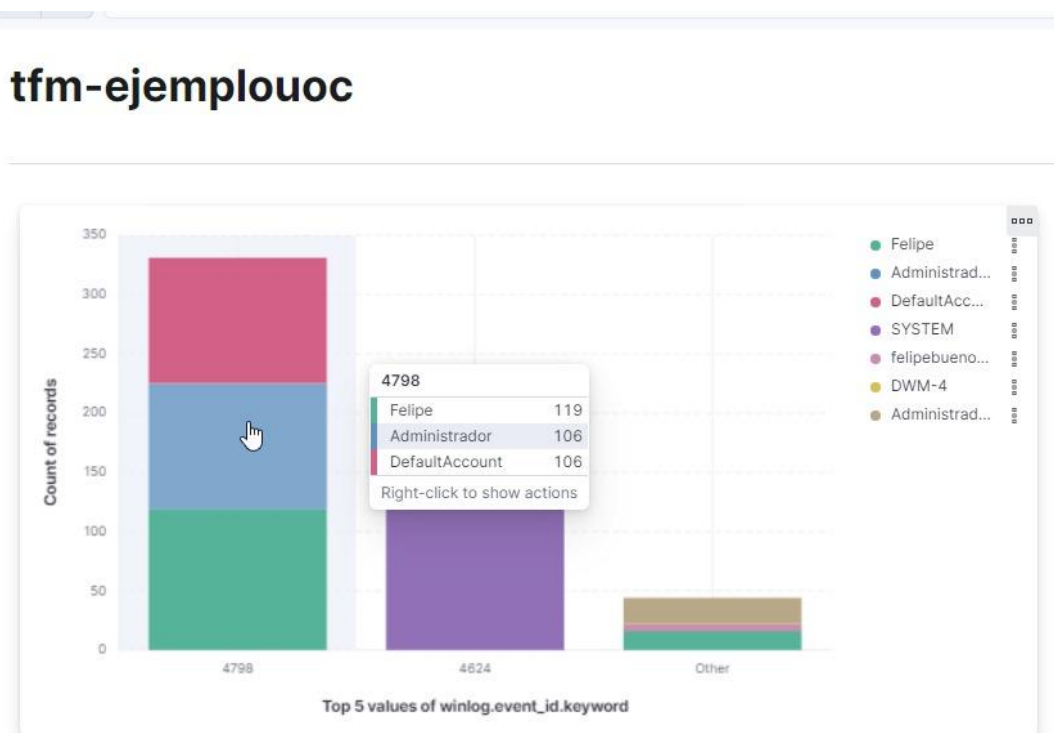


Figura 19: *Dashboard* de ejemplo

4 Conclusiones y trabajos futuros

4.1 Conclusiones del trabajo

Este Trabajo de Fin de Máster ha culminado en la creación de una guía exhaustiva para la instalación exitosa de la pila ELK en un entorno Windows, destacando la integración clave de *Winlogbeat*. Esta guía proporciona no solo los pasos concretos para la implementación, sino también *insights* valiosos sobre desafíos específicos del entorno Windows y las soluciones aplicadas.

La demostración de la funcionalidad operativa de ELK como Sistema de Gestión de Eventos de Seguridad (SIEM) en un entorno IT es un hito fundamental de este trabajo. La integración eficiente de *Winlogbeat* ha permitido una visión integral de los eventos del sistema Windows, evidenciando la eficacia de ELK en la gestión y análisis de datos de seguridad.

La implementación de una regla de correlación y la creación de un *dashboard* básico han sido elementos esenciales para ilustrar la utilidad práctica del sistema. La regla de correlación ha permitido ilustrar la facilidad para identificar patrones significativos en los eventos de seguridad mediante el lenguaje KQL (*Kibana Query Language*), mientras que el *dashboard* proporciona una interfaz visual y fácil de entender para el análisis en tiempo real.

Este trabajo, en su conjunto, destaca la relevancia de ELK como una solución esencial para un Centro de Operaciones de Seguridad (SOC). La visibilidad mejorada, la capacidad de correlación y las herramientas de visualización demuestran que ELK no solo es funcional, sino también operativo y eficaz en entornos IT.

Este Trabajo de Fin de Máster no solo ha sido un ejercicio técnico, sino también una contribución práctica al campo de la ciberseguridad al proporcionar una guía completa y una demostración tangible de la utilidad operativa de la pila ELK en un SOC.

4.2 Consecución de objetivos planteados

En términos generales, el trabajo ha alcanzado satisfactoriamente la mayoría de los objetivos propuestos. Sin embargo, se reconoce que hay áreas específicas, como la presentación visual en los dashboards y la profundización en las pruebas de detección de amenazas, que podrían haberse explorado más a fondo para enriquecer aún más la calidad del trabajo.

En futuras investigaciones o iteraciones, se sugiere dedicar más tiempo a la mejora de la representación visual de datos y a la realización de pruebas más exhaustivas, lo que podría elevar aún más la efectividad y robustez del SOC implementado.

Este proyecto no solo ha cumplido con los objetivos establecidos, sino que también ha proporcionado una base sólida para futuros desarrollos y mejoras

en la gestión de eventos de seguridad utilizando la pila ELK en un entorno Windows.

4.3 Seguimiento de la planificación y metodología a lo largo del producto

La planificación trazada en fases y pasos específicos fue un componente esencial para guiar el progreso del trabajo. Sin embargo, la naturaleza técnica y compleja de la implementación de la pila ELK en un entorno Windows ha presentado desafíos inesperados.

La planificación inicial, aunque proporcionó un marco general, se vio alterada por la necesidad de adaptarse a situaciones específicas que surgieron durante la instalación y configuración de la pila ELK. La realidad de tener que planificar de manera tan concreta, paso a paso, a meses vista, reveló la complejidad única de este tipo de proyectos y la dificultad de anticipar todos los obstáculos.

En este contexto, se hizo evidente la necesidad de introducir cambios en la planificación y metodología para garantizar el éxito del trabajo. La instalación y configuración, puntos críticos en el desarrollo, se encontraron con desafíos no previstos que exigieron una adaptación continua y ajustes en la marcha. Surgieron complicaciones durante la ejecución que lógicamente no estaban previstas en la planificación inicial.

Este proceso de ajuste continuo no solo ilustra la importancia de la flexibilidad en la gestión de proyectos, sino que también destaca la capacidad de adaptación necesaria al enfrentarse a proyectos técnicamente exigentes. Los cambios introducidos fueron esenciales para superar obstáculos específicos y garantizar que el proyecto avanzara de manera efectiva hacia la consecución de sus objetivos.

En resumen, la experiencia de planificar y ejecutar este proyecto ha proporcionado lecciones valiosas sobre la gestión de proyectos en entornos técnicos desafiantes. La adaptabilidad y la capacidad de ajustar la planificación según sea necesario fueron factores cruciales para superar obstáculos inesperados y garantizar el éxito global del trabajo.

4.4 Posibles mejoras y líneas de trabajo futuro

Durante la ejecución de este proyecto, se han identificado áreas clave que podrían beneficiarse de mejoras y enfoques adicionales, así como líneas de trabajo futuro que podrían elevar la eficacia y la robustez del sistema implementado.

Explorar la implementación de una arquitectura que separe la integración de *Logstash* y *Winlogbeat* proporcionaría beneficios en términos de modularidad y mantenimiento, permitiendo actualizaciones y ajustes independientes en cada componente sin afectar el funcionamiento general del sistema.

Introducir medidas de seguridad adicionales mediante la implementación de cifrado en el envío de logs ayudaría a prevenir posibles ataques de "man in the

middle" y garantizaría la integridad y confidencialidad de los datos transferidos entre los distintos componentes de la pila ELK.

Dedicar más tiempo a la preparación y refinamiento de reglas de correlación y dashboards implicaría una evaluación más profunda de los eventos para detectar patrones específicos y señales de incidentes potenciales. La mejora continua en este aspecto puede fortalecer la capacidad del sistema para identificar amenazas de manera proactiva.

Por último, considerar la generación intencionada de incidentes en las fuentes de datos como línea de trabajo futuro permitiría comprobar de manera efectiva la funcionalidad y eficacia de las reglas de correlación, así como la capacidad de respuesta del sistema ante situaciones de amenaza simuladas. Este enfoque práctico podría proporcionar una validación más completa de la robustez del sistema.

5 Bibliografía

- [1] *El estado de la ciberseguridad en España | Deloitte España*. (n.d.). Retrieved October 6, 2023, from <https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html>
- [2] *Retos de los SOC | WatchGuard Blog*. (n.d.). Retrieved October 6, 2023, from <https://www.watchguard.com/es/wgrd-news/blog/que-retos-se-enfrentan-los-socs-en-ciberseguridad-en-los-proximos-meses>
- [3] *SOC y SIEM: Monitorización continua frente a ciberataques*. (n.d.). Retrieved October 8, 2023, from <https://globalt4e.com/soc-siem-monitorizacion-continua-ciberataques/>
- [4] *Los beneficios de la pila ELK sin la carga operativa*. (n.d.). Retrieved October 12, 2023, from <https://aws.amazon.com/es/opensearch-service/resources/the-benefits-of-the-elk-stack/>
- [5] *Topics | IBM*. (n.d.). Retrieved October 14, 2023, from <https://www.ibm.com/topics>
- [6] *¿Qué es SOC (Centro de Operaciones de Seguridad)? - Software Check Point*. (n.d.). Retrieved October 30, 2023, from <https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-soc/>
- [7] *SIEM: Qué es, cómo funciona y cuáles son sus beneficios*. (n.d.). Retrieved October 30, 2023, from <https://www.deltaprotect.com/blog/siem-que-es>
- [8] *What is SIEM? | Microsoft Security*. (n.d.). Retrieved October 30, 2023, from <https://www.microsoft.com/en-us/security/business/security-101/what-is-siem>
- [9] *¿Qué significa SIEM y cómo funciona?* (n.d.). Retrieved October 30, 2023, from <https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona>
- [10] *¿Qué es SIEM (gestión de eventos e información de seguridad)? | Elastic SIEM*. (n.d.). Retrieved October 30, 2023, from <https://www.elastic.co/es/what-is/siem>
- [11] *ELK Stack: ¿Qué es y cómo implementarlo fácilmente mediante DOCKER?* (n.d.). Retrieved October 31, 2023, from

<https://www.encora.com/es/blog/elk-stack-que-es-y-como-implementarlo-facilmente-mediante-docker>

- [12] *¿Qué es ELK? Elasticsearch, Logstash y Kibana | OpenWebinars.* (n.d.). Retrieved October 31, 2023, from <https://openwebinars.net/blog/que-es-elk-elasticsearch-logstash-y-kibana/>
- [13] *Beats Parte 1 - ¿Conoces los Beats de Elasticsearch? Introducción y casos de uso.* (n.d.). Retrieved October 31, 2023, from <https://datadope.io/beats-parte-1-conoces-los-beats-de-elasticsearch-introduccion-y-casos-de-uso/>
- [14] *Usar Elasticsearch, ¿qué ventajas ofrece esta tecnología?* (n.d.). Retrieved October 31, 2023, from <https://itelligent.es/ventajas-elasticsearch/>
- [15] *¿Qué es un stack de ELK y qué ventajas tiene implementarlo? - Blog de hiberus.* (n.d.). Retrieved November 10, 2023, from <https://www.hiberus.com/crecemos-contigo/que-es-un-stack-de-elk-y-que-ventajas-tiene-implementarlo/>
- [16] *¿Qué son los eventos de Windows? | KeepCoding Bootcamps.* (n.d.). Retrieved November 10, 2023, from <https://keepcoding.io/blog/que-son-los-eventos-de-windows/>
- [17] *Gestión de registros de eventos | NetIQ.* (n.d.). Retrieved November 10, 2023, from <https://www.netiq.com/es-es/documentation/directory-and-resource-administrator-92/drauserguide/data/b151ta9f.htm>
- [18] *Descarga los productos de Elastic | Elastic.* (n.d.). Retrieved November 10, 2023, from <https://www.elastic.co/es/downloads>
- [19] *Java Archive Downloads - Java SE 17.* (n.d.). Retrieved November 10, 2023, from <https://www.oracle.com/java/technologies/javase/jdk17-archive-downloads.html>
- [20] *Prebuilt rule reference | Elastic Security Solution [8.11] | Elastic.* (n.d.). Retrieved December 17, 2023, from <https://www.elastic.co/guide/en/security/current/prebuilt-rules.html>

- [21] *Windows Security Log Event ID 4798 - A user's local group membership was enumerated.* (n.d.). Retrieved December 17, 2023, from <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4798>
- [22] *Te damos la bienvenida a Chrome Webstore | Chrome Webstore.* (n.d.). Retrieved December 17, 2023, from <https://chrome.google.com/webstore?hl=es>
- [23] *Elasticsearch: Motor de búsqueda y analítica distribuido oficial | Elastic.* (n.d.). Retrieved December 17, 2023, from <https://www.elastic.co/es/elasticsearch>
- [24] *Download Winlogbeat | Ship Windows Event Logs | Elastic | Elastic.* (n.d.). Retrieved December 15, 2023, from <https://www.elastic.co/es/downloads/beats/winlogbeat>
- [25] *Winlogbeat quick start: installation and configuration | Winlogbeat Reference [8.11] | Elastic.* (n.d.). Retrieved December 15, 2023, from <https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-installation-configuration.html>
- [26] *Install Winlogbeat And Configure With Logstash On Windows | Tutorials24x7.* (n.d.). Retrieved December 15, 2023, from <https://elasticsearch.tutorials24x7.com/blog/install-winlogbeat-and-configure-with-logstash-on-windows>
- [27] *Encryption key generator | generate-random.org.* (n.d.). Retrieved December 16, 2023, from <https://generate-random.org/encryption-key-generator>
- [28] *Secure saved objects | Elastic.* (n.d.). Retrieved December 16, 2023, from <https://www.elastic.co/guide/en/kibana/current/xpack-security-secure-saved-objects.html>
- [29] *Create and manage rules | Elastic.* (n.d.). Retrieved December 16, 2023, from <https://www.elastic.co/guide/en/kibana/current/create-and-manage-rules.html>

6 Anexos

A. Guía de instalación de la pila ELK

1. Elasticsearch

En primer lugar, es necesario instalar Java si no se dispone ya de él. Para ello se ha descargado la última versión (17.0.9) disponible desde el repositorio oficial de *Oracle* [19].



Figura 20: Descarga de Java

Además, es necesario editar la variable de entorno para hacer que coincida con la versión de Java que acabamos de instalar.

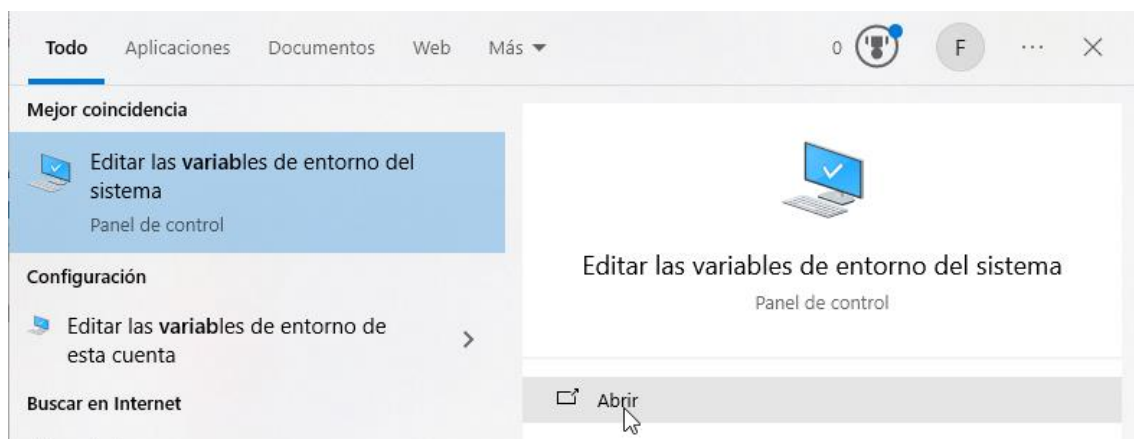


Figura 21: Editar variables de entorno 1

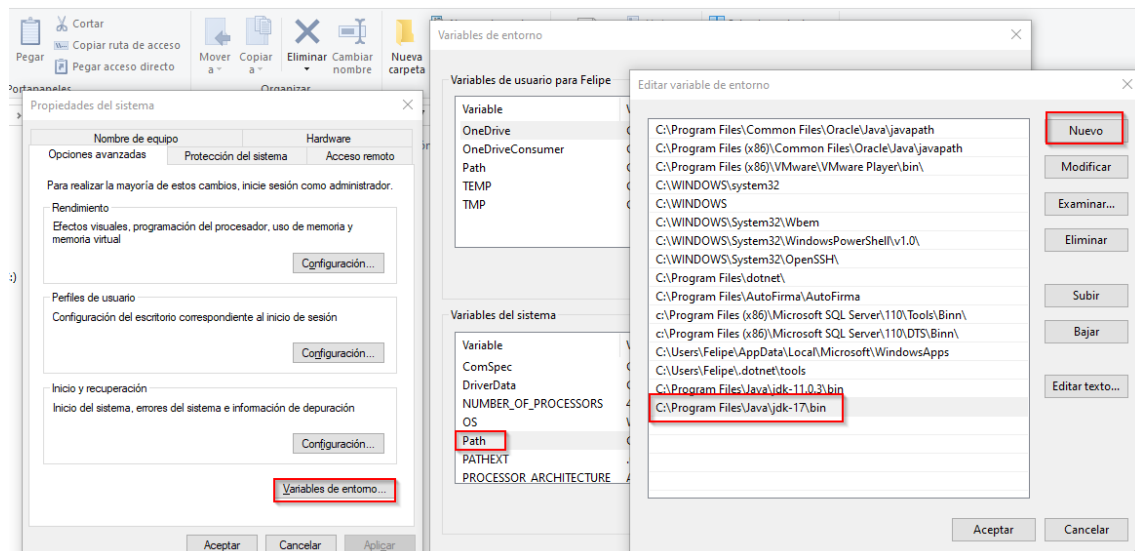


Figura 22: Editar variables de entorno 2

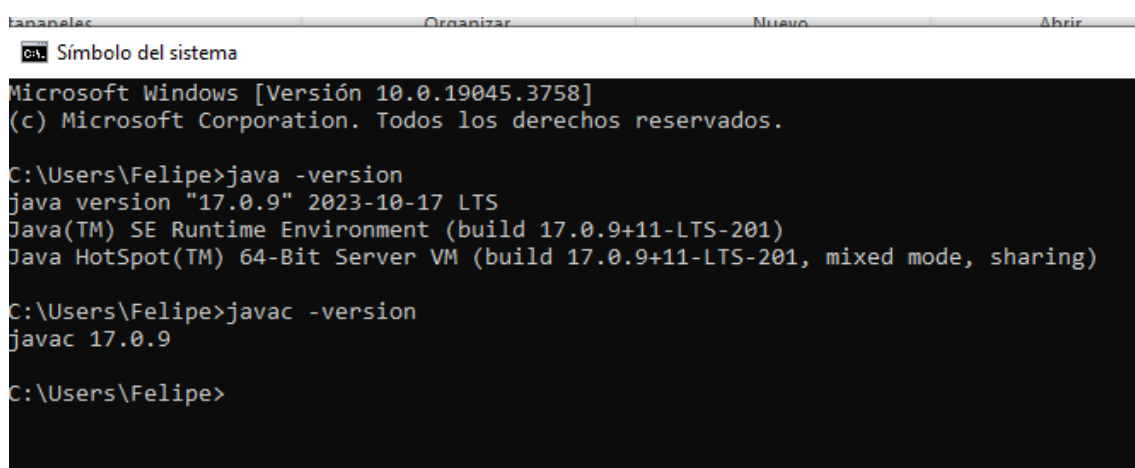


Figura 23: Demostración ruta binario *javac*

Adicionalmente, se añade la ruta al programa a una nueva variable de entorno llamada `SE_JAVA_HOME`, que utiliza *Elasticsearch*.

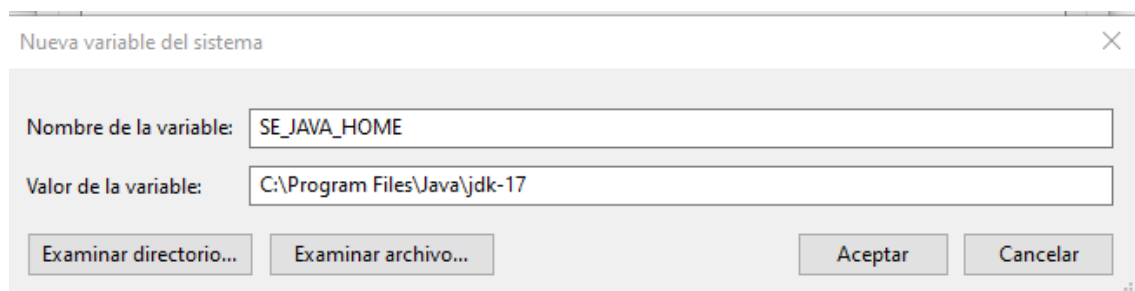


Figura 24: Nueva variable de entorno `SE_JAVA_HOME`

Tras haber instalado Java en su última versión, descargamos Elasticsearch del repositorio oficial [18] y descomprimos.

Se abre una terminal y se ejecuta el fichero “`elasticsearch.bat`” disponible en el repositorio “`bin`”.

2. Kibana

De manera análoga a Elasticsearch, se descarga el servicio del repositorio oficial [18], se descomprime y se ejecuta en un terminal el fichero “kibana.bat”.








Nombre	Fecha de modificacion	tipo	tamaño
 kibana	05/12/2023 12:17	Archivo por lotes ...	1 KB
 kibana-encryption-keys	05/12/2023 12:17	Archivo por lotes ...	1 KB
 kibana-health-gateway	05/12/2023 12:17	Archivo por lotes ...	1 KB
 kibana-keystore	05/12/2023 12:17	Archivo por lotes ...	1 KB
 kibana-plugin	05/12/2023 12:17	Archivo por lotes ...	1 KB
 kibana-setup	05/12/2023 12:17	Archivo por lotes ...	1 KB
 kibana-verification-code	05/12/2023 12:17	Archivo por lotes ...	1 KB

Figura 27: Carpeta "bin" de Kibana

Se ejecuta el fichero también por terminal.

```
[2023-12-08T12:45:01.918+01:00][INFO ][plugins-service] Plugin "serverlessObservability" is disabled.
[2023-12-08T12:45:01.919+01:00][INFO ][plugins-service] Plugin "serverlessSearch" is disabled.
[2023-12-08T12:45:02.413+01:00][INFO ][http.server.Preboot] http server running at http://localhost:5601
[2023-12-08T12:45:02.909+01:00][INFO ][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
[2023-12-08T12:45:02.915+01:00][INFO ][preboot] "interactiveSetup" plugin is holding setup: Validating Elasticsearch connection configuration...
[2023-12-08T12:45:03.056+01:00][INFO ][root] Holding setup until preboot stage is completed.

i Kibana has not been configured.
Go to http://localhost:5601/?code=746152 to get started.
```

Figura 28: Resultado de la ejecución de kibana.bat

Tras la ejecución, el terminal nos muestra un enlace para configurar Kibana vía interfaz web.

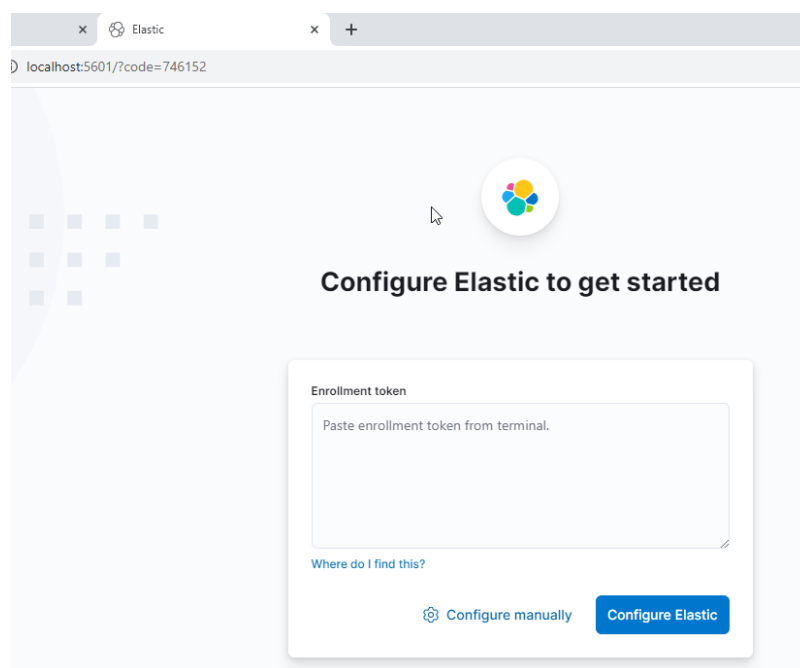


Figura 29: Configuración de Kibana vía interfaz

Ahora es cuando se necesita pegar el token apuntado en el paso anterior de Elasticsearch, una vez realizado se pincha en “Configure Elastic”.

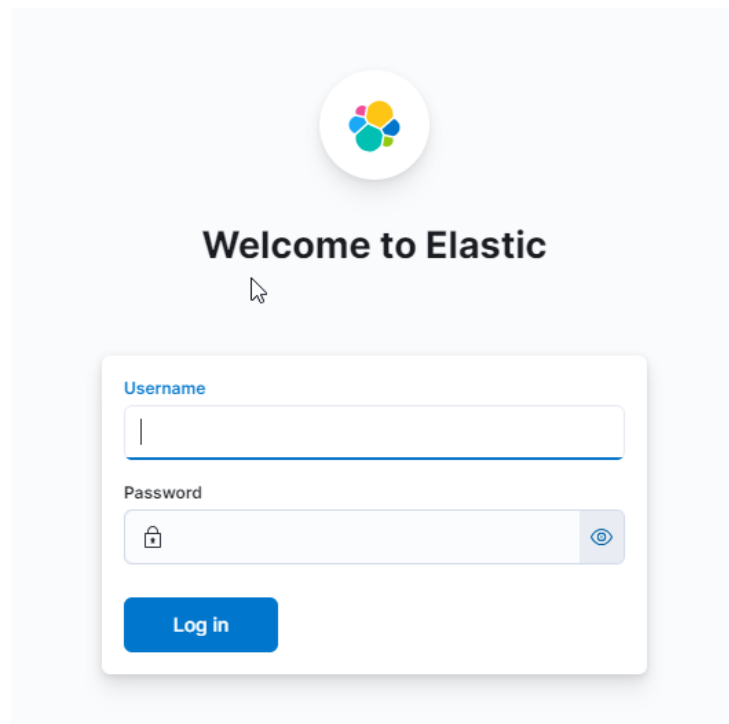


Figura 30: Inicio de sesión en Kibana

Una vez configurado, Kibana solicita un login que también debió ser apuntado en el paso anterior.

Tras iniciar sesión de manera satisfactoria, Kibana es perfectamente accesible en el puerto 5601.

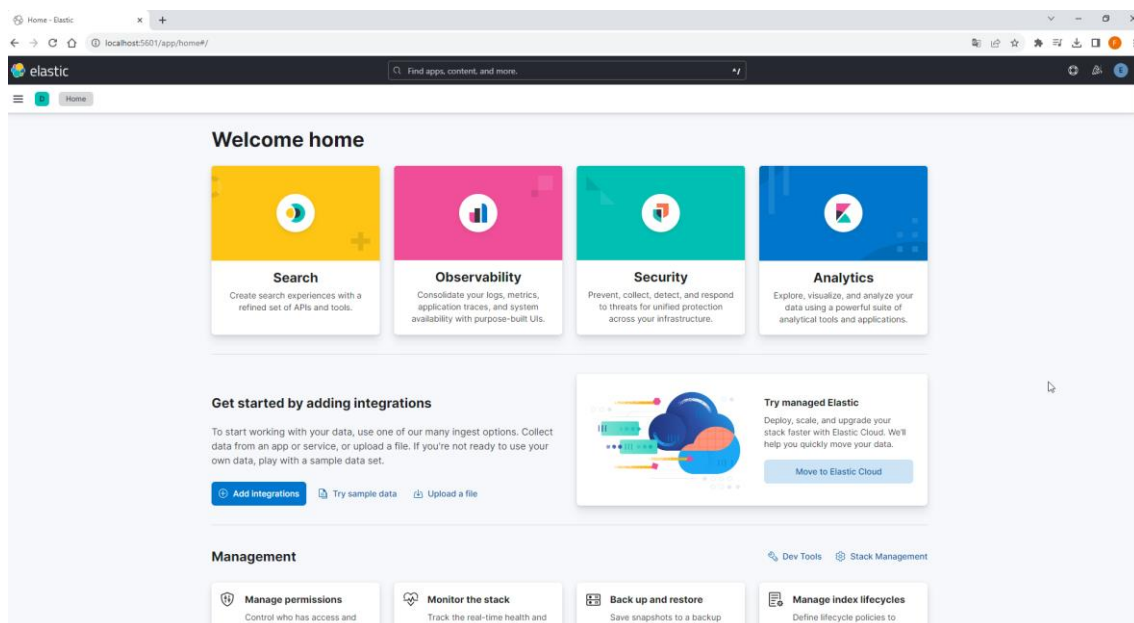
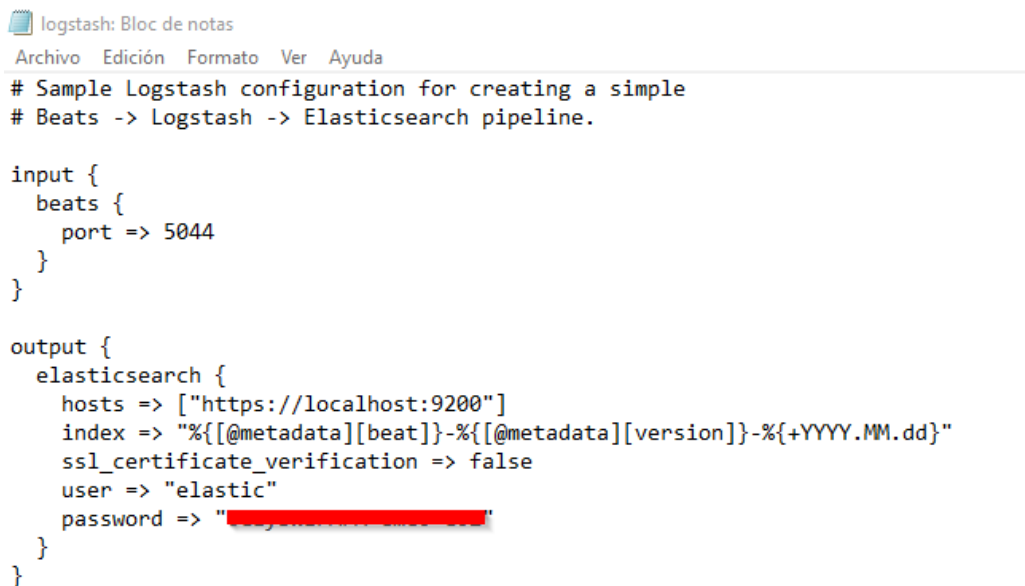


Figura 31: Página inicial de Kibana

3. Logstash

Para instalar y configurar Logstash, además de realizar la descarga y extracción como en los servicios anteriores, es necesario modificar el fichero “logstash.conf” con los parámetros deseados de envío hacia Elasticsearch y recepción de logs.

En nuestro caso, Logstash ha sido configurado para recibir *beats* por el puerto 5044, y enviar datos a Elasticsearch hacia <https://localhost:9200>, con el usuario y contraseña utilizado por Elasticsearch.

A screenshot of a Notepad window titled "logstash: Bloc de notas". The window has a menu bar with "Archivo", "Edición", "Formato", "Ver", and "Ayuda". The text content is a Logstash configuration file. It starts with two comments: "# Sample Logstash configuration for creating a simple" and "# Beats -> Logstash -> Elasticsearch pipeline.". The configuration is divided into an "input" section and an "output" section. The "input" section has a "beats" block with "port => 5044". The "output" section has an "elasticsearch" block with "hosts => [\"https://localhost:9200\"]", "index => \"%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}\"", "ssl_certificate_verification => false", "user => \"elastic\"", and "password => \"[REDACTED]\"". The password field is highlighted with a red background.

```
logstash: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
# Sample Logstash configuration for creating a simple
# Beats -> Logstash -> Elasticsearch pipeline.

input {
  beats {
    port => 5044
  }
}

output {
  elasticsearch {
    hosts => [\"https://localhost:9200\"]
    index => \"%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}\"
    ssl_certificate_verification => false
    user => \"elastic\"
    password => \"[REDACTED]\"
  }
}
```

Figura 32: Fichero de configuración Logstash

Para que la configuración anterior sea efectiva, es necesario cargarla con el parámetro “-f” al ejecutar vía terminal. El comando en este caso ha quedado de la siguiente manera:

```
logstash -f
C:\Users\Felipe\Downloads\TFM\ELK\logstash\config\logstash.conf
```

Tras la ejecución del comando, ya tenemos Logstash preparado para la recepción de datos y su posterior envío a Elasticsearch.

4. Winlogbeat

En primer lugar, como siempre, descarga y descompresión desde el repositorio oficial [24]

Para instalar y configurar correctamente Winlogbeat de la manera deseada para este trabajo, es necesario modificar el fichero de configuración “winlogbeat.conf” con los apartados deseados.

En nuestro caso, se añaden los siguientes eventos de Windows para enviar.

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security

  - name: Microsoft-Windows-Sysmon/Operational

  - name: Windows PowerShell
    event_id: 400, 403, 600, 800

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

  - name: ForwardedEvents
    tags: [forwarded]
```

Figura 33: Configuración eventos de Windows en Winlogbeat

Se configura el envío a Kibana para nuestro sistema, añadiendo la URL y el login correspondiente.

```
# ===== Kibana =====

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "http://localhost:5601"
  username: "elastic"
  password: "6GEysWEFAFM-cmc0-G0Z"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

# ===== Elastic Cloud =====
```

Figura 34: Envío a Kibana desde Winlogbeat

También es necesario configurar el envío a Logstash, para lo que añadimos el host donde escucha Logstash. En este trabajo se ha obviado la protección SSL en esta dirección de la comunicación.

```
# ----- Logstash Output -----
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

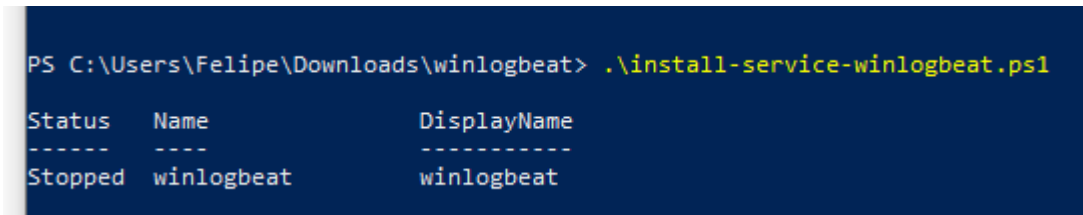
  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

Figura 35: Envío a Logstash desde Winlogbeat

Para que Winlogbeat sea instalado como un servicio de Windows, podemos basarnos en la configuración recomendada del servicio [25], donde explica detalladamente los comandos a realizar.

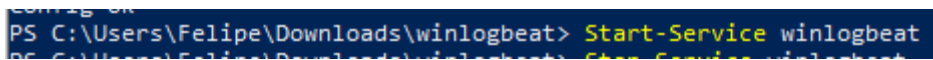
En primer lugar, abrimos un *Powershell* y ejecutamos el script disponible desde el repositorio principal.



```
PS C:\Users\Felipe\Downloads\winlogbeat> .\install-service-winlogbeat.ps1

Status  Name      DisplayName
-----
Stopped winlogbeat winlogbeat
```

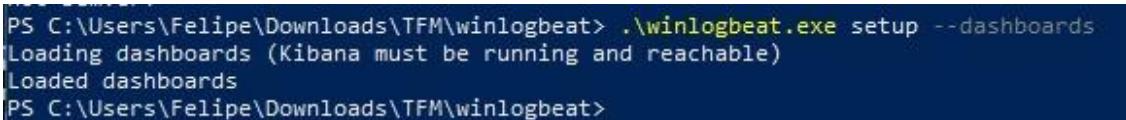
Figura 36: Comando instalación Winlogbeat como servicio 1



```
PS C:\Users\Felipe\Downloads\winlogbeat> Start-Service winlogbeat
PS C:\Users\Felipe\Downloads\winlogbeat> Stop-Service winlogbeat
```

Figura 37: Comando instalación Winlogbeat como servicio 2

Adicionalmente, podemos ejecutar el siguiente comando para cargar los dashboard por defecto de los que dispone Winlogbeat [26].



```
PS C:\Users\Felipe\Downloads\TFM\winlogbeat> .\winlogbeat.exe setup --dashboards
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
PS C:\Users\Felipe\Downloads\TFM\winlogbeat>
```

Figura 38: Cargar dashboards de Winlogbeat

B. Guía de configuración de reglas y *dashboards*

1. Reglas de correlación

En primer lugar, al navegar hacia la pestaña Security-Rules en Kibana, nos aparece el siguiente mensaje.

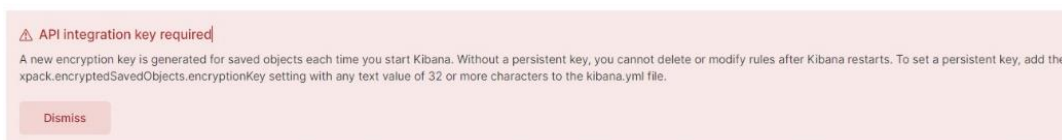


Figura 39: Solicitud de integración API Key

Para cumplir con el requisito (ya que queremos que los cambios realizados persistan), se genera una API Key aleatoria con una herramienta online gratuita [27] y se añade al fichero de configuración de Kibana, concretamente al parámetro `xpack.encryptedSavedObjects`, tal y como recomienda la documentación oficial [28].

Ahora si, siguiendo la guía oficial de creación y manipulación de reglas [29], se procede a crear una regla básica de correlación que detecte el evento de windows 4798 y el username "Felipe".

Se pincha en "Detection rules (SIEM)" en el panel principal de Security-Rules.

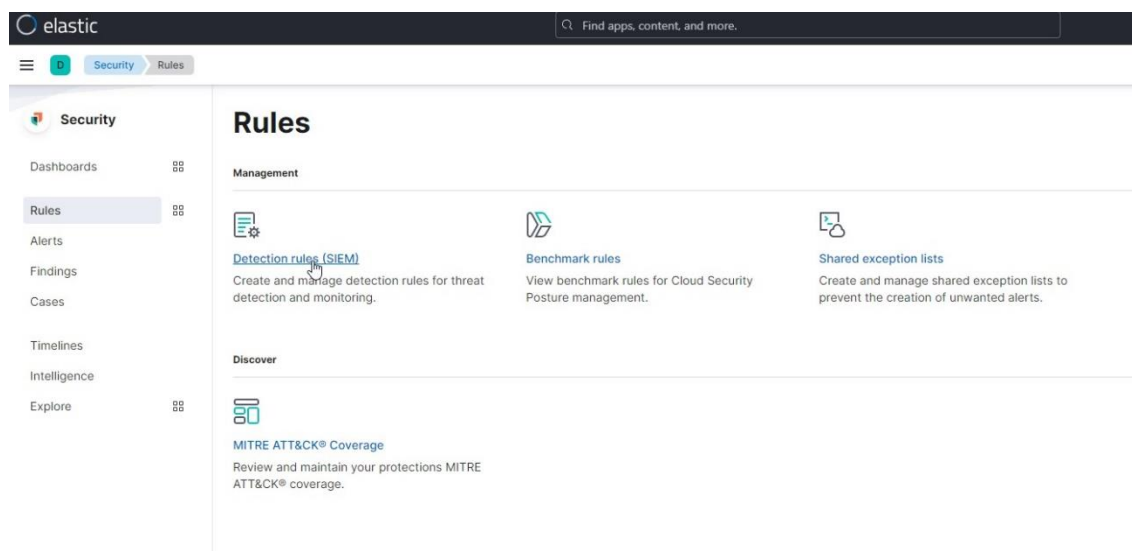


Figura 40: Panel principal de Reglas

Posteriormente, pinchamos en “Create new rule”

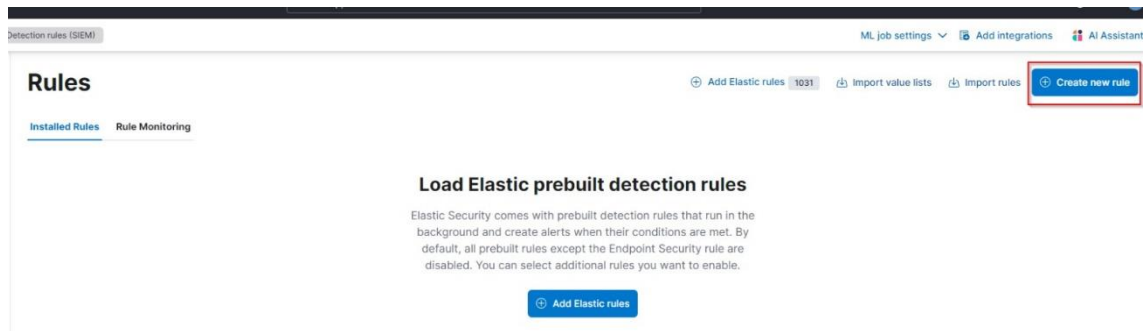


Figura 41: Creación de regla 1

Seleccionamos “Custom query”, para crear la regla a través de una Query que introduciremos manualmente.

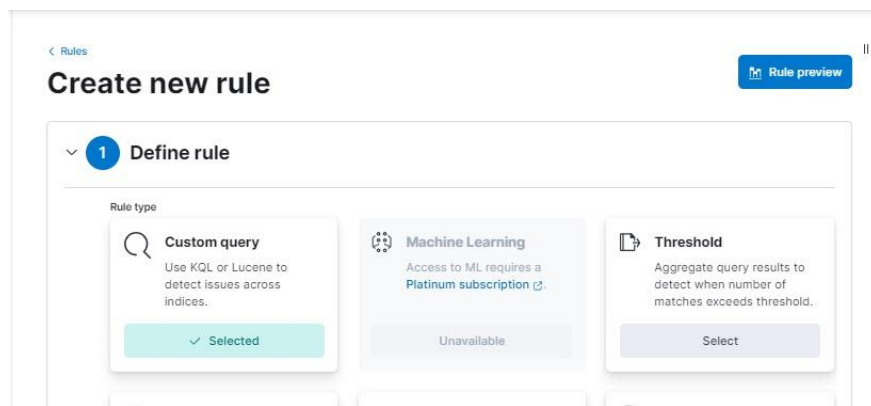


Figura 42: Definición de regla

Tras esto, introducimos la siguiente Query: “
_index : winlogbeat-* and winlog.event_id : 4798 and
winlog.event_data.TargetUserName : Felipe”.

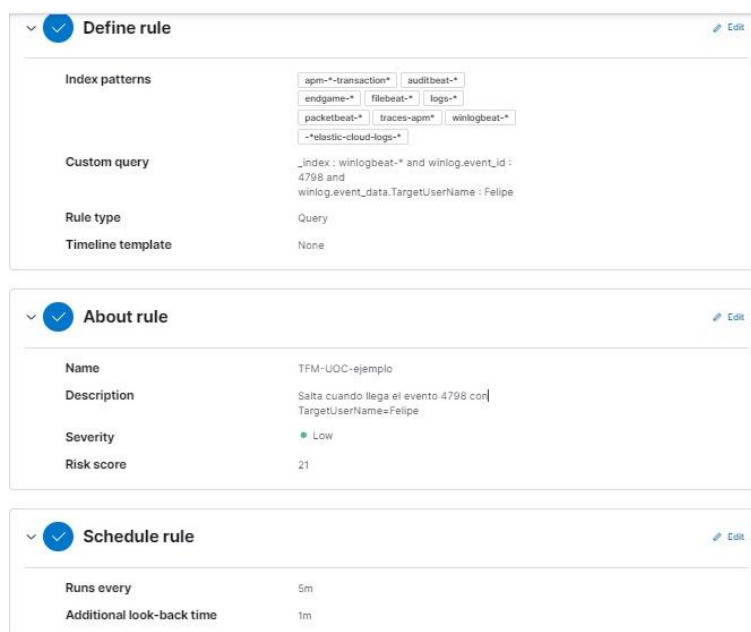


Figura 43: Regla TFM-UOC-ejemplo

2. Dashboards

Para la creación de un dashboard básico, pinchamos en “Create Dashboard”, disponible en la pestaña Security-Dashboards.

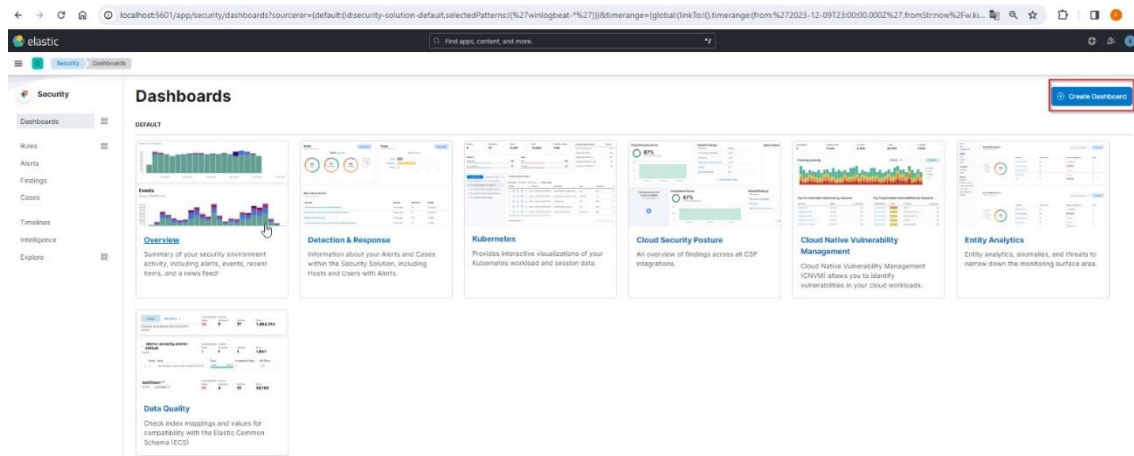


Figura 44: Pestaña Security-Dashboards

Posteriormente, pinchamos en “Create visualization”

Editing new dashboard



Tras esto, se abrirá un panel donde podemos manipular los parámetros deseados que estarán presentes en el dashboard, en nuestro caso, se ha añadido una cuenta (eje vertical) de los top 5 valores del parámetro `winlog.event_id.keyword` (eje horizontal), donde se almacenan los valores de Windows ID.

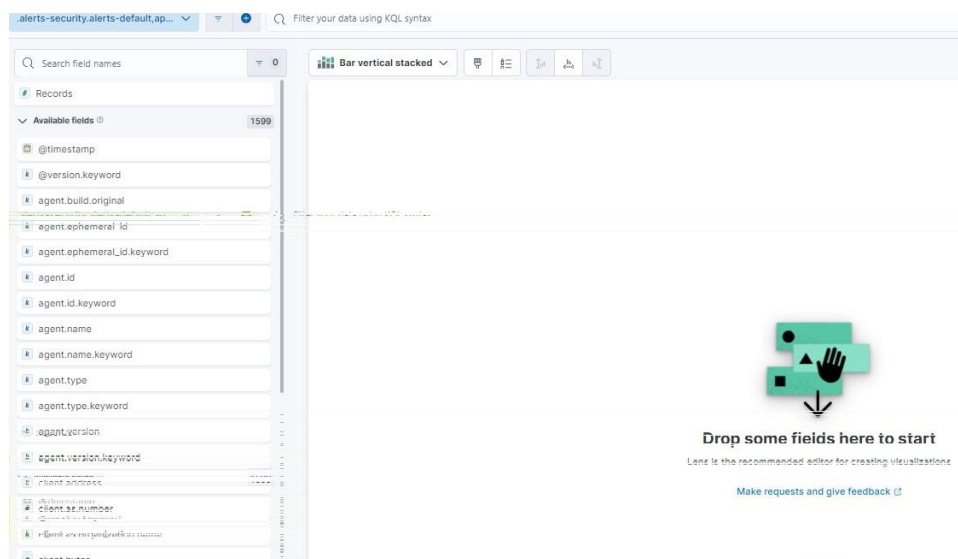


Figura 45: Creación de dashboard

La ejecución del dashboard en la última semana se ve de la siguiente manera.

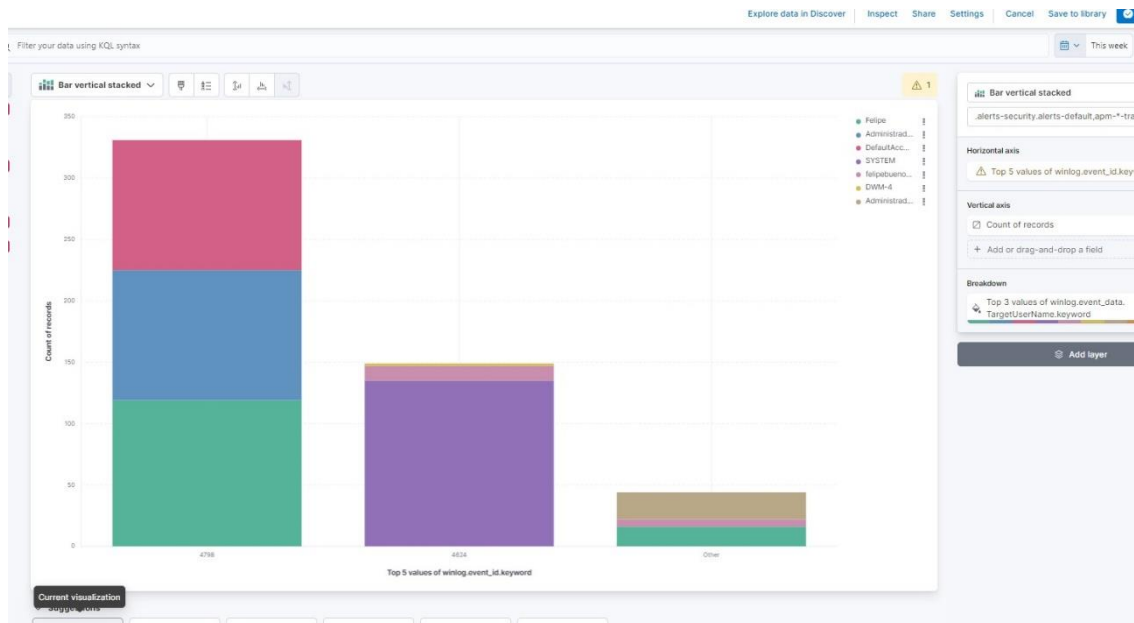


Figura 46: Dashboard creado ejecutado en última semana

Pinchamos en “Save Dashboard” y lo guardamos con un nombre y descripción.

The screenshot shows the 'Save dashboard' dialog box. The dialog box has a title 'Save dashboard' and a close button. It contains the following fields and options:

- Title:** A text input field containing 'TFM-Ejemplo'.
- Description:** A text area containing 'Muestra los TargetUserName de los eventos 4798'. The word 'TargetUserName' is underlined in red.
- Tags:** A list of tags with 'Security Solution' selected. There is a dropdown arrow next to the tag.
- Store time with dashboard:** A checkbox that is currently unchecked. Below it, a note says: 'This changes the time filter to the currently selected time each time this dashboard is loaded.'
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

Figura 47: Guardar dashboard

